Zbiór Orzeczeń

WYROK TRYBUNAŁU (wielka izba)

z dnia 21 czerwca 2022 r.*

Spis treści

I. Ramy prawne . . . 5

A. Prawo Unii . . . 5

1. Dyrektywa 95/46 . . . 5

2. Dyrektywa API . . . 6

3. Dyrektywa 2010/65 . . . 8

4. RODO . . . 9

5. Dyrektywa 2016/680 . . . 12

6. Dyrektywa PNR . . . 13

7. Decyzja ramowa 2002/475 . . . 27

B. Prawo belgijskie . . . 28

1. Konstytucja . . . 28

2. Ustawa z dnia 25 grudnia 2016 r. . . . 28

II. Spór w postępowaniu głównym i pytania prejudycjalne . . . 32

III. W przedmiocie pytań prejudycjalnych . . . 36

A. W przedmiocie pytania pierwszego . . . 36

B. W przedmiocie pytań od drugiego do czwartego oraz pytania szóstego . . . 40

1. W przedmiocie wynikającej z dyrektywy PNR ingerencji w prawa podstawowe zagwarantowane w art. 7 i 8 karty . . . 41

* Język postępowania: francuski.

2. W przedmiocie uzasadnienia ingerencji wynikającej z dyrektywy PNR 44

a) W przedmiocie poszanowania zasady legalności oraz istoty rozpatrywanych praw podstawowych 45

b) W zakresie celu interesu ogólnego oraz przydatności przetwarzania danych PNR w świetle tego celu 46

c) W przedmiocie koniecznego charakteru ingerencji wynikających z dyrektywy PNR 47

1) W przedmiocie danych pasażerów lotniczych wskazanych w dyrektywie PNR . 47

2) W przedmiocie celów przetwarzania danych PNR 49

3) W przedmiocie powiązania pomiędzy danymi PNR a celami przetwarzania tych danych 51

4) W przedmiocie pasażerów lotniczych i konkretnych lotów 52

5) W przedmiocie wstępnej oceny danych PNR za pomocą zautomatyzowanego przetwarzania 55

i) W przedmiocie zestawiania danych PNR z bazami danych 56

ii) W przedmiocie przetwarzania danych PNR według wcześniej ustalonych kryteriów 58

iii) W przedmiocie gwarancji towarzyszących zautomatyzowanemu przetwarzaniu danych PNR 60

6) W przedmiocie przekazywania i późniejszej oceny danych PNR 62

C. W przedmiocie pytania piątego 65

D. W przedmiocie pytania siódmego 66

E. W przedmiocie pytania ósmego 68

F. W przedmiocie pytania dziewiątego lit. a) 70

G. W przedmiocie pytania dziewiątego lit. b) 71

H. W przedmiocie pytania dziesiątego 75

IV. W przedmiocie kosztów 77

Odesłanie prejudycjalne – Przetwarzanie danych osobowych – Dane dotyczące przelotu pasażera (PNR) – Rozporządzenie (UE) 2016/679 – Artykuł 2 ust. 2 lit. d) – Zakres stosowania – Dyrektywa (UE) 2016/681 – Wykorzystywanie danych PNR pasażerów odbywających loty między Unią i państwami trzecimi – Możliwość włączenia danych pasażerów lotów wewnątrzunijnych – Zautomatyzowane przetwarzanie danych – Okres zatrzymania – Zwalczanie przestępstw terrorystycznych i poważnej przestępczości – Ważność – Karta praw

podstawowych Unii Europejskiej – Artykuły 7, 8 i 21 oraz art. 52 ust. 1 – Uregulowanie krajowe rozszerzające zastosowanie systemu PNR na inne rodzaje przewozów wewnątrz Unii – Swoboda przemieszczania się w obrębie Unii – Karta praw podstawowych – Artykuł 45

W sprawie C-817/19

mającej za przedmiot wniosek o wydanie, na podstawie art. 267 TFUE, orzeczenia w trybie prejudycjalnym, złożony przez Cour constitutionnelle (trybunał konstytucyjny, Belgia) postanowieniem z dnia 17 października 2019 r., które wpłynęło do Trybunału w dniu 31 października 2019 r., w postępowaniu:

Ligue des droits humains

przeciwko

Conseil des ministres,

TRYBUNAŁ (wielka izba),

w składzie: K. Lenaerts, prezes, A. Arabadjiev, S. Rodin, I. Jarukaitis i N. Jääskinen, prezesi izb, T. von Danwitz (sprawozdawca), M. Safjan, F. Biltgen, P. G. Xuereb, N. Piçarra, L. S. Rossi, A. Kumin i N. Wahl, sędziowie,

rzecznik generalny: G. Pitruzzella,

sekretarz: M. Krausenböck, administratorka,

uwzględniając pisemny etap postępowania i po przeprowadzeniu rozprawy w dniu 13 lipca 2021 r.,

rozważywszy uwagi, które przedstawili:

– w imieniu Ligue des droits humains – C. Forget, avocate,

– w imieniu rządu belgijskiego – P. Cottin, J.-C. Halleux, C. Pochet i M. Van Regemorter, w charakterze pełnomocników, których wspierali C. Caillet, advocaat, E. Jacubowitz, avocat oraz G. Ceuppens, V. Dethy i D. Vertongen,

– w imieniu rządu czeskiego – T. Machovičová, O. Serdula, M. Smolek i J. Vláčil, w charakterze pełnomocników,

– w imieniu rządu duńskiego – M. Jespersen, J. Nymann-Lindegren, V. Pasternak Jørgensen i M. Søndahl Wolff, w charakterze pełnomocników,

– w imieniu rządu niemieckiego – D. Klebs i J. Möller, w charakterze pełnomocników,

– w imieniu rządu estońskiego – N. Grünberg, w charakterze pełnomocnika,

– w imieniu Irlandii – M. Browne, A. Joyce i J. Quaney, w charakterze pełnomocników, których wspierał D. Fennelly, BL,

– w imieniu rządu hiszpańskiego – L. Aguilera Ruiz, w charakterze pełnomocnika,

– w imieniu rządu francuskiego – D. Dubois, E. de Moustier i T. Stehelin, w charakterze pełnomocników,

– w imieniu rządu cypryjskiego – E. Neofytou, w charakterze pełnomocnika,

– w imieniu rządu łotewskiego – E. Bārdiņš, K. Pommere i V. Soņeca, w charakterze pełnomocników,

– w imieniu rządu niderlandzkiego – M. K. Bulterman, A. Hanje, J. Langer i C. S. Schillemans, w charakterze pełnomocników,

– w imieniu rządu austriackiego – G. Kunnert, A. Posch i J. Schmoll, w charakterze pełnomocników,

– w imieniu rządu polskiego – B. Majczyna, w charakterze pełnomocnika,

– w imieniu rządu słowackiego – B. Ricziová, w charakterze pełnomocnika,

– w imieniu rządu fińskiego – A. Laine i H. Leppo, w charakterze pełnomocników,

– w imieniu Parlamentu Europejskiego – O. Hrstková Šolcová i P. López-Carceller, w charakterze pełnomocników,

– w imieniu Rady Unii Europejskiej – J. Lotarski, N. Rouam, E. Sitbon i C. Zadra, w charakterze pełnomocników,

– w imieniu Komisji Europejskiej – D. Nardi i M. Wasmeier, w charakterze pełnomocników,

– w imieniu Europejskiego Inspektora Ochrony Danych – P. Angelov, A. Buchta, F. Coudert i C.-A. Marnier, w charakterze pełnomocników,

– w imieniu Agencji Praw Podstawowych Unii Europejskiej – L. López, T. Molnar, M. Nespor i M. O'Flaherty, w charakterze pełnomocników,

po zapoznaniu się z opinią rzecznika generalnego na posiedzeniu w dniu 27 stycznia 2022 r.,

wydaje następujący

Wyrok

1 Wniosek o wydanie orzeczenia w trybie prejudycjalnym w niniejszej sprawie dotyczy co do istoty:

– wykładni art. 2 ust. 2 lit. d) oraz art. 23 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia 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, zwanego dalej

„RODO”), dyrektywy Rady 2004/82/WE z dnia 29 kwietnia 2004 r. w sprawie zobowiązania przewoźników do przekazywania danych pasażerów (Dz.U. 2004, L 261, s. 24, zwanej dalej „dyrektywą API”) oraz dyrektywy Parlamentu Europejskiego i Rady 2010/65/UE z dnia 20 października 2010 r. w sprawie formalności sprawozdawczych dla statków wchodzących do lub wychodzących z portów państw członkowskich i uchylającej dyrektywę 2002/6/WE (Dz.U. 2010, L 283, s. 1);

– wykładni i ważności, w świetle art. 7 i 8 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej „kartą”), art. 3 pkt 4, art. 6 i 12 oraz załącznika I do dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz.U. 2016, L 119, s. 132, zwanej dalej „dyrektywą PNR”), a także

– wykładni oraz ważności, w świetle art. 3 ust. 2 TUE oraz art. 45 karty, dyrektywy API.

2 Przedmiotowy wniosek został złożony w ramach sporu między Ligue des droits humains a Conseil des ministres (radą ministrów, Belgia) w przedmiocie zgodności z prawem ustawy z dnia 25 grudnia 2016 r. o przetwarzaniu danych pasażerów.

I. Ramy prawne

A. Prawo Unii

1. Dyrektywa 95/46

3 Dyrektywa 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) została uchylona z dniem 25 maja 2018 r. przez RODO. Artykuł 3 ust. 2 owej dyrektywy stanowił:

„Niniejsza dyrektywa nie ma zastosowania do przetwarzania danych osobowych:

– w ramach działalności wykraczającej poza zakres prawa Wspólnoty, jak np. dane, o których stanowi tytuł V i VI Traktatu o Unii Europejskiej, a w żadnym razie do działalności na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (łącznie z dobrą kondycją gospodarczą państwa, gdy działalność ta dotyczy spraw związanych z bezpieczeństwem państwa) oraz działalności państwa w obszarach prawa karnego,

– przez osobę fizyczną w trakcie czynności o czysto osobistym lub domowym charakterze”.

2. Dyrektywa API

4 Motywy 1, 7, 9 i 12 dyrektywy API mają następujące brzmienie:

„(1) W celu skutecznego zwalczania nielegalnej imigracji i polepszenia kontroli granicznej niezbędne jest wprowadzenie przez wszystkie państwa członkowskie przepisów ustanawiających zobowiązania przewoźników przywożących pasażerów na terytorium państw członkowskich drogą powietrzną. Ponadto, aby zapewnić niniejszemu celowi większą skuteczność, kary finansowe przewidywane obecnie przez państwa członkowskie dla przewoźników zaniedbujących wywiązywanie się ze swych zobowiązań powinny być w możliwym zakresie zharmonizowane, biorąc pod uwagę różnice w systemach i praktykach prawnych między państwami członkowskimi.

[…]

(7) Zobowiązania nałożone na przewoźników na mocy niniejszej dyrektywy uzupełniają te, ustanowione na mocy postanowień art. 26 [k]onwencji z Schengen z 1990 r. wprowadzającej w życie [u]kład z Schengen z dnia 14 czerwca 1985 r., uzupełnione dyrektywą Rady 2001/51/WE [z dnia 28 czerwca 2001 r. uzupełniającą postanowienia art. 26 konwencji wykonawczej do układu z Schengen z dnia 14 czerwca 1985 r. (Dz.U. 2001, L 187, s. 45)] – dwa rodzaje zobowiązań służące temu samemu celowi kontrolowania ruchów migracyjnych i zwalczaniu nielegalnej imigracji.

[…]

(9) W celu skutecznego zwalczania nielegalnej imigracji oraz aby zapewnić niniejszemu celowi większą skuteczność, niezbędne jest, bez uszczerbku dla postanowień dyrektywy [95/46], uwzględnienie przy najbliższej okazji wszelkich innowacji technicznych, zwłaszcza w odniesieniu do integracji i wykorzystywania cech biometrycznych w informacjach, które mają zostać przekazane przez przewoźników.

[…]

(12) Dyrektywa [95/46] ma zastosowanie w odniesieniu do przetwarzania danych osobowych przez organy państw członkowskich. Niniejsze oznacza, że gdy dopuszczone będzie przetwarzanie danych osobowych przekazanych do przeprowadzania kontroli granicznej również do celów wykorzystania ich jako dowodu w postępowaniu mającym na celu stosowanie przepisów ustawowych i wykonawczych dotyczących wjazdu i imigracji, zawierających ich przepisy dotyczące ochrony porządku publicznego (porządek publiczny) i krajowego bezpieczeństwa, jakiekolwiek dalsze przetwarzanie niezgodne z tymi celami jest sprzeczne z zasadą określoną w art. 6 ust. 1 lit. b) dyrektywy [95/46]. Państwa członkowskie powinny zapewnić system sankcji mających zastosowanie w przypadku wykorzystania niezgodnego z celem obecnej dyrektywy”.

5 Artykuł 1 dyrektywy API, zatytułowany „Cel”, przewiduje:

„Niniejsza dyrektywa ma na celu zwalczanie nielegalnej imigracji i ulepszenie kontroli granicznej w drodze przesyłania z wyprzedzeniem danych pasażerów przez przewoźników właściwym krajowym organom”.

6 Artykuł 2 tej dyrektywy, zatytułowany „Definicje”, stanowi:

„Do celów niniejszej dyrektywy:

a) »przewoźnik« oznacza każdą osobę fizyczną lub prawną, która zajmuje się zapewnianiem transportu pasażerskiego drogą powietrzną;

b) »granice zewnętrzne« oznaczają granice zewnętrzne państw członkowskich z państwami trzecimi;

c) »kontrola graniczna« oznacza kontrolę przeprowadzoną na granicy wyłącznie w odpowiedzi na zamiar przekroczenia tej granicy, bez względu na pozostałe aspekty;

d) »przejście graniczne« oznacza jakikolwiek punkt graniczny, autoryzowany przez właściwe organy do przekraczania granic zewnętrznych;

e) »dane osobowe«, »przetwarzanie danych osobowych« i »system archiwizacji danych osobowych« mają znaczenie nadane na mocy art. 2 dyrektywy [95/46]”.

7 Artykuł 3 wspomnianej dyrektywy, zatytułowany „Przesyłanie danych”, stanowi w ust. 1 i 2:

„1. Państwa członkowskie podejmują niezbędne kroki do ustanowienia zobowiązania dla przewoźników do przesyłania na wniosek organów odpowiedzialnych za przeprowadzanie kontroli osób na granicach zewnętrznych, przed końcem kontroli, informacji dotyczących pasażerów, których będą wprowadzać przez autoryzowane przejścia graniczne, przez które te osoby wchodzą na terytorium państwa członkowskiego.

2. Informacje określone powyżej zawierają:

– numer i rodzaj wykorzystanego dokumentu podróży,

– obywatelstwo,

– pełne imię i nazwisko,

– data urodzenia,

– przejście graniczne wejścia na terytorium państw członkowskich,

– kod transportu,

– czas wylotu i przylotu tego transportu,

– całkowita liczba pasażerów tego transportu,

– punkt początkowy załadowania”.

8 Artykuł 6 dyrektywy API, zatytułowany „Przetwarzanie danych”, stanowi:

„1. Dane osobowe określone w art. 3 ust. 1 są przekazywane do organów odpowiedzialnych za przeprowadzanie kontroli osób na granicach zewnętrznych, przez które te osoby wchodzą na terytorium państwa członkowskiego, aby wzmocnić skuteczność takich kontroli w celu bardziej skutecznego zwalczania nielegalnej imigracji.

Państwa członkowskie zapewniają, że te dane są zbierane przez przewoźników i przesyłane elektronicznie lub, w przypadku błędu, innym odpowiednim środkiem organom odpowiedzialnym za przeprowadzanie kontroli granicznej na autoryzowanym przejściu granicznym, przez które pasażerowie wchodzą na terytorium państwa członkowskiego. Organy odpowiedzialne za przeprowadzanie kontroli osób na granicach zewnętrznych zapisują dane na pliku tymczasowym.

Po wejściu pasażerów organy te kasują dane, w ciągu 24 godzin od momentu przesłania, chyba że dane są później potrzebne do celów wypełnienia funkcji statutowych organów odpowiedzialnych za przeprowadzanie kontroli osób na granicach zewnętrznych, zgodnie z prawem krajowym i uwzględniając przepisy dotyczące ochrony danych na mocy dyrektywy [95/46].

Państwa członkowskie podejmują niezbędne środki, aby zobowiązać przewoźników do usunięcia, w ciągu 24 godzin od dotarcia środków transportu, na podstawie art. 3 ust. 1, danych osobowych, które zgromadzili i przesłali organom granicznym do celów niniejszej dyrektywy.

Zgodnie z ich prawem krajowym i uwzględniając przepisy dotyczące ochrony danych na mocy dyrektywy [95/46], państwa członkowskie mogą również wykorzystać dane osobowe określone w art. 3 ust. 1 do celów wykonania prawa.

2. Państwa członkowskie podejmują niezbędne środki, aby zobowiązać przewoźników do powiadomienia pasażerów, zgodnie z przepisami ustanowionymi w dyrektywie [95/46]. Niniejsze [zobowiązanie] zawiera również informacje określone w art. 10 lit. c) oraz art. 11 ust. 1 lit. c) dyrektywy [95/46]”.

3. Dyrektywa 2010/65

9 Dyrektywa 2010/65 została uchylona na podstawie art. 25 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1239 z dnia 20 czerwca 2019 r. ustanawiającego europejski system morskich pojedynczych punktów kontaktowych i uchylającego dyrektywę 2010/65/UE (Dz.U. 2019, L 198, s. 64), ze skutkiem od dnia 15 sierpnia 2025 r.

10 Motyw 2 tej dyrektywy stanowi:

„Aby ułatwić transport morski i zmniejszyć obciążenia administracyjne przedsiębiorstw żeglugowych, należy w jak największym stopniu uprościć i zharmonizować formalności sprawozdawcze wymagane przez akty prawne Unii i przez państwa członkowskie […]”.

11 Artykuł 1 wspomnianej dyrektywy, zatytułowany „Przedmiot i zakres stosowania”, przewiduje w ust. 1 i 2:

„1. Niniejsza dyrektywa ma na celu uproszczenie i zharmonizowanie procedur administracyjnych stosowanych w transporcie morskim poprzez upowszechnienie elektronicznej transmisji informacji i usprawnienie formalności sprawozdawczych.

2. Niniejsza dyrektywa ma zastosowanie do formalności sprawozdawczych mających zastosowanie w transporcie morskim w odniesieniu do statków wchodzących do portów lub wychodzących z portów znajdujących się w państwach członkowskich”.

12 Zgodnie z art. 8 tej samej dyrektywy, zatytułowanym „Poufność”:

„1. Zgodnie z mającymi zastosowanie aktami prawnymi Unii lub prawodawstwem krajowym państwa członkowskie przyjmują niezbędne środki w celu zapewnienia poufności handlowych i innych poufnych informacji wymienianych zgodnie z niniejszą dyrektywą.

2. Państwa członkowskie dbają w szczególności o ochronę danych handlowych zebranych zgodnie z niniejszą dyrektywą. Co do danych osobowych – państwa członkowskie zapewniają ich zgodność z dyrektywą [95/46]. Instytucje i organy Unii [Europejskiej] zapewniają ich zgodność z rozporządzeniem (WE) nr 45/2001 [Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. 2001, L 8, s. 1)]”.

4. RODO

13 Motyw 19 RODO stanowi:

„Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy w ramach zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych, lub wykonywania kar, w tym w celu ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, oraz swobodny przepływ takich danych podlegają szczególnemu aktowi prawnemu Unii. Niniejsze rozporządzenie nie powinno zatem mieć zastosowania do czynności przetwarzania w tych celach. Jeżeli jednak dane osobowe przetwarzane przez organy publiczne na mocy niniejszego rozporządzenia są wykorzystywane do tych celów, dane te powinny podlegać szczególnemu aktowi prawnemu Unii, mianowicie dyrektywie 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 (Dz.U. 2016, L 119, s. 89)]. Państwa członkowskie mogą powierzyć właściwym organom w rozumieniu dyrektywy [2016/680] zadania – które niekoniecznie służą zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych, lub też wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom – tak by przetwarzanie danych osobowych do tych innych celów, o ile objęte jest zakresem prawa Unii, wchodziło w zakres zastosowania niniejszego rozporządzenia.

[…]”.

14 Artykuł 2 tego rozporządzenia, zatytułowany „Materialny zakres stosowania”, stanowi w ust. 1 i 2:

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

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

a) w ramach działalności nieobjętej zakresem prawa Unii;

b) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE;

[…]

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”.

15 Artykuł 4 wspomnianego rozporządzenia, zatytułowany „Definicje”, stanowi:

„Na użytek niniejszego rozporządzenia stosuje się następujące definicje:

1) »dane osobowe« oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej […];

2) »przetwarzanie« oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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;

[…]”.

16 Artykuł 23 RODO, zatytułowany „Ograniczenia”, stanowi:

„1. Prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12–22 i w art. 34, a także w art. 5 – o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22 – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym:

a) bezpieczeństwu narodowemu;

b) obronie;

c) bezpieczeństwu publicznemu;

d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom;

[…]

h) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a)–e) oraz g);

2. W szczególności akt prawny, o którym mowa w ust. 1, musi zawierać szczegółowe przepisy przynajmniej – w stosownym przypadku – o:

a) celach przetwarzania lub kategorii przetwarzania;

b) kategoriach danych osobowych;

c) zakresie wprowadzonych ograniczeń;

d) zabezpieczeniach zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu;

e) określeniu administratora lub kategorii administratorów;

f) okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania;

g) ryzykach naruszenia praw lub wolności osoby, której dane dotyczą; oraz

h) prawie osób, których dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia”.

17 Artykuł 94 tego rozporządzenia, zatytułowany „Uchylenie dyrektywy [95/46]” stanowi, co następuje:

„1. Dyrektywa [95/46] zostaje uchylona ze skutkiem od dnia 25 maja 2018 r.

2. Odesłania do uchylonej dyrektywy należy traktować jako odesłania do niniejszego rozporządzenia. Odniesienia do Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych ustanowionej w art. 29 dyrektywy [95/46] należy odczytywać jako odniesienia do Europejskiej Rady Ochrony Danych ustanowionej w niniejszym rozporządzeniu”.

5. Dyrektywa 2016/680

18 Dyrektywa 2016/680 uchyliła i zastąpiła, na mocy jej art. 59, ze skutkiem od dnia 6 maja 2018 r. decyzję ramową Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz.U. 2008, L 350, s. 60).

19 Zgodnie z motywami 9–11 dyrektywy 2016/680:

„(9) Na tej podstawie [RODO] ustanawia ogólne przepisy mające chronić osoby fizyczne w związku z przetwarzaniem danych osobowych oraz zapewnić swobodny przepływ danych osobowych w Unii.

(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 [RODO]. [RODO] 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. Przykładowo do celów postępowania przygotowawczego, wykrywania lub ścigania czynów zabronionych określone instytucje finansowe zatrzymują przetwarzane przez siebie dane osobowe i udostępniają takie dane osobowe tylko właściwym organom krajowym w konkretnych sytuacjach i w zgodzie z prawem państwa członkowskiego. Organ lub podmiot, który w imieniu takich organów przetwarza dane osobowe w ramach niniejszej dyrektywy, powinien podlegać umowie lub innemu aktowi prawnemu oraz przepisom mającym zgodnie z niniejszą dyrektywą zastosowanie do podmiotu przetwarzającego, podczas gdy w odniesieniu do przetwarzania danych osobowych przez podmiot przetwarzający spoza zakresu niniejszej dyrektywy zastosowanie [RODO] pozostaje niezmienione”.

20 Artykuł 1 tej dyrektywy, zatytułowany „Przedmiot i cele”, który jest tożsamy co do zasady z art. 1 decyzji ramowej 2008/977, przewiduje w ust. 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”.

21 Artykuł 3 dyrektywy, zatytułowany „Definicje”, ma następujące brzmienie:

„Na użytek niniejszej dyrektywy:

[…]

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;

[…]”.

6. Dyrektywa PNR

22 Motywy 4–12 oraz 15, 19, 20, 22, 25, 27, 28, 33, 36 i 37 dyrektywy PNR stanowią:

„(4) Dyrektywa [API] reguluje przekazywanie przez przewoźników lotniczych właściwym organom krajowym danych pasażera przekazanych przed podróżą (zwanych dalej »danymi API«) w celu poprawy kontroli granicznej i zwalczania nielegalnej imigracji.

(5) Celem niniejszej dyrektywy jest, między innymi, zapewnienie bezpieczeństwa ogólnego, ochrona życia i bezpieczeństwa osób oraz stworzenie ram prawnych służących ochronie danych PNR w związku z ich przetwarzaniem przez właściwe organy.

(6) Skuteczne wykorzystywanie danych PNR, między innymi poprzez porównanie danych PNR z danymi zawartymi w różnych bazach danych poszukiwanych osób i przedmiotów, jest niezbędne do zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, a tym samym do zwiększania bezpieczeństwa wewnętrznego, do zebrania dowodów a – w odpowiednich przypadkach – do wykrycia współsprawców przestępstw i rozpracowania siatek przestępczych.

(7) Sprawdzenie danych PNR umożliwia identyfikację osób, które przed dokonaniem takiego sprawdzenia nie były podejrzewane o udział w przestępstwach terrorystycznych lub w poważnej przestępczości i które powinny być poddane dalszemu sprawdzeniu przez właściwe organy. Dzięki wykorzystywaniu danych PNR można reagować na zagrożenie przestępstwami terrorystycznymi i poważną przestępczością z innej perspektywy niż w przypadku przetwarzania innych kategorii danych osobowych. Jednakże, aby ograniczyć

przetwarzanie danych PNR do niezbędnego minimum, ustalanie i stosowanie kryteriów dokonywania sprawdzeń należy ograniczyć do przestępstw terrorystycznych i poważnej przestępczości, w przypadku których stosowanie takich kryteriów jest właściwe. Ponadto kryteria dokonywania sprawdzeń powinny zostać określone w taki sposób, by ograniczyć do minimum liczbę osób niewinnych błędnie zidentyfikowanych przez system.

(8) Przewoźnicy lotniczy już zbierają i przetwarzają dane PNR swoich pasażerów do celów prowadzonej przez siebie działalności gospodarczej. Niniejsza dyrektywa nie powinna nakładać na przewoźników lotniczych żadnych obowiązków dotyczących zbierania lub zatrzymywania jakichkolwiek dodatkowych danych pochodzących od pasażerów ani nie powinna nakładać na pasażerów żadnych obowiązków dotyczących dostarczania jakichkolwiek innych danych niż te, które już są dostarczane przewoźnikom lotniczym.

(9) Niektórzy przewoźnicy lotniczy zatrzymują zebrane przez nich dane API jako część danych PNR, podczas gdy inni przewoźnicy tego nie czynią. Wykorzystywanie danych PNR wraz z danymi API stanowi wartość dodaną w zakresie pomocy państwom członkowskim w weryfikacji tożsamości osób, zwiększając tym samym przydatność wyników tych działań dla ścigania przestępczości i minimalizując ryzyko dokonywania sprawdzeń i prowadzenia postępowań przygotowawczych w stosunku do osób niewinnych. Ważne jest zatem zapewnienie, by przewoźnicy lotniczy, którzy zbierają dane API, przekazywali je bez względu na to, czy środki techniczne, za pomocą których zatrzymują dane API, są takie same jak w przypadku innych danych PNR.

(10) W celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania istotne jest, by wszystkie państwa członkowskie ustanowiły przepisy nakładające na przewoźników lotniczych obsługujących loty pozaunijne obowiązek przekazywania zebranych danych PNR, w tym danych API. Państwa członkowskie powinny mieć również możliwość rozszerzenia tego obowiązku na przewoźników lotniczych obsługujących loty wewnątrzunijne. Przepisy te nie powinny naruszać dyrektywy [API].

(11) Przetwarzanie danych osobowych powinno być proporcjonalne do szczególnych celów dotyczących bezpieczeństwa, którym służy niniejsza dyrektywa.

(12) Definicja przestępstw terrorystycznych przyjęta na potrzeby niniejszej dyrektywy powinna być taka sama jak definicja w decyzji ramowej Rady 2002/475/WSiSW [z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu (Dz.U. 2002, L 164, s. 3)]. Definicja poważnej przestępczości powinna obejmować rodzaje przestępstw wymienione w załączniku II do niniejszej dyrektywy.

[…]

(15) Wykaz danych PNR otrzymywany przez [jednostkę do spraw informacji o pasażerach (JIP)] należy sporządzać w taki sposób, by czynił on zadość zarówno uzasadnionym potrzebom organów publicznych w związku z zapobieganiem przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywaniem, prowadzeniem postępowań przygotowawczych w ich sprawie i ich ściganiem, przyczyniając się tym samym do poprawy bezpieczeństwa wewnętrznego w Unii, jak również ochronie praw podstawowych, w szczególności prawa do prywatności i ochrony danych osobowych. W tym celu należy stosować wysokie standardy zgodnie z [kartą], Konwencją o ochronie

osób w związku z automatycznym przetwarzaniem danych osobowych (zwaną dalej »konwencją nr 108«) i [europejską] Konwencją o ochronie praw człowieka i podstawowych wolności [podpisaną w Rzymie dnia 4 listopada 1950 r. (EKPC)]. Wykaz taki nie powinien opierać się na rasie ani pochodzeniu etnicznym, na religii ani przekonaniach, na poglądach politycznych ani jakichkolwiek innych poglądach, na przynależności do związków zawodowych, stanie zdrowia, życiu seksualnym ani orientacji seksualnej danej osoby. Dane PNR powinny zawierać wyłącznie informacje dotyczące rezerwacji i tras podróży danego pasażera, które umożliwią właściwym organom identyfikację pasażerów lotniczych stanowiących zagrożenie dla bezpieczeństwa wewnętrznego.

[…]

(19) Każde państwo członkowskie powinno odpowiadać za ocenę potencjalnych zagrożeń związanych z przestępstwami terrorystycznymi i poważną przestępczością.

(20) Uwzględniając w pełni prawo do ochrony danych osobowych oraz prawo do niedyskryminacji, nie można podejmować wyłącznie na podstawie automatycznego przetwarzania danych PNR żadnych decyzji, które miałyby negatywne skutki prawne dla danej osoby lub znacząco wpływałyby na jej sytuację. Ponadto, mając na uwadze art. 8 i 21 [karty], żadna taka decyzja nie powinna nikogo dyskryminować ze względu na płeć, rasę, kolor skóry, pochodzenie etniczne lub społeczne, cechy genetyczne, język, religię lub przekonania, poglądy polityczne lub wszelkie inne poglądy, przynależność do mniejszości narodowej, majątek, urodzenie, niepełnosprawność, wiek lub orientację seksualną. Komisja [Europejska] powinna również uwzględnić te zasady, dokonując przeglądu stosowania niniejszej dyrektywy.

[…]

(22) Uwzględniając w pełni zasady przedstawione w najnowszym orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej dotyczącym przedmiotowej kwestii, przy stosowaniu niniejszej dyrektywy należy zapewnić pełne poszanowanie praw podstawowych, prawa do prywatności i zasady proporcjonalności. Należy również zapewnić faktyczną zgodność z celami, jakimi są konieczność i proporcjonalność, w celu realizacji interesu publicznego uznanego przez Unię oraz potrzeby zapewnienia ochrony praw i wolności innych osób w walce z przestępstwami terrorystycznymi i poważną przestępczością. Stosowanie niniejszej dyrektywy powinno być należycie uzasadnione; należy wprowadzić niezbędne gwarancje, aby zapewnić zgodność z prawem przechowywania, analizowania, przekazywania lub wykorzystywania danych PNR.

[…]

(25) Dane PNR powinny być zatrzymywane na okres niezbędny i proporcjonalny do celów, jakimi są zapobieganie przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywanie, prowadzenie postępowań przygotowawczych w ich sprawie i ich ściganie. Ze względu na charakter danych i ich wykorzystanie, niezbędne jest zatrzymywanie danych PNR przez okres wystarczająco długi, aby możliwe było ich analizowanie i wykorzystywanie w postępowaniach przygotowawczych. Po upływie początkowego okresu zatrzymania dane PNR powinny zostać poddane depersonalizacji poprzez maskowanie elementów danych, aby zapobiec ich nieproporcjonalnemu wykorzystywaniu.

Po upływie początkowego okresu zatrzymania dostęp do pełnych danych PNR, które umożliwiają bezpośrednie zidentyfikowanie osoby, której dane dotyczą, powinien być możliwy wyłącznie po spełnieniu bardzo restrykcyjnych i ściśle określonych warunków, aby zapewnić jak najwyższy poziom ochrony danych.

[…]

(27) Przetwarzanie danych PNR w każdym państwie członkowskim przez JIP oraz przez właściwe organy powinno podlegać standardom ochrony danych osobowych wynikającym z prawa krajowego, zgodnym z decyzją ramową [2008/977] oraz ze szczególnymi wymogami w zakresie ochrony danych określonymi w niniejszej dyrektywie. Odesłania do decyzji ramowej [2008/977] należy rozumieć jako odesłania do przepisów obecnie obowiązujących, jak i do przepisów, które je zastąpią.

(28) Mając na uwadze prawo do ochrony danych osobowych, prawa osób, których dane dotyczą, odnoszące się do przetwarzania ich danych PNR, takie jak prawo dostępu do tych danych, ich poprawiania, usunięcia i ograniczania oraz prawo do odszkodowania i prawo do sądowych środków ochrony prawnej, powinny być zgodne zarówno z decyzją ramową [2008/977], jak również z wysokim poziomem ochrony przewidzianym w [karcie] i [EKPC].

[…]

(33) Niniejsza dyrektywa nie wpływa na możliwość ustanowienia przez państwa członkowskie, na mocy przepisów krajowych, systemu zbierania i przetwarzania danych PNR przekazywanych przez podmioty gospodarcze niebędące przewoźnikami, takie jak biura podróży i organizatorzy wycieczek świadczący usługi związane z podróżowaniem, w tym rezerwację lotów, na potrzeby których zbierają i przetwarzają dane PNR, lub przez dostawców usług transportowych innych niż dostawcy określeni w niniejszej dyrektywie, pod warunkiem że takie przepisy krajowe są zgodne z prawem Unii.

[…]

(36) Niniejsza dyrektywa jest zgodna z prawami podstawowymi i zasadami uznanymi w [karcie], w szczególności z prawem do ochrony danych osobowych, prawem do prywatności i prawem do niedyskryminacji, chronionymi na mocy art. 8, 7 i 21 [karty]; powinna zatem zostać odpowiednio wdrożona. Niniejsza dyrektywa jest zgodna z zasadami ochrony danych, a jej przepisy pozostają w zgodności z decyzją ramową [2008/977]. Ponadto, aby uczynić zadość zasadzie proporcjonalności, w odniesieniu do niektórych kwestii niniejsza dyrektywa przewiduje bardziej rygorystyczne przepisy dotyczące ochrony danych niż decyzja ramowa [2008/977].

(37) Zakres stosowania niniejszej dyrektywy jest maksymalnie ograniczony, ponieważ: przewiduje ona zatrzymanie danych PNR w JIP przez okres nieprzekraczający pięciu lat, po upływie którego dane powinny zostać usunięte; przewiduje poddanie danych depersonalizacji poprzez maskowanie elementów danych po upływie początkowego okresu sześciu miesięcy; oraz zakazuje zbierania i wykorzystywania danych szczególnie chronionych. W celu zapewnienia skuteczności i wysokiego poziomu ochrony danych państwa członkowskie są zobowiązane do zapewnienia, by za doradztwo i monitorowanie w zakresie sposobu przetwarzania danych PNR odpowiadał niezależny krajowy organ nadzorczy oraz, w szczególności, inspektor ochrony danych. Wszelkie operacje

przetwarzania danych PNR powinny być ewidencjonowane lub dokumentowane na potrzeby weryfikacji zgodności z prawem tych operacji, monitorowania własnej działalności oraz zapewnienia odpowiedniej integralności danych i bezpiecznego przetwarzania. Ponadto państwa członkowskie powinny zapewnić, by pasażerowie byli informowani w sposób jasny i dokładny o zbieraniu danych PNR i o przysługujących im prawach".

23 Artykuł 1 dyrektywy PNR, zatytułowany „Przedmiot i zakres stosowania", stanowi:

„1. Niniejsza dyrektywa określa:

a) przekazywanie przez przewoźników lotniczych danych dotyczących przelotu pasażera [danymi PNR], które dotyczą pasażerów lotów pozaunijnych;

b) przetwarzanie danych, o których mowa w lit. a), w tym ich zbieranie, wykorzystywanie i zatrzymywanie przez państwa członkowskie oraz wymianę tych danych między państwami członkowskimi.

2. Dane PNR zebrane zgodnie z niniejszą dyrektywą mogą być przetwarzane wyłącznie w celach zapobiegania przestępstwom terrorystycznym i poważnej przestępczości oraz ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, jak przewidziano w art. 6 ust. 2 lit. a), b) i c)".

24 Artykuł 2 dyrektywy, zatytułowany „Stosowanie niniejszej dyrektywy do lotów wewnątrzunijnych", stanowi, co następuje:

„1. Jeżeli państwo członkowskie podejmie decyzję o stosowaniu niniejszej dyrektywy do lotów wewnątrzunijnych, powiadamia o tym Komisję na piśmie. Państwo członkowskie może złożyć lub cofnąć takie powiadomienie w każdym czasie. Komisja publikuje takie powiadomienia oraz wszelkie ich cofnięcia w *Dzienniku Urzędowym Unii Europejskiej*.

2. Po złożeniu powiadomienia, o którym mowa w ust. 1, wszystkie przepisy niniejszej dyrektywy stosuje się do lotów wewnątrzunijnych, tak jakby były one lotami pozaunijnymi, oraz do danych PNR dotyczących lotów wewnątrzunijnych, tak jakby były one danymi PNR dotyczącymi lotów pozaunijnych.

3. Państwo członkowskie może podjąć decyzję o stosowaniu niniejszej dyrektywy wyłącznie do wybranych lotów wewnątrzunijnych. Podejmując taką decyzję, państwo członkowskie dokonuje wyboru lotów, które uważa za niezbędne z punktu widzenia realizacji celów niniejszej dyrektywy. Państwo członkowskie może w każdym czasie podjąć decyzję o zmianie wyboru lotów wewnątrzunijnych".

25 Artykuł 3 dyrektywy, zatytułowany „Definicje", stanowi:

„Na potrzeby niniejszej dyrektywy stosuje się następujące definicje:

1) »przewoźnik lotniczy« oznacza przedsiębiorstwo transportu lotniczego posiadające ważną koncesję lub równorzędne zezwolenie uprawniające do lotniczego przewozu pasażerów;

2) »lot pozaunijny« oznacza regularny lub nieregularny lot, obsługiwany przez przewoźnika lotniczego, odbywający się z państwa trzeciego, z zaplanowanym lądowaniem na terytorium państwa członkowskiego albo odbywający się z terytorium państwa członkowskiego, z zaplanowanym lądowaniem w państwie trzecim, w tym – w obu przypadkach – loty z postojami na terytorium państw członkowskich lub państw trzecich;

3) »lot wewnątrzunijny« oznacza regularny lub nieregularny lot, obsługiwany przez przewoźnika lotniczego, odbywający się z terytorium państwa członkowskiego, z zaplanowanym lądowaniem na terytorium co najmniej jednego państwa członkowskiego, bez postojów na terytorium państwa trzeciego;

4) »pasażer« oznacza osobę, w tym pasażera transferowego lub tranzytowego, z wyjątkiem członków załogi, która jest przewożona lub ma być przewieziona na pokładzie samolotu za zgodą przewoźnika lotniczego wyrażoną w formie wpisu tej osoby na listę pasażerów;

5) »dane dotyczące przelotu pasażera« lub »dane PNR« oznaczają zbiór danych o podróży każdego pasażera, który zawiera informacje niezbędne, aby umożliwić przetwarzanie i weryfikowanie rezerwacji przez przewoźników lotniczych obsługujących rezerwację i lot w odniesieniu do każdego przelotu zarezerwowanego przez jakąkolwiek osobę lub w jej imieniu, bez względu na to, czy zbiór ten znajduje się w systemach rezerwacji, systemach odpraw pasażerskich lub równorzędnych systemach pełniących te same funkcje;

6) »system rezerwacji« oznacza wewnętrzny system przewoźnika lotniczego, w którym zbierane są dane PNR w celu obsługi rezerwacji;

7) »metoda dostarczania« (metoda »push«) oznacza metodę polegającą na przekazywaniu przez przewoźników lotniczych danych PNR, wymienionych w załączniku I, do bazy danych organów, które się o nie zwróciły;

8) »przestępstwa terrorystyczne« oznaczają przestępstwa w rozumieniu prawa krajowego, o których mowa w art. 1–4 decyzji ramowej [2002/475];

9) »poważna przestępczość« oznacza przestępstwa wymienione w załączniku II, które na mocy prawa krajowego państwa członkowskiego podlegają karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności o maksymalnym wymiarze co najmniej trzech lat;

10) »depersonalizacja poprzez maskowanie elementów danych« oznacza uczynienie niewidocznymi dla użytkownika takich elementów danych, które mogłyby posłużyć do bezpośredniego zidentyfikowania osoby, której dane dotyczą”.

26 Artykuł 4 dyrektywy PNR, zatytułowany „Jednostka do spraw informacji o pasażerach”, stanowi w ust. 1–3:

„1. Każde państwo członkowskie ustanawia lub wyznacza organ właściwy do zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie lub ich ścigania albo dział takiego organu do pełnienia roli jednostki do spraw informacji o pasażerach [JIP].

2. JIP odpowiada za:

a) zbieranie od przewoźników lotniczych danych PNR, ich przechowywanie i przetwarzanie oraz za przekazywanie tych danych lub wyników ich przetwarzania właściwym organom, o których mowa w art. 7;

b) wymianę zarówno danych PNR, jak i wyników ich przetwarzania z JIP w innych państwach członkowskich i z Europolem zgodnie z art. 9 i 10.

3. Pracownicy JIP mogą być oddelegowani z właściwych organów. Państwa członkowskie zapewniają JIP odpowiednie zasoby umożliwiające im realizację ich zadań".

27 Artykuł 5 tej dyrektywy, zatytułowany „Inspektor ochrony danych w JIP", brzmi:

„1. JIP powołuje inspektora ochrony danych, który odpowiada za monitorowanie przetwarzania danych PNR i stosowanie odpowiednich gwarancji.

2. Państwa członkowskie udostępniają inspektorom ochrony danych środki umożliwiające im wykonywanie w sposób skuteczny i niezależny obowiązków i zadań określonych w niniejszym artykule.

3. Państwa członkowskie zapewniają osobie, której dane dotyczą, prawo do kontaktowania się z inspektorem ochrony danych, jako pojedynczym punktem kontaktowym, we wszystkich sprawach związanych z przetwarzaniem danych PNR tej osoby".

28 Artykuł 6 wspomnianej dyrektywy, zatytułowany „Przetwarzanie danych PNR", stanowi:

„1. Dane PNR przekazane przez przewoźników lotniczych są zbierane przez JIP we właściwym państwie członkowskim w sposób określony w art. 8. Jeżeli wśród danych PNR przekazanych przez przewoźników lotniczych znajdują się dane inne niż wymienione w załączniku I, JIP usuwa takie dane w sposób trwały niezwłocznie po ich otrzymaniu.

2. JIP przetwarza dane PNR wyłącznie w następujących celach:

a) dokonania sprawdzenia pasażerów przed ich planowanym przylotem do lub odlotem z państwa członkowskiego w celu identyfikacji osób, które wymagają dalszego sprawdzenia przez właściwe organy, o których mowa w art. 7, oraz – w stosownych przypadkach – przez Europol zgodnie z art. 10, ze względu na możliwość udziału takich osób w przestępstwach terrorystycznych lub w poważnej przestępczości;

b) odpowiadania, na podstawie oceny każdego indywidualnego przypadku, na należycie uzasadniony i oparty na wystarczających podstawach wniosek właściwych organów o przekazanie i przetwarzanie danych PNR w określonych przypadkach w celach zapobiegania przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, oraz o przekazanie właściwym organom, lub – w stosownych przypadkach – Europolowi, wyników takiego przetwarzania; i

c) analizowania danych PNR do celów aktualizacji lub tworzenia nowych kryteriów stosowanych przy sprawdzeniach dokonywanych na podstawie ust. 3 lit. b), w celu identyfikacji wszystkich osób, które mogą brać udział w przestępstwach terrorystycznych lub w poważnej przestępczości.

3. Dokonując sprawdzenia, o którym mowa w ust. 2 lit. a), JIP może:

a) porównywać dane PNR z bazami danych, które mają znaczenie dla zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, w tym z bazami danych o osobach lub przedmiotach poszukiwanych lub objętych wpisem, zgodnie z przepisami unijnymi, międzynarodowymi i krajowymi mającymi zastosowanie do takich baz danych; lub

b) przetwarzać dane PNR według wcześniej ustalonych kryteriów.

4. Sprawdzenie pasażerów przed ich planowym przylotem do lub odlotem z państwa członkowskiego dokonywane na podstawie ust. 3 lit. b) według wcześniej ustalonych kryteriów odbywa się w sposób niedyskryminacyjny. Te ustalone wcześniej kryteria muszą być ukierunkowane, proporcjonalne i szczegółowe. Państwa członkowskie zapewniają, by kryteria te były ustanawiane i poddawane regularnym przeglądom przez JIP we współpracy z właściwymi organami, o których mowa w art. 7. Kryteria te w żadnym przypadku nie mogą opierać się na rasie ani pochodzeniu etnicznym, na poglądach politycznych, przekonaniach religijnych lub światopoglądowych, przynależności do związków zawodowych, stanie zdrowia, życiu seksualnym ani orientacji seksualnej danej osoby.

5. Państwa członkowskie zapewniają, by każdy pozytywny wynik automatycznego przetwarzania danych PNR dokonanego zgodnie z ust. 2 lit. a) był indywidualnie oceniany w sposób niezautomatyzowany w celu ustalenia, czy właściwy organ, o którym mowa w art. 7, powinien podjąć działania zgodnie z prawem krajowym.

6. JIP w danym państwie członkowskim przekazuje do dalszego sprawdzenia dane PNR osób zidentyfikowanych zgodnie z ust. 2 lit. a) lub wyniki przetwarzania tych danych właściwym organom, o których mowa w art. 7, w tym samym państwie członkowskim. Przekazywanie to odbywa się wyłącznie na podstawie oceny każdego indywidualnego przypadku, a w przypadku automatycznego przetwarzania danych PNR – po indywidualnej ocenie przeprowadzonej w sposób niezautomatyzowany.

7. Państwa członkowskie zapewniają, by inspektor ochrony danych miał dostęp do wszystkich danych przetwarzanych przez JIP. Jeżeli inspektor ochrony danych uzna, że przetwarzanie jakichkolwiek danych było niezgodne z prawem, może przekazać sprawę do krajowego organu nadzorczego.

[…]

9. Skutki sprawdzenia pasażerów, o którym mowa w ust. 2 lit. a) niniejszego artykułu, nie naruszają prawa osób, którym przysługuje unijne prawo do swobodnego przemieszczania się, do wjazdu na terytorium danego państwa członkowskiego, zgodnie z dyrektywą [2004/38/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie prawa obywateli Unii i członków ich rodzin do swobodnego przemieszczania się i pobytu na terytorium państw członkowskich, zmieniająca rozporządzenie (EWG) nr 1612/68 i uchylająca dyrektywy

64/221/EWG, 68/360/EWG, 72/194/EWG, 73/148/EWG, 75/34/EWG, 75/35/EWG, 90/364/EWG, 90/365/EWG i 93/96/EWG (Dz.U. 2004, L 158, s. 77)]. Ponadto, jeżeli sprawdzenie jest dokonywane w odniesieniu do lotów wewnątrzunijnych pomiędzy państwami członkowskimi, do których stosuje się rozporządzenie [nr 562/2006 Parlamentu Europejskiego i Rady (WE) z dnia 15 marca 2006 r. ustanawiające wspólnotowy kodeks zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen) (Dz.U. 2006, L 105, s. 1)], skutki takiego sprawdzenia nie naruszają tego rozporządzenia".

29 Zgodnie z art. 7 dyrektywy PNR, zatytułowanym „Właściwe organy":

„1. Każde państwo członkowskie sporządza wykaz właściwych organów uprawnionych do występowania do JIP o dane PNR lub o wyniki przetwarzania tych danych lub do otrzymywania takich danych i wyników ich przetwarzania od JIP na potrzeby dalszego sprawdzenia tych informacji lub podjęcia odpowiednich czynności w celu zapobiegania przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania.

2. Organy, o których mowa w ust. 1, są organami właściwymi do zapobiegania przestępstwom terrorystycznym lub poważnym przestępstwom, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania.

[…]

4. Dane PNR oraz wyniki przetwarzania tych danych, otrzymane od JIP, mogą być poddane dalszemu przetwarzaniu przez właściwe organy państw członkowskich wyłącznie do określonych celów, jakimi są zapobieganie przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywanie, prowadzenie postępowań przygotowawczych w ich sprawie lub ich ściganie.

5. Ustęp 4 nie narusza określonych prawem krajowym uprawnień organów ścigania i organów wymiaru sprawiedliwości, w przypadku gdy w toku czynności podejmowanych w ramach ścigania przestępstw wykryte zostaną, na podstawie wyników takiego przetwarzania, inne przestępstwa lub okoliczności na nie wskazujące.

6. Właściwe organy nie podejmują żadnych decyzji, które miałyby negatywne skutki prawne dla danej osoby lub znacząco wpływałyby na jej sytuację, wyłącznie na podstawie automatycznego przetwarzania danych PNR. Takie decyzje nie mogą zostać podjęte w oparciu o rasę ani pochodzenie etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, stan zdrowia, życie seksualne ani orientację seksualną danej osoby".

30 Artykuł 8 tej dyrektywy, zatytułowany „Obowiązki przewoźników lotniczych dotyczące przekazywania danych", przewiduje w ust. 1–3:

„1. Państwa członkowskie przyjmują środki niezbędne do zapewnienia, by przewoźnicy lotniczy przekazywali, za pomocą »metody push«, dane PNR wymienione w załączniku I – w zakresie, w jakim już zbierają takie dane w ramach swojej normalnej działalności – do bazy danych JIP w państwie członkowskim, na którego terytorium nastąpi przylot lub z którego terytorium nastąpi odlot. W przypadku gdy lot odbywa się pod wspólnym kodem z udziałem jednego lub większej liczby przewoźników lotniczych, obowiązek przekazania danych PNR wszystkich pasażerów uczestniczących w locie spoczywa na przewoźniku lotniczym obsługującym lot. Jeżeli lot

pozaunijny odbywa się z jednym lub kilkoma postojami na lotniskach różnych państw członkowskich, przewoźnicy lotniczy przekazują dane PNR dotyczące wszystkich pasażerów JIP we wszystkich odpowiednich państwach członkowskich. Dotyczy to również lotów wewnątrzunijnych z jednym lub kilkoma postojami na lotniskach różnych państw członkowskich, ale wyłącznie w przypadku państw członkowskich, które zbierają dane PNR z lotów wewnątrzunijnych.

2. Jeżeli przewoźnicy lotniczy zebrali jakiekolwiek [dane API] wymienione w pkt 18 załącznika I, ale nie zatrzymują tych danych za pomocą takich samych technicznych środków jak w przypadku innych danych PNR, państwa członkowskie przyjmują środki niezbędne do zapewnienia, by przewoźnicy lotniczy przekazywali, za pomocą »metody push«, także te dane do JIP w państwie członkowskim, o którym mowa w ust. 1. W przypadku takiego przekazania stosuje się do tych danych API wszystkie przepisy niniejszej dyrektywy.

3. Przewoźnicy lotniczy przekazują dane PNR za pomocą środków elektronicznych z wykorzystaniem wspólnych protokołów i obsługiwanych formatów danych, które to protokoły i formaty zostaną określone zgodnie z procedurą sprawdzającą, o której mowa w art. 17 ust. 2, a w przypadku awarii technicznej – innymi właściwymi sposobami zapewniającymi odpowiedni poziom bezpieczeństwa danych:

a) 24 do 48 godzin przez planowym odlotem; oraz

b) niezwłocznie po zakończeniu odprawy, czyli bezpośrednio po wejściu pasażerów na pokład samolotu przygotowującego się do odlotu, kiedy to pasażerowie nie mogą już wejść na pokład ani go opuścić".

31 Zgodnie z art. 12 wspomnianej dyrektywy, zatytułowanym „Okres zatrzymania danych i depersonalizacja":

„1. Państwa członkowskie zapewniają, by dane PNR dostarczone przez przewoźników lotniczych JIP były zatrzymywane w bazie danych JIP przez okres pięciu lat od przekazania ich JIP w państwie członkowskim, na którego terytorium ma miejsce przylot lub z którego terytorium ma miejsce odlot.

2. Po upływie okresu sześciu miesięcy od przekazania danych PNR, o którym mowa w ust. 1, wszystkie dane PNR zostają poddane depersonalizacji poprzez maskowanie następujących ich elementów mogących posłużyć do bezpośredniej identyfikacji pasażera, którego dotyczą dane:

a) imię i nazwisko (imiona i nazwiska), w tym imię i nazwisko innych pasażerów wymienionych w danych PNR oraz liczba pasażerów wymienionych w danych PNR podróżujących razem;

b) adres i dane kontaktowe;

c) wszystkie informacje o formie płatności, w tym adres na fakturze, o ile zawierają one jakiekolwiek informacje mogące posłużyć do bezpośredniej identyfikacji pasażera, którego dotyczą dane PNR, lub wszelkich innych osób;

d) informacje dotyczące programów lojalnościowych;

e) ogólne uwagi, o ile zawierają one informacje mogące posłużyć do bezpośredniej identyfikacji pasażera, którego dotyczą dane PNR; oraz

f) wszelkie zebrane dane API.

3. Po upływie okresu sześciu miesięcy, o którym mowa w ust. 2, ujawnienie pełnych danych PNR jest dopuszczalne wyłącznie wtedy, gdy:

a) istnieje uzasadnienie, by uznać, że jest to niezbędne do celów określonych w art. 6 ust. 2 lit. b); oraz

b) uzyskano zgodę:
   (i) organu wymiaru sprawiedliwości; lub
   (ii) innego organu krajowego, który zgodnie z prawem krajowym jest właściwy do ustalenia, czy warunki ujawnienia zostały spełnione, z zastrzeżeniem poinformowania inspektora ochrony danych w JIP oraz dokonania przez tego inspektora ochrony danych weryfikacji ex post.

4. Państwa członkowskie zapewniają, by po upływie okresu, o którym mowa w ust. 1, dane PNR zostały usunięte w sposób trwały. Obowiązek ten nie ma wpływu na przypadki, w których określone dane PNR zostały przekazane właściwemu organowi i są wykorzystywane w konkretnej sprawie w celu zapobiegania przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie lub ich ścigania; w takim przypadku zatrzymanie takich danych przez właściwy organ regulowane jest prawem krajowym.

5. Wyniki przetwarzania, o którym mowa w art. 6 ust. 2 lit. a), są przechowywane przez JIP wyłącznie przez okres niezbędny do poinformowania o pozytywnym wyniku właściwych organów oraz – zgodnie z art. 9 ust. 1 – JIP w pozostałych państwach członkowskich. Jeżeli wynik automatycznego przetwarzania, po indywidualnej ocenie przeprowadzonej w sposób niezautomatyzowany, o której mowa w art. 6 ust. 5, okaże się negatywny, może on mimo to być przechowywany, by zapobiec przyszłym wynikom fałszywie pozytywnym, dopóki dane bazowe nie zostaną usunięte zgodnie z ust. 4 niniejszego artykułu".

32 Artykuł 13 dyrektywy PNR, zatytułowany „Ochrona danych osobowych", w ust. 1–5 stanowi:

„1. Każde państwo członkowskie zapewnia, by w odniesieniu do wszelkich operacji przetwarzania danych osobowych na podstawie niniejszej dyrektywy, każdemu pasażerowi przysługiwało prawo do ochrony jego danych osobowych, prawo dostępu do tych danych, ich poprawiania, usunięcia i ograniczania oraz prawo do odszkodowania i prawo do sądowych środków ochrony prawnej, odpowiadające prawom ustanowionym w prawie Unii i w prawie krajowym oraz w ramach wdrożenia art. 17, 18, 19 i 20 decyzji ramowej [2008/977]. Artykuły te zatem stosuje się.

2. Każde państwo członkowskie stanowi, że przepisy przyjęte w prawie krajowym w ramach wdrożenia art. 21 i 22 decyzji ramowej [2008/977] w odniesieniu do poufności przetwarzania oraz bezpieczeństwa danych stosuje się także do wszelkich operacji przetwarzania danych osobowych na podstawie niniejszej dyrektywy.

3. Niniejsza dyrektywa nie ma wpływu na możliwość stosowania dyrektywy Parlamentu Europejskiego i Rady [95/46] do przetwarzania danych osobowych przez przewoźników

lotniczych, w szczególności w zakresie ich obowiązku podjęcia odpowiednich środków technicznych i organizacyjnych w celu ochrony bezpieczeństwa i poufności danych osobowych.

4. Państwa członkowskie zakazują przetwarzania danych PNR ujawniających rasę lub pochodzenie etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, stan zdrowia, życie seksualne lub orientację seksualną danej osoby. W przypadku otrzymania przez JIP danych PNR ujawniających takie informacje, dane takie są niezwłocznie usuwane.

5. Państwa członkowskie zapewniają, by JIP prowadziły dokumentację dotyczącą wszystkich systemów i procedur przetwarzania, za które są odpowiedzialne. Dokumentacja ta zawiera co najmniej:

a) nazwę i dane kontaktowe organizacji oraz imiona i nazwiska i dane kontaktowe personelu JIP, którym powierzono przetwarzanie danych PNR wraz z poszczególnymi poziomami prawa dostępu;

b) wnioski złożone przez właściwe organy i JIP w innych państwach członkowskich;

c) wszystkie wnioski o przekazanie i przypadki przekazania danych PNR do państwa trzeciego.

JIP na wniosek krajowego organu nadzorczego udostępnia mu całą dokumentację".

33 Zgodnie z art. 15 tej dyrektywy, zatytułowanym „Krajowy organ nadzorczy":

„1. Każde państwo członkowskie stanowi, że krajowy organ nadzorczy, o którym mowa w art. 25 decyzji ramowej [2008/977], odpowiada za doradztwo i monitorowanie w zakresie stosowania na jego terytorium przepisów przyjętych przez państwa członkowskie na podstawie niniejszej dyrektywy. [Artykuł] 25 decyzji ramowej [2008/977] stosuje się.

2. Te krajowe organy nadzorcze realizują swoje zadania, o których mowa w ust. 1, w celu ochrony praw podstawowych w związku z przetwarzaniem danych osobowych.

3. Każdy krajowy organ nadzorczy:

a) rozpatruje skargi złożone przez osoby, których dane dotyczą, bada daną sprawę oraz w rozsądnym terminie informuje osoby, których dane dotyczą, o postępach i wyniku rozpatrzenia ich skarg;

b) sprawdza zgodność z prawem przetwarzania danych, prowadzi postępowania, inspekcje i audyty zgodnie z prawem krajowym, z własnej inicjatywy lub na podstawie skargi, o której mowa w lit. a).

4. Każdy krajowy organ nadzorczy doradza, na wniosek, osobie, której dane dotyczą, w sprawie wykonywania praw określonych w przepisach przyjętych na podstawie niniejszej dyrektywy".

34 Artykuł 19 wspomnianej dyrektywy, zatytułowany „Przegląd", przewiduje:

„1. Na podstawie informacji dostarczonych przez państwa członkowskie, w tym informacji statystycznych, o których mowa w art. 20 ust. 2, Komisja w terminie do dnia 25 maja 2020 r.

dokonuje przeglądu wszystkich elementów niniejszej dyrektywy oraz przedkłada i przedstawia sprawozdanie Parlamentowi Europejskiemu i Radzie [Unii Europejskiej].

2. Dokonując tego przeglądu, Komisja zwraca szczególną uwagę na:

a) przestrzeganie mających zastosowanie standardów ochrony danych osobowych;

b) konieczność i proporcjonalność zbierania i przetwarzania danych PNR w odniesieniu do każdego celu określonego w niniejszej dyrektywie;

c) długość okresu zatrzymania danych;

d) skuteczność wymiany informacji między państwami członkowskimi; oraz

e) jakość sprawdzeń, w tym w odniesieniu do informacji statystycznych zgromadzonych na podstawie art. 20.

3. Sprawozdanie, o którym mowa w ust. 1, zawiera również przegląd konieczności, proporcjonalności i skuteczności włączenia do zakresu stosowania niniejszej dyrektywy obowiązkowego zbierania i przekazywania danych PNR w odniesieniu do wszystkich lub wybranych lotów wewnątrzunijnych. Komisja uwzględnia doświadczenia państw członkowskich, zwłaszcza tych, które stosują niniejszą dyrektywę do lotów wewnątrzunijnych zgodnie z art. 2. W sprawozdaniu rozważa się także konieczność włączenia do zakresu stosowania niniejszej dyrektywy podmiotów gospodarczych niebędących przewoźnikami, takich jak biura podróży i organizatorzy wycieczek świadczący usługi turystyczne związane z podróżowaniem, w tym rezerwację lotów.

4. W stosownym przypadku, w świetle przeglądu, dokonanego na podstawie niniejszego artykułu, Komisja przedkłada Parlamentowi Europejskiemu i Radzie wniosek ustawodawczy mający na celu zmianę niniejszej dyrektywy”.

35 Artykuł 21 tej samej dyrektywy, zatytułowany „Stosunek do innych instrumentów prawnych”, stanowi w ust. 2:

„Niniejsza dyrektywa nie ma wpływu na możliwość stosowania dyrektywy [95/46] do przetwarzania danych osobowych przez przewoźników lotniczych”.

36 Załącznik I do dyrektywy PNR, zatytułowany „Dane dotyczące przelotu pasażera zbierane przez przewoźników lotniczych” ma następujące brzmienie:

„1. Kod identyfikacyjny danych PNR

2. Data rezerwacji/wystawienia biletu

3. Data(-y) planowanej podróży

4. Imię i nazwisko (imiona i nazwiska)

5. Adres i dane kontaktowe (numer telefonu, adres e-mail)

6. Wszystkie informacje o formie płatności, w tym adres na fakturze

7. Kompletna trasa podróży dla konkretnych danych PNR

8. Informacje o programach lojalnościowych

9. Biuro podróży/agencja turystyczna

10. Dane o statusie podróży pasażera, w tym potwierdzenia, stan odprawy biletowo-bagażowej, dane typu: pasażer nie stawił się lub pasażer nabył bilet w czasie odprawy bez wcześniejszej rezerwacji

11. Informacje o podzieleniu/rozdzieleniu danych PNR

12. Uwagi ogólne (w tym wszelkie dostępne informacje o osobach małoletnich bez opieki w wieku poniżej 18 lat, takie jak: imię i nazwisko, płeć, wiek, języki, którymi włada, imię i nazwisko oraz dane kontaktowe opiekuna w momencie odlotu i rodzaj więzi łączącej go z osobą małoletnią, imię i nazwisko oraz dane kontaktowe opiekuna w momencie lądowania i rodzaj więzi łączącej go z osobą małoletnią, przedstawiciel obecny przy odlocie i przylocie)

13. Informacje o wystawieniu biletu, w tym numer biletu, data wystawienia biletu i bilety w jedną stronę, informacja o automatycznie skalkulowanej taryfie

14. Numer miejsca na pokładzie i inne informacje o miejscu

15. Informacje o wspólnej obsłudze połączeń

16. Wszystkie informacje o bagażu

17. Liczba oraz imiona i nazwiska innych podróżnych wymienionych w PNR

18. Wszelkie zebrane dane pasażera przekazane przed podróżą (dane API) (w tym rodzaj, numer, kraj wydania i data ważności dokumentu tożsamości, obywatelstwo, nazwisko, imię, płeć, data urodzenia, linia lotnicza, numer lotu, data odlotu, data przylotu, port lotniczy odlotu, port lotniczy przylotu, godzina odlotu i godzina przylotu)

19. Wszystkie dotychczasowe zmiany danych PNR wymienionych w pkt 1–18”.

37 Z kolei załącznik II do dyrektywy, zatytułowany „Wykaz przestępstw, o których mowa w art. 3 pkt 9”, ma następujące brzmienie:

„1. Udział w organizacji przestępczej

2. Handel ludźmi

3. Wykorzystywanie seksualne dzieci i pornografia dziecięca

4. Nielegalny handel narkotykami i substancjami psychotropowymi

5. Nielegalny handel bronią, amunicją i materiałami wybuchowymi

6. Korupcja

7. Oszustwo, w tym oszustwo przeciwko interesom finansowym Unii

8. Pranie dochodów z przestępstwa i fałszowanie pieniędzy, w tym euro

9. Przestępczość komputerowa i cyberprzestępczość

10. Przestępstwa przeciwko środowisku, w tym nielegalny handel zagrożonymi gatunkami zwierząt oraz zagrożonymi gatunkami i odmianami roślin

11. Ułatwianie bezprawnego wjazdu i pobytu

12. Zabójstwo, spowodowanie ciężkiego uszczerbku na zdrowiu

13. Nielegalny obrót organami i tkankami ludzkimi

14. Uprowadzenie, bezprawne pozbawienie wolności i wzięcie zakładników

15. Kradzież zorganizowana i rozbój przy użyciu broni

16. Nielegalny handel dobrami kultury, w tym antykami i dziełami sztuki

17. Podrabianie i piractwo produktów

18. Fałszowanie dokumentów urzędowych i handel nimi

19. Nielegalny handel substancjami hormonalnymi i innymi środkami pobudzającymi wzrost

20. Nielegalny handel materiałami jądrowymi lub promieniotwórczymi

21. Zgwałcenie

22. Przestępstwa podlegające jurysdykcji Międzynarodowego Trybunału Karnego

23. Bezprawne zawładnięcie statkiem powietrznym lub statkiem

24. Sabotaż

25. Handel skradzionymi pojazdami

26. Szpiegostwo przemysłowe”.

7. Decyzja ramowa 2002/475

38 Artykuł 1 decyzji ramowej 2002/475 definiował pojęcie „przestępstwa terrorystycznego”, formułując listę zamierzonych czynów wskazanych w lit. od a) do i) tego przepisu, popełnionych w celu „poważnego zastraszenia ludności”, „bezprawnego zmuszenia rządu lub organizacji międzynarodowej do podjęcia lub zaniechania działania” lub „poważnej destabilizacji lub

zniszczenia podstawowych politycznych, konstytucyjnych, gospodarczych lub społecznych struktur kraju lub organizacji międzynarodowej". Artykuły 2 i 3 przedmiotowej decyzji ramowej definiowały z kolei pojęcia „przestępstwa dotyczącego grupy terrorystycznej" oraz „przestępstwa związanego z działalnością terrorystyczną". Artykuł 4 decyzji ramowej regulował zaś karalność pomocnictwa lub współsprawstwa w popełnieniu tych przestępstw, podżegania do ich popełnienia, a także usiłowania ich popełnienia.

39 Decyzja ramowa 2002/475 została uchylona dyrektywą Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępującą decyzję ramową Rady 2002/475/WSiSW oraz zmieniającą decyzję Rady 2005/671/WSiSW (Dz.U. 2017, L 88, s. 6), której art. 3–14 zawierają analogiczne definicje.

B. Prawo belgijskie

1. Konstytucja

40 Artykuł 22 konstytucji stanowi:

„Każdy człowiek ma prawo do poszanowania jego życia prywatnego i rodzinnego, z wyjątkiem przypadków i warunków określonych w ustawie.

Ustawa, dekret lub norma wskazana w art. 134 gwarantują ochronę tego prawa".

2. Ustawa z dnia 25 grudnia 2016 r.

41 Artykuł 2 loi du 25 décembre 2016, relative au traitement des données des passagers (ustawy z dnia 25 grudnia 2016 r. o przetwarzaniu danych pasażerów, *Moniteur belge* z dnia 25 stycznia 2017 r., s. 12905, zwanej dalej „ustawą z dnia 25 grudnia 2016 r.") stanowi:

„Niniejsza ustawa oraz rozporządzenia królewskie, które zostaną przyjęte celem jej wykonania, dokonują transpozycji [dyrektywy API] oraz [dyrektywy PNR]. Niniejsza ustawa oraz rozporządzenie królewskie dotyczące sektora morskiego dokonują częściowej transpozycji dyrektywy [2010/65]".

42 Artykuł 3 przedmiotowej ustawy ma następujące brzmienie:

„§ l. Niniejsza ustawa określa obowiązki przewoźników i operatorów turystycznych związane z przekazywaniem danych pasażerów udających się na terytorium kraju, przybywających z niego lub przez nie przejeżdżających.

§ 2. Król, w drodze rozporządzenia poddanego pod obrady rady ministrów, określa dla sektora transportu i operatorów turystycznych dane pasażerów, które mają być przekazywane, oraz sposoby ich przekazywania, po zasięgnięciu opinii Commission de la protection de la vie privé (komisji ds. ochrony życia prywatnego)".

43 Artykuł 4 wspomnianej ustawy stanowi:

„Do celów stosowania niniejszej ustawy i rozporządzeń wykonawczych do niej przyjmuje się następujące definicje:

[…]

8) »właściwe służby« – służby wskazane w art. 14 § 1 pkt 2;

9) »PNR« – zbiór danych o podróży każdego pasażera, który zawiera informacje, o których mowa w art. 9, niezbędne, aby umożliwić przetwarzanie i weryfikowanie rezerwacji przez przewoźników i operatorów turystycznych obsługujących rezerwacje w odniesieniu do każdego przelotu zarezerwowanego przez jakąkolwiek osobę lub w jej imieniu, bez względu na to, czy zbiór ten znajduje się w systemach rezerwacji, systemach odpraw pasażerskich (wykorzystywanych do kontrolowania pasażerów podczas wchodzenia na pokład) lub równorzędnych systemach pełniących te same funkcje;

10) »pasażer« – każda osoba, w tym osoba przesiadająca się lub przejeżdżająca, z wyjątkiem członków załogi, która jest przewożona lub ma być przewieziona przez przewoźnika, za zgodą tego ostatniego wyrażoną w formie wpisu tej osoby na listę pasażerów;

[…]”.

44 Artykuł 8 ustawy z dnia 25 grudnia 2016 r. stanowi:

„§ l. Dane pasażerów są przetwarzane w celu:

1) prowadzenia dochodzeń, w tym wykonywania kar lub środków ograniczenia wolności, dotyczących przestępstw, o których mowa w art. 90 ter § 2 […] pkt 7, […] pkt 8, […] pkt 11, […] pkt 14, […] pkt 17, 18, 19 oraz § 3 Code d’instruction criminelle (kodeksu postępowania karnego);

2) prowadzenia dochodzeń, w tym wykonywania kar oraz środków ograniczenia wolności dotyczących przestępstw wskazanych w art. 196 w zakresie przestępstw podrabiania dokumentów urzędowych i publicznych, art. 198, 199, 199 bis, 207, 213, 375 oraz 505 Code pénal (kodeksu karnego);

[…]

4) monitorowania działalności, o której mowa w art. 7 pkt 1 i pkt 3 ppkt 1 oraz art. 11 § 1 pkt 1–3 i 5 loi du 30 novembre 1998 organique des services de renseignement et de sécurité (ustawy organicznej z dnia 30 listopada 1998 r. o służbie wywiadowczej i bezpieczeństwa);

5) prowadzenia dochodzeń w odniesieniu do przestępstw wskazanych w art. 220 § 2 loi générale sur les douanes et accises (ogólnej ustawy o cłach i akcyzie) z dnia 18 lipca 1977 r. oraz art. 45 akapit trzeci loi du 22 décembre 2009 relative au régime général d’accise (ustawy z dnia 22 grudnia 2009 r. w sprawie ogólnych zasad dotyczących podatku akcyzowego) […].

§ 2. Na warunkach przewidzianych w rozdziale 11 dane pasażerów są również przetwarzane w celu ulepszenia kontroli osób na granicach zewnętrznych oraz w celu zwalczania nielegalnej imigracji".

45 Zgodnie z art. 14 § 1 tej ustawy:

„W skład JIP wchodzą:

[…]

2) delegowani członkowie pochodzący z następujących służb:
   a) służb policji, o których mowa w loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (ustawie z dnia 7 grudnia 1998 r., regulującej działanie zintegrowanych służb policyjnych, zorganizowanych na dwóch poziomach);
   b) służb bezpieczeństwa państwa, o których mowa w loi du 30 novembre 1998 organique des services de renseignement et de sécurité (ustawie organicznej z dnia 30 listopada 1998 r. w sprawie służb wywiadowczych i bezpieczeństwa);
   c) ogólnych służb wywiadowczych i bezpieczeństwa, o których mowa w loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

[…]".

46 Artykuł 24 wspomnianej ustawy, który znajduje się w sekcji 1, zatytułowanej „Przetwarzanie danych pasażerów w ramach wstępnej oceny pasażerów", rozdziału 10 rzeczonej ustawy, dotyczącego przetwarzania danych, ma następujące brzmienie:

„§ 1. Dane pasażerów są przetwarzane w celu dokonania wstępnej oceny pasażerów przed ich przyjazdem, ich wyjazdem lub ich planowanym przejazdem przez terytorium kraju w celu ustalenia, które osoby powinny podlegać bardziej szczegółowemu badaniu.

§ 2. W ramach celów, o których mowa w art. 8 § 1 pkt 1, 4 i 5, lub dotyczących zagrożeń, o których mowa w art. 8 pkt 1 lit. a), b), c), d), f), g) i art. 11 § 2 loi du 30 novembre 1998 organique des services de renseignement et de sécurité, wstępna ocena pasażerów opiera się na skojarzeniu danych w wyniku skorelowania danych pasażerów z:

1) bankami danych zarządzanymi przez właściwe służby lub które są w ich bezpośredniej dyspozycji, lub do których mają dostęp w ramach swoich zadań, lub z wykazami osób opracowanymi przez właściwe służby w ramach ich zadań;

2) kryteriami oceny, o których mowa w art. 25, ustalonymi wcześniej przez JIP.

§ 3. W ramach celów, o których mowa w art. 8 § 1 pkt 3, wstępna ocena pasażerów opiera się na skojarzeniu danych w wyniku skorelowania danych pasażerów z bankami danych, o których mowa w § 2 pkt 1.

§ 4. Skojarzenie danych jest zatwierdzane przez JIP w ciągu 24 godzin od otrzymania automatycznego powiadomienia o tym skojarzeniu.

§ 5. Jak tylko dojdzie do tego zatwierdzenia, odpowiednia służba, której dane leżą u źródła skojarzenia, podejmuje jak najszybciej konieczne działania".

47 Rozdział 11 ustawy z dnia 25 grudnia 2016 r., zatytułowany „Przetwarzanie danych pasażerów z zamiarem ulepszenia kontroli na granicach zewnętrznych i zwalczania nielegalnej imigracji", zawiera art. 28–31.

48 Artykuł 28 tej ustawy stanowi:

„§ 1. Niniejszy rozdział ma zastosowanie do przetwarzania danych pasażerów przez służby policji odpowiedzialne za kontrolę graniczną oraz przez Office des étrangers [urząd ds. cudzoziemców] w celu ulepszenia kontroli osób na granicach zewnętrznych oraz w celu zwalczania nielegalnej imigracji.

§ 2. Nie narusza on zobowiązań, jakie spoczywają na służbach policyjnych odpowiedzialnych za kontrolę granic oraz Office des étrangers w zakresie przekazywania danych osobowych lub informacji na podstawie ustaw lub rozporządzeń".

49 Zgodnie z art. 29 wspomnianej ustawy:

„§ 1. W celach wskazanych w art. 28 § 1 dane pasażerów są przekazywane służbom policyjnym odpowiedzialnym za kontrolę granic oraz Office des étrangers celem umożliwienia im wykonywania ich ustawowych zadań, w granicach przewidzianych w niniejszym artykule.

§ 2. Przekazywane są jedynie dane pasażerów, o których mowa w art. 9 § 1 pkt 18, dotyczące następujących kategorii pasażerów:

1) pasażerów, którzy zamierzają wjechać lub wjechali na terytorium przez granice zewnętrzne Belgii;

2) pasażerów, którzy zamierzają opuścić terytorium lub opuścili terytorium przez granice zewnętrzne Belgii;

3) pasażerów, którzy planują przejazd, znajdują się lub przejechali przez międzynarodową strefę tranzytu położoną w Belgii.

§ 3. Dane pasażerów, o których mowa w § 2, są przekazywane służbom policyjnym odpowiedzialnym za kontrolę granic zewnętrznych Belgii natychmiast po wpisaniu ich do banku danych pasażerów. Służby te przechowują te dane w tymczasowym pliku i usuwają je w ciągu 24 godzin następujących po przekazaniu.

§ 4. Dane pasażerów, o których mowa w § 2, są przekazywane do Office des étrangers niezwłocznie po ich zarejestrowaniu w bazie danych pasażerów, jeśli jest to potrzebne do wykonywania ustawowych zadań tego organu. Organ ten przechowuje dane w tymczasowym pliku i usuwa je w ciągu 24 godzin po przekazaniu.

Jeśli po upływie tego czasu dostęp do danych pasażerów, o których mowa w § 2, jest konieczny w ramach wykonywania zadań ustawowych Office des étrangers, przesyła on JIP wniosek z odpowiednim uzasadnieniem.

[…]".

50 Ustawa z dnia 25 grudnia 2016 r. znalazła zastosowanie do linii lotniczych, przewoźników obsługujących międzynarodowy przewóz podróżnych (przewoźników HST) oraz do pośredników podróży, których łączą umowy z tymi przewoźnikami (dystrybutorów biletów HST), jak również do przewoźników autobusowych, zgodnie z, odpowiednio, arrêté royal du 18 juillet 2017 relatif à l'exécution de la loi du 25 décembre 2016, reprenant les obligations pour les compagnies aériennes (rozporządzeniem królewskim z dnia 18 lipca 2017 r., wydanym w celu wykonania ustawy z dnia 25 grudnia 2016 r. w zakresie obowiązków linii lotniczych, *Moniteur belge* z dnia 28 lipca 2017 r., s. 75934), arrêté royal du 3 février 2019 relatif à l'exécution de la loi du 25 décembre 2016, reprenant les obligations pour les transporteurs HST et distributeurs de tickets HST (rozporządzeniem królewskim z dnia 3 lutego 2019 r. wydanym w celu wykonania ustawy z dnia 25 grudnia 2016 r. w zakresie obowiązków przewoźników HST oraz dystrybutorów biletów HST, *Moniteur belge* z dnia 12 lutego 2019 r., s. 13018) oraz arrêté royal du 3 février 2019 relatif à l'exécution de la loi du 25 décembre 2016, reprenant les obligations pour les transporteurs par bus (rozporządzeniem królewskim z dnia 3 lutego 2019 r. wydanym w celu wykonania ustawy z dnia 25 grudnia 2016 r. w zakresie obowiązków dla przewoźników autobusowych, *Moniteur belge* z dnia 12 lutego 2019 r., s. 13023).

II. Spór w postępowaniu głównym i pytania prejudycjalne

51 Pismem z dnia 24 lipca 2017 r. Ligue des droits humains wniosła do Cour constitutionnelle (trybunału konstytucyjnego, Belgia) skargę o stwierdzenie całkowitej lub częściowej nieważności ustawy z dnia 25 grudnia 2016 r.

52 Sąd odsyłający wskazuje, że ustawa ta dokonuje transpozycji do prawa krajowego dyrektywy PNR oraz dyrektywy API, a także, częściowo, dyrektywy 2010/65. Z prac przygotowawczych nad ustawą wynika, że zmierza ona do „stworzenia ram prawnych celem nałożenia na różne sektory przewozu osób o charakterze międzynarodowym (lotnictwo, kolej, międzynarodowe przewozy drogowe i morskie) oraz na operatorów turystycznych obowiązku przekazywania danych ich pasażerów do bazy danych zarządzanej przez [Service public fédéral intérieur (ministerstwo spraw wewnętrznych, Belgia)]". Ustawodawca krajowy doprecyzował również, że cele ustawy z dnia 25 grudnia 2016 r. dzielą się na trzy kategorie, a mianowicie, po pierwsze, na zapobieganie przestępstwom, ich wykrywanie i ściganie lub wykonywanie sankcji karnych, po drugie, na zadania służb wywiadowczych i bezpieczeństwa oraz po trzecie, na poprawę kontroli na granicach zewnętrznych i zwalczanie nielegalnej imigracji.

53 Na poparcie skargi Ligue des droits humains formułuje dwa zarzuty, po pierwsze, naruszenia art. 22 konstytucji w związku z art. 23 RODO, art. 7, 8 i art. 52 ust. 1 karty oraz art. 8 EKPC, a po drugie, pomocniczo, naruszenia wspomnianego art. 22 konstytucji w związku z art. 3 ust. 2 TUE i art. 45 karty.

54 W swoim pierwszym zarzucie Ligue des droits humains podnosi zasadniczo, że ustawa z dnia 25 grudnia 2016 r. stanowi ingerencję w prawo do poszanowania życia prywatnego oraz prawo ochrony danych osobowych, która nie jest zgodna z art. 52 ust. 1 karty, a w szczególności z zasadą proporcjonalności. Jej zdaniem, zbyt szerokie są zakres stosowania ustawy oraz sposób definiowania zbieranych danych, i mogą one prowadzić do ujawnienia informacji szczególnie chronionych. Również pojęcie „pasażera" w rozumieniu ustawy pozwala na zautomatyzowane i systematyczne, a nie ukierunkowane, przetwarzanie danych pasażerów. Ponadto nie zostały określone w sposób wystarczająco jasny zarówno charakter i sposoby zastosowania metody *prescreening*, jak i bazy danych, z którymi są porównywane uprzednio przekazane dane. Poza

tym, ustawa z dnia 25 grudnia 2016 r. służy innym celom niż dyrektywa PNR. Wreszcie okres pięciu lat przewidziany przez tę ustawę na zatrzymanie rzeczonych danych jest nieproporcjonalny.

55 W swoim drugim zarzucie, obejmującym art. 3 § 1, art. 8 § 2 oraz art. 28–31 ustawy z dnia 25 grudnia 2016 r., Ligue des droits humains podnosi, że rozszerzając system wprowadzony dyrektywą PNR na przewozy wewnątrzunijne, wskazane przepisy skutkują pośrednio przywróceniem kontroli na granicach wewnętrznych Unii, co jest sprzeczne ze swobodą przemieszczania się. Jak tylko bowiem dana osoba znajdzie się na terytorium belgijskim, czy to przy okazji przyjazdu, wyjazdu czy przesiadki, jej dane są automatycznie zbierane.

56 Rada ministrów kwestionuje tę argumentację. Uważa w szczególności, że pierwszy zarzut jest niedopuszczalny, jako że dotyczy RODO, które nie ma zastosowania do ustawy z dnia 25 grudnia 2016 r. Ponadto przetwarzanie danych przewidziane w tej ustawie, zgodnie z dyrektywą PNR, stanowi kluczowe narzędzie w szczególności do zwalczania terroryzmu i poważnej przestępczości, a środki wynikające z tej ustawy są proporcjonalne i niezbędne do osiągnięcia wyznaczonych celów.

57 W odniesieniu do zarzutu pierwszego sąd odsyłający pyta w pierwszej kolejności o możliwość zastosowania ochrony przewidzianej w RODO do przetwarzania danych wprowadzonego ustawą z dnia 25 grudnia 2016 r., której celem jest przede wszystkim wprowadzenie w życie dyrektywy PNR. Sąd ten zauważa następnie, odnosząc się do orzecznictwa, które miało swoje źródło w opinii 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r. (EU:C:2017:592), że definicja danych PNR zawarta w art. 3 pkt 5 oraz w załączniku I do dyrektywy PNR może, z jednej strony, być niewystarczająco jasna i precyzyjna, z uwagi na niewyczerpujący charakter opisu niektórych spośród danych, których dotyczą te przepisy, a z drugiej strony, może prowadzić pośrednio do ujawnienia danych szczególnie chronionych. Ponadto definicja pojęcia „pasażera", zawarta w art. 3 pkt 4 dyrektywy, może skutkować tym, że zbieranie, przekazywanie, przetwarzanie oraz zatrzymywanie danych PNR będzie stanowić ogólny i niezróżnicowany obowiązek mający zastosowanie do każdej osoby, która jest przewożona lub ma być przewożona oraz jest wpisana na listę pasażerów, niezależnie od tego, czy występują istotne powody, by podejrzewać, że ta osoba popełniła lub jest o krok od popełnienia przestępstwa, lub została uznana winną jego popełnienia.

58 Sąd odsyłający zauważył ponadto, że dane PNR, zgodnie z przepisami dyrektywy PNR, są systematycznie przedmiotem wstępnej oceny, która pociąga za sobą ich krzyżowanie się z bazami danych lub wcześniej ustalonymi kryteriami, w celu dokonania skojarzeń. Tymczasem, Komitet Doradczy konwencji nr 108 Rady Europy wskazał w swojej opinii z dnia 19 sierpnia 2016 r. dotyczącej konsekwencji w zakresie ochrony danych wynikających z przetwarzania danych pasażerów [T-PD(2016)18rev], że przetwarzanie danych osobowych może dotyczyć wszystkich pasażerów, a nie tylko poszczególnych jednostek podejrzewanych o udział w przestępstwie lub stwarzanie bezpośredniego zagrożenia dla bezpieczeństwa narodowego lub porządku publicznego oraz że dane PNR mogą być nie tylko porównywane (*data matching*) z bazami danych, ale również być poddawane eksploracji (*data mining*), przy użyciu selektorów lub algorytmów predykcyjnych, w celu znalezienia kogokolwiek, kto może być zamieszany lub zaangażowany w działalność przestępczą, przy czym taka ocena pasażerów poprzez mapowanie danych może wywoływać wątpliwości co do przewidywalności, w szczególności gdy jest ono dokonywane na podstawie algorytmów predykcyjnych wykorzystujących kryteria dynamiczne, które mogą ulegać zmianie w sposób ciągły w zależności od zdolności samodzielnego uczenia się. W tym kontekście sąd odsyłający zauważa, że jeśli wcześniej ustalone kryteria służące do

określenia profili ryzyka mają być szczegółowe, wiarygodne i niedyskryminacyjne, zgodnie z opinią 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r. (EU:C:2017:592), wcześniejsze zdefiniowanie owych kryteriów wydaje się technicznie niemożliwe.

59 Co się tyczy pięcioletniego okresu zatrzymania oraz dostępu do danych, o których mowa w art. 12 dyrektywy PNR, sąd odsyłający podnosi, że Commission de la protection de la vie privée (komisja ds. ochrony życia prywatnego, Belgia) w swojej opinii z inicjatywy własnej nr 01/2010 z dnia 13 stycznia 2010 r. dotyczącej projektu ustawy w sprawie przystąpienia do umowy PNR między Unią Europejską a Stanami Zjednoczonymi Ameryki oceniła, iż w przypadku gdy okres przechowywania danych jest długi, a dane są przechowywane masowo, ryzyko profilowania osób, których dane dotyczą, wzrasta, podobnie jak ryzyko nadużycia wykorzystania danych do innych celów niż początkowo przewidziane. Ponadto z opinii Komitetu Doradczego konwencji nr 108 Rady Europy z dnia 19 sierpnia 2016 r. wynika, że zamaskowane dane nadal umożliwiają identyfikację osób i z tego tytułu pozostają danymi osobowymi, a ich przechowywanie powinno być również ograniczone w czasie, aby zapobiec ciągłemu uogólnionemu nadzorowi.

60 Mając na względzie powyższe, biorąc pod uwagę orzecznictwo wynikające w szczególności z opinii 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r. (EU:C:2017:592), sąd odsyłający dąży do ustalenia, czy system zbierania, przekazywania, przetwarzania i zatrzymywania danych PNR wprowadzony dyrektywą PNR może zostać uznany za ograniczający się do tego, co ściśle niezbędne. Sąd ten uważa, że należy ustalić ponadto, czy omawiana dyrektywa stoi na przeszkodzie przepisom krajowym zezwalającym na przetwarzanie danych PNR w celu innym niż przewidziane w dyrektywie oraz czy przekazanie całości danych po ich depersonalizacji, na podstawie art. 12 tej dyrektywy, może być zatwierdzane przez organ krajowy, taki jak JIP, utworzony na podstawie ustawy z dnia 25 grudnia 2016 r.

61 Co do drugiego zarzutu, sąd odsyłający wskazuje, że art. 3 § 1 ustawy z dnia 25 grudnia 2016 r. określa obowiązki przewoźników i operatorów turystycznych związane z przekazywaniem danych pasażerów „udających się na terytorium kraju, przybywających z niego lub przez nie przejeżdżających". Sąd odsyłający dodaje, odnosząc się do zakresu zastosowania tej ustawy, że ustawodawca krajowy zdecydował się na „gromadzenie danych w zakresie przewozów wewnątrzunijnych" celem uzyskania „bardziej kompleksowego obrazu przejazdów pasażerów stanowiących potencjalne zagrożenie dla bezpieczeństwa wewnątrzwspólnotowego i krajowego", co przewiduje art. 2 dyrektywy PNR, w związku z jej motywem 10 – dla lotów wewnątrzunijnych. Sąd ów wskazuje ponadto, że komisja ds. ochrony życia prywatnego w swojej opinii nr 55/2015 z dnia 16 grudnia 2015 r. w sprawie wstępnego projektu ustawy z dnia 25 grudnia 2016 r. zadaje pytanie o ewentualny konflikt między belgijskim systemem PNR a zasadą swobodnego przepływu osób, jako że system ten obejmuje przewozy wykonywane w ramach Unii.

62 W tych okolicznościach Cour constitutionnelle (trybunał konstytucyjny) postanowił zawiesić postępowanie i zwrócić się do Trybunału z następującymi pytaniami prejudycjalnymi:

„1) Czy art. 23 [RODO] w związku z art. 2 ust. 2

lit. d) tego rozporządzenia należy interpretować w ten sposób, że ma on zastosowanie do przepisów krajowych takich jak ustawa [z dnia 25 grudnia 2016 r.], która dokonuje transpozycji [dyrektywy PNR], [dyrektywy API] oraz dyrektywy [2010/65]?

2) Czy w zakresie, w jakim wymienione w załączniku I do [dyrektywy PNR] dane są bardzo obszerne – w szczególności dane, o których mowa w pkt 18 załącznika I [do tej dyrektywy], które wykraczają poza dane określone w art. 3 ust. 2 [dyrektywy API] – oraz w zakresie, w jakim mogą one, rozpatrywane łącznie, ujawniać dane szczególnie chronione, a tym samym naruszać granice tego, co »absolutnie konieczne«, załącznik ten jest zgodny z art. 7, 8 i art. 52 ust. 1 [karty]?

3) Czy w zakresie, w jakim ze względu na wyrażenia »w szczególności« i »w tym«, zawarte w pkt 12 i 18 załącznika I do [dyrektywy PNR], dane, o których w nich mowa, zostały wymienione tytułem przykładu, a nie w sposób wyczerpujący, w związku z czym nie jest spełniony wymóg precyzyjności i jasności przepisów pociągających za sobą ingerencję w prawo do poszanowania życia prywatnego oraz w prawo do ochrony danych osobowych, wspomniane punkty tego załącznika są zgodne z art. 7, 8 i art. 52 ust. 1 [karty]?

4) Czy w zakresie, w jakim ustanowiony w art. 3 pkt 4 [dyrektywy PNR] i w załączniku I do tej dyrektywy system uogólnionego gromadzenia, przekazywania i przetwarzania danych pasażerów dotyczy każdej osoby, która wykorzystuje dany środek transportu, niezależnie od jakiegokolwiek obiektywnego czynnika pozwalającego na uznanie, że osoba ta może stanowić zagrożenie dla bezpieczeństwa publicznego, przepisy te są zgodne z art. 7, 8 i art. 52 ust. 1 [karty]?

5) Czy art. 6 [dyrektywy PNR] w związku z art. 7, 8 i art. 52 ust. 1 [karty] należy interpretować w ten sposób, że stoi on na przeszkodzie ustawodawstwu krajowemu takiemu jak ustawa [z dnia 25 grudnia 2016 r.], które dopuszcza, jako cel przetwarzania danych PNR, monitorowanie działalności wywiadowczej [monitorowanie działalności będącej przedmiotem zainteresowania] służb wywiadowczych i bezpieczeństwa, a tym samym uwzględnia ten cel w ramach celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania?

6) Czy art. 6 [dyrektywy PNR] jest zgodny z art. 7, 8 i art. 52 ust. 1 [karty] w zakresie, w jakim wstępna ocena danych pasażerów, którą on reguluje, poprzez korelację z bazami danych i określonymi wcześniej kryteriami, jest stosowana w sposób systematyczny i uogólniony, niezależnie od jakiegokolwiek obiektywnego czynnika pozwalającego na uznanie, że pasażerowie ci mogą stanowić zagrożenie dla bezpieczeństwa publicznego?

7) Czy pojęcie »innego właściwego organu krajowego«, o którym mowa w art. 12 ust. 3 [dyrektywy PNR], można interpretować w ten sposób, że dotyczy ono JIP utworzonej przez ustawę z dnia 25 grudnia 2016 r., która może zatem zezwolić na dostęp do danych PNR po upływie sześciomiesięcznego terminu w ramach wyszukiwań ad hoc?

8) Czy art. 12 [dyrektywy PNR] w związku z art. 7, 8 i art. 52 ust. 1 [karty] należy interpretować w ten sposób, że stoi on na przeszkodzie ustawodawstwu krajowemu takiemu jak ustawa [z dnia 25 grudnia 2016 r.], która przewiduje ogólny termin przechowywania danych wynoszący pięć lat, nie dokonując rozróżnienia co do tego, czy w ramach wstępnej oceny okazuje się, że dani pasażerowie mogą lub nie mogą stanowić zagrożenia dla bezpieczeństwa publicznego?

9) a) Czy [dyrektywa API] jest zgodna z art. 3 ust. 2 [TUE] i art. 45 [karty] w zakresie, w jakim ustanowione w niej obowiązki mają zastosowanie do lotów wewnątrz Unii Europejskiej?

b) Czy [dyrektywę API] w związku z art. 3 ust. 2 [TUE] i art. 45 [karty] należy interpretować w ten sposób, że stoi ona na przeszkodzie ustawodawstwu krajowemu takiemu jak zaskarżona ustawa, która w celu zwalczania nielegalnej imigracji i ulepszenia kontroli granicznych zezwala na system gromadzenia i przetwarzania danych pasażerów »udających się do, przybywających z i przejeżdżających przez terytorium kraju«, co może powodować w sposób pośredni przywrócenie kontroli na granicach wewnętrznych?

10) Jeżeli na podstawie odpowiedzi udzielonych na poprzednie pytania prejudycjalne Cour constitutionnelle [trybunał konstytucyjny] miałby dojść do wniosku, że zaskarżona ustawa, transponująca w szczególności [dyrektywę PNR], narusza jeden lub więcej obowiązków wynikających z przepisów wskazanych w tych pytaniach, to czy mógłby on tymczasowo utrzymać w mocy skutki [ustawy z dnia 25 grudnia 2016 r.], aby uniknąć niepewności prawa i zapewnić możliwość dalszego wykorzystywania uprzednio zgromadzonych i przechowywanych danych do celów określonych w ustawie?".

III. W przedmiocie pytań prejudycjalnych

A. W przedmiocie pytania pierwszego

63 W swoim pytaniu pierwszym sąd odsyłający dąży zasadniczo do ustalenia, czy art. 2 ust. 2 lit. d) oraz art. 23 RODO należy interpretować w ten sposób, że rozporządzenie to ma zastosowanie do przetwarzania danych osobowych przewidzianego przez uregulowanie krajowe dokonujące transpozycji do prawa krajowego jednocześnie przepisów dyrektywy PNR, dyrektywy API i dyrektywy 2010/65, w szczególności w odniesieniu do przekazywania, zatrzymywania oraz przetwarzania danych PNR.

64 Jak wynika z art. 2 ust. 1 RODO, rozporządzenie to ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych. Pojęcie „przetwarzania" zostało zdefiniowane w sposób szeroki w art. 4 pkt 2 rozporządzenia jako obejmujące w szczególności zbieranie, utrwalanie, przechowywanie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub usuwanie takich danych lub ich zbiorów.

65 Rząd belgijski podniósł jednakże, że przekazywanie danych PNR przez podmioty gospodarcze do JIP w celu zapobiegania i wykrywania przestępstw, o którym mowa w art. 1 ust. 1 lit. a), art. 1 ust. 2 oraz art. 8 dyrektywy PNR, które stanowi „przetwarzanie" danych osobowych w rozumieniu art. 4 pkt 2 RODO, podobnie jak ich wcześniejsze zbieranie, nie wchodzi w zakres stosowania tego rozporządzenia na podstawie art. 2 ust. 2 lit. d) tego rozporządzenia z tego względu, że wyrok z dnia 30 maja 2006 r., Parlament/Rada i Komisja (C-317/04 i C-318/04, EU:C:2006:346, pkt 57–59), odnoszący się do art. 3 ust. 2 tiret pierwsze dyrektywy 95/46, można zastosować do wskazanego przepisu RODO.

66 W tym zakresie jest prawdą, że, jak stwierdził już Trybunał, art. 3 ust. 2 tiret pierwsze dyrektywy 95/46, która została uchylona i zastąpiona RODO ze skutkiem na dzień 25 maja 2018 r., wyłączył z zakresu stosowania dyrektywy w sposób ogólny „działalność na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa" bez rozróżnienia w zależności od rozpatrywanego podmiotu przetwarzającego dane. A zatem przetwarzanie danych dokonywane

przez podmioty prywatne, wynikające z obowiązków nałożonych przez władze publiczne, mogło w danym przepadku być objęte wyjątkiem przewidzianym w tym przepisie, biorąc pod uwagę fakt, że jego sformułowanie dotyczyło każdego przetwarzania, niezależnie od podmiotu go dokonującego, którego celem była działalność na rzecz bezpieczeństwa publicznego, obronności lub bezpieczeństwa państwa (zob. podobnie 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, pkt 101).

67 Jednakże art. 2 ust. 2 lit. d) RODO wprowadza takie rozróżnienie, ponieważ, jak wskazał rzecznik generalny w pkt 41 i 46 opinii, z brzmienia tego przepisu jasno wynika, że do objęcia przetwarzania danych wyjątkiem przewidzianym w tym przepisie muszą być spełnione dwa warunki. O ile pierwszy z warunków dotyczy celów przetwarzania, a mianowicie zapobiegania przestępstwom i ich wykrywania lub ścigania, lub wykonywania sankcji karnych, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, drugi warunek dotyczy podmiotu dokonującego przetwarzania, a mianowicie „właściwego organu" w rozumieniu omawianego przepisu.

68 Jak wskazał Trybunał, z art. 23 ust. 1 lit. d) i h) RODO wynika, że przetwarzanie danych osobowych dokonywane przez podmioty prywatne w celach wskazanych w art. 2 ust. 2 lit. d) tego rozporządzenia wchodzi w zakres jego zastosowania (zob. podobnie 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, pkt 102).

69 W związku z tym przywołane przez rząd belgijski orzecznictwo wynikające z wyroku z dnia 30 maja 2006 r., Parlament/Rada i Komisja (C-317/04 i C-318/04, EU:C:2006:346) nie ma przełożenia na wyjątek od zakresu stosowania RODO, o którym mowa w jego art. 2 ust. 2 lit. d).

70 Poza tym wyjątek ten należy, podobnie jak inne wyjątki od zakresu stosowania RODO przewidziane w jego art. 2 ust. 2, interpretować ściśle.

71 Jak wynika z motywu 19 tego rozporządzenia, rzeczony wyjątek jest uzasadniony tym, że przetwarzanie 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, jest uregulowany bardziej szczegółowym aktem Unii, a mianowicie dyrektywą 2016/680, która została przyjęta tego samego dnia co RODO [wyrok z dnia 22 czerwca 2021 r., Latvijas Republikas Saeima (Punkty karne), C-439/19, EU:C:2021:504, pkt 69].

72 Jak zostało uściślone ponadto w motywach 9–11 dyrektywy 2016/680, formułuje ona szczególne zasady dotyczące ochrony osób fizycznych w zakresie przetwarzania ich danych, przy poszanowaniu szczególnego charakteru tych czynności podlegających dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej, podczas gdy RODO tworzy zasady bardziej ogólne, dotyczące ochrony osób, które mają zastosowanie do rzeczonego przetwarzania wtedy, gdy akt bardziej szczegółowy, tj. dyrektywa 2016/680 nie znajduje zastosowania. W szczególności, zgodnie z motywem 11 tej dyrektywy, RODO ma zastosowanie do przetwarzania danych osobowych przeprowadzanego przez „właściwy organ", w rozumieniu art. 3 ust. 7 tej dyrektywy, ale w celach innych niż w niej przewidziane [zob. podobnie wyrok z dnia 22 czerwca 2021 r., Latvijas Republikas Saeima (Punkty karne), C-439/19, EU:C:2021:504, pkt 70].

73 Co do pierwszego warunku wskazanego w pkt 67 niniejszego wyroku, a w szczególności w zakresie celów realizowanych przez przetwarzanie danych osobowych przewidziane w dyrektywie PNR, należy przypomnieć, że zgodnie z art. 1 ust. 2 tej dyrektywy dane PNR mogą być przetwarzane wyłącznie w celach zapobiegania przestępstwom terrorystycznym i poważnej przestępczości oraz ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania. Cele te są tożsame z tymi wskazanymi w art. 2 ust. 2 lit. d) RODO oraz art. 1 ust. 1 dyrektywy 2016/680, a zatem rzeczone przetwarzanie może być objęte wyjątkiem wskazanym w art. 2 ust. 2 lit. d) rozporządzenia, a tym samym znajdować się w zakresie zastosowania dyrektywy 2016/680.

74 Nie jest tak natomiast w przypadku przetwarzania, o którym mowa w dyrektywie API i dyrektywie 2010/65, których cele są inne od tych przewidzianych w art. 2 ust. 2 lit. d) RODO oraz w art. 1 ust. 1 dyrektywy 2016/680.

75 Jeśli chodzi o dyrektywę API, zmierza ona bowiem do ulepszenia kontroli na granicach oraz zwalczania nielegalnej imigracji w drodze przesyłania z wyprzedzeniem danych pasażerów przez przewoźników właściwym krajowym organom, co wynika z jej motywów 1 oraz 7–9, a także jej art. 1. Ponadto inne jej motywy i przepisy pokazują, że przetwarzanie danych przewidziane w celu jej wdrożenia jest objęte zakresem stosowania RODO. Zgodnie z motywem 12 tej dyrektywy „dyrektywa [95/46] ma zastosowanie w odniesieniu do przetwarzania danych osobowych przez organy państw członkowskich". Poza tym art. 6 ust. 1 akapit piąty dyrektywy API wskazuje, że państwa członkowskie mogą również wykorzystać dane API do celów wykonania prawa, „uwzględniając przepisy dotyczące ochrony danych na mocy dyrektywy [95/46]", przy czym to wyrażenie zostało użyte również w akapicie trzecim tego przepisu. Z kolei wyrażenie „bez uszczerbku dla dyrektywy [95/46]" jest użyte w szczególności w motywie 9 dyrektywy API. Artykuł 6 ust. 2 dyrektywy API przewiduje wreszcie, że pasażerowie winni być powiadamiani przez przewoźników „zgodnie z przepisami ustanowionymi w dyrektywie [95/46]".

76 Co się tyczy dyrektywy 2010/65, z jej motywu 2 oraz art. 1 ust. 1 wynika, że dyrektywa ta ma na celu uproszczenie i zharmonizowanie procedur administracyjnych stosowanych w transporcie morskim poprzez upowszechnienie elektronicznej transmisji informacji i usprawnienie formalności sprawozdawczych, aby ułatwić transport morski i zmniejszyć obciążenia administracyjne przedsiębiorstw żeglugowych. Artykuł 8 ust. 2 tej dyrektywy potwierdza tymczasem, że przetwarzanie danych przewidziane w celu jej realizacji objęte jest zakresem stosowania RODO, nakładając na państwa członkowskie obowiązek zapewnienia poszanowania dyrektywy 95/46 w zakresie danych osobowych.

77 Wynika z tego, że przetwarzanie danych, o którym mowa w uregulowaniu krajowym dokonującym transpozycji do prawa krajowego dyrektywy API oraz dyrektywy 2010/65, jest objęte zakresem stosowania RODO. Z kolei przetwarzanie danych przewidziane w uregulowaniu krajowym dokonującym transpozycji do prawa krajowego dyrektywy PNR może nie podlegać, zgodnie z wyjątkiem wskazanym w art. 2 ust. 2 lit. d) RODO, zakresowi stosowania tego rozporządzenia, z zastrzeżeniem spełnienia drugiego z warunków wspomnianych w pkt 67 niniejszego wyroku, a mianowicie, by podmiot przetwarzający dane był właściwym organem w rozumieniu tego przepisu.

78 Jeśli chodzi o ten drugi warunek, Trybunał orzekł już, że w zakresie, w jakim dyrektywa 2016/680 definiuje w swoim art. 3 ust. 7 pojęcie „właściwego organu", definicja ta winna być stosowana, analogicznie, do art. 2 ust. 2 lit. d) RODO [zob. podobnie wyrok z dnia 22 czerwca 2021 r., Latvijas Republikas Saeima (Punkty karne), C-439/19, EU:C:2021:504, pkt 69].

79 Tymczasem zgodnie z art. 4 i 7 dyrektywy PNR każde państwo członkowskie ustanawia lub wyznacza jako swoją JIP organ właściwy do zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie lub ich ścigania oraz sporządza wykaz właściwych organów uprawnionych do występowania do JIP o dane PNR lub o wyniki przetwarzania tych danych, przy czym te ostatnie organy również są organami właściwymi, na co wskazuje art. 7 ust. 2 wspomnianej dyrektywy.

80 Z powyższego wynika, że przetwarzanie danych PNR dokonywane przez JIP i organy właściwe do takich celów, o których mowa wyżej, spełnia oba warunki wymienione w pkt 67 niniejszego wyroku i dlatego to przetwarzanie jest objęte nie tylko dyrektywą PNR, ale i dyrektywą 2016/680, lecz nie RODO, co potwierdza zresztą motyw 27 dyrektywy PNR.

81 Ponieważ jednak podmioty gospodarcze, takie jak przewoźnicy lotniczy, nawet jeśli mają ustawowy obowiązek przekazywania danych PNR, nie są ani zobowiązane do wykonywania władzy publicznej, ani wyposażone w uprawnienia publiczne przez przedmiotową dyrektywę, podmioty te nie mogą być uznawane za właściwe organy w rozumieniu art. 3 ust. 7 dyrektywy 2016/680 oraz art. 2 ust. 2 lit. d) RODO i dlatego gromadzenie i przekazywanie JIP przedmiotowych danych przez przewoźników lotniczych podlega temu rozporządzeniu. Ten wniosek odnosi się również do sytuacji przewidzianej w ustawie z dnia 25 grudnia 2016 r., w której gromadzenie i przekazywanie rzeczonych danych jest wykonywane przez innych przewoźników oraz operatorów turystycznych.

82 Sąd odsyłający pyta wreszcie o możliwy skutek przyjęcia przepisów krajowych zmierzających do transpozycji jednocześnie przepisów dyrektywy PNR, dyrektywy API i dyrektywy 2010/65, takich jak ustawa z dnia 25 grudnia 2016 r. W tym zakresie należy przypomnieć, że jak wynika z pkt 72 i 75–77 niniejszego wyroku, przetwarzanie danych, o którym mowa w dwóch ostatnich dyrektywach, jest objęte zakresem stosowania RODO, które zawiera ogólne zasady w zakresie ochrony osób fizycznych dotyczące przetwarzania danych osobowych.

83 Tak więc, jeśli przetwarzanie danych wykonywane na podstawie tych przepisów krajowych jest objęte dyrektywą API lub dyrektywą 2010/65, RODO znajduje zastosowanie do tego przetwarzania. Tak samo rzecz się ma z przetwarzaniem danych na tej samej podstawie, objętym, w zakresie swojego celu, poza dyrektywą PNR, dyrektywą API lub dyrektywą 2010/65. Wreszcie, jeśli przetwarzanie danych na podstawie tego samego uregulowania jest objęte, w zakresie swojego celu jedynie dyrektywą PNR, RODO ma zastosowanie w przypadku gromadzenia i przekazywania danych PNR do JIP przez przewoźników lotniczych. Z kolei, jeśli takie przetwarzanie jest dokonywane przez JIP lub organy właściwe w celach przewidzianych w art. 1 ust. 2 dyrektywy PNR, przetwarzanie to jest objęte, poza prawem krajowym, dyrektywą 2016/680.

84 Biorąc pod uwagę całokształt powyższych rozważań, na pytanie pierwsze należy odpowiedzieć w ten sposób, że art. 2 ust. 2 lit. d) oraz art. 23 RODO należy interpretować w ten sposób, iż rozporządzenie to ma zastosowanie do przetwarzania danych osobowych przewidzianego przez uregulowanie krajowe dokonujące transpozycji do prawa krajowego jednocześnie przepisów dyrektywy API, dyrektywy 2010/65 i dyrektywy PNR w zakresie, po pierwsze, przetwarzania danych dokonywanego przez podmioty prywatne, a po drugie, dokonywanego przez organy publiczne przetwarzania danych objętego dyrektywą API, dyrektywą 2010/65 lub obiema tymi dyrektywami. Rozporządzenie to nie ma natomiast zastosowania do przewidzianego przez to uregulowanie przetwarzania danych objętego jedynie dyrektywą PNR, które jest dokonywane przez JIP lub właściwe organy w celach wskazanych w art. 1 ust. 2 tej dyrektywy.

B. W przedmiocie pytań od drugiego do czwartego oraz pytania szóstego

85 W pytaniach od drugiego do czwartego oraz w pytaniu szóstym, które należy rozpatrzyć łącznie, sąd odsyłający dąży zasadniczo do ustalenia ważności dyrektywy PNR w świetle art. 7 i 8 oraz art. 52 ust. 1 karty. Pytania te dotyczą w szczególności:

– załącznika I do tej dyrektywy oraz danych, które są w nim wymienione, zwłaszcza tych figurujących w pkt 12 i 18, w świetle wymagań jasności i precyzji (pytania drugie i trzecie);

– art. 3 pkt 4 wspomnianej dyrektywy oraz załącznika I do niej w zakresie tego, czy system uogólnionego gromadzenia, przekazywania i przetwarzania danych PNR, który wprowadzają przedmiotowe przepisy, może być stosowany do każdej osoby odbywającej lot podlegającej przepisom dyrektywy (pytanie czwarte) oraz

– art. 6 dyrektywy PNR w zakresie, w jakim przewiduje on wstępną ocenę, celem zestawienia danych PNR z bazami danych lub ich przetwarzanie w świetle wcześniej ustalonych kryteriów, któremu te dane są poddawane w sposób systematyczny i uogólniony, niezależnie od istnienia jakiejkolwiek obiektywnej przesłanki pozwalającej uznać, że dani pasażerowie mogą stanowić ryzyko dla bezpieczeństwa publicznego (pytanie szóste).

86 Tytułem wstępu należy przypomnieć, że zgodnie z ogólną zasadą wykładni akt prawa Unii powinien być interpretowany tak dalece, jak to możliwe, w sposób, który nie podważa jego ważności, i w zgodzie z całością prawa pierwotnego, w tym w szczególności z postanowieniami karty. W związku z tym, wówczas gdy tekst prawa wtórnego Unii można poddać więcej niż jednej wykładni, należy dać raczej pierwszeństwo tej wykładni, która zapewnia zgodność przepisu z prawem pierwotnym, niż wykładni prowadzącej do uznania jego niezgodności z tym prawem (wyrok z dnia 2 lutego 2021 r., Consob, C-481/19, EU:C:2021:84, pkt 50 i przytoczone tam orzecznictwo).

87 Poza tym, zgodnie z utrwalonym orzecznictwem, w przypadku gdy przepisy dyrektywy pozostawiają państwom członkowskim zakres swobodnego uznania przy określeniu środków mających na celu ich transpozycję, tak by można je było dostosować do różnych możliwych sytuacji, przy przyjmowaniu tych środków państwa członkowskie są zobowiązane nie tylko dokonywać wykładni ich prawa krajowego w sposób zgodny z konkretnymi dyrektywami, lecz także nie opierać się na takiej wykładni tych dyrektyw, która pozostawałaby w konflikcie z prawami podstawowymi chronionymi przez porządek prawny Unii lub z innymi ogólnymi zasadami uznanymi przez ten porządek [zob. podobnie wyroki: z dnia 15 lutego 2016 r., N., C-601/15 PPU, EU:C:2016:84, pkt 60 i przytoczone tam orzecznictwo; z dnia 16 lipca 2020 r., État belge (Łączenie rodzin – małoletnie dziecko), C-133/19, C-136/19 i C-137/19, EU:C:2020:577, pkt 33 i przytoczone tam orzecznictwo].

88 Jeśli chodzi o dyrektywę PNR, należy zauważyć w szczególności, że w jej motywach 15, 20, 22, 25, 36 i 37 podkreślono wagę, jaką ustawodawca Unii przykłada, odnosząc się do wysokiego poziomu ochrony danych, do pełnego poszanowania praw podstawowych zagwarantowanych w art. 7, 8 i 21 karty, jak również zasady proporcjonalności i dlatego, jak wskazano w motywie 36, dyrektywa ta „powinna […] zostać odpowiednio wdrożona”.

89 W szczególności w motywie 22 dyrektywy PNR podkreślono, że „uwzględniając w pełni zasady przedstawione w najnowszym orzecznictwie [Trybunału] dotyczącym przedmiotowej kwestii, przy stosowaniu [tej] dyrektywy należy zapewnić pełne poszanowanie praw podstawowych,

prawa do prywatności i zasady proporcjonalności" oraz „zapewnić faktyczną zgodność z celami, jakimi są konieczność i proporcjonalność, w celu realizacji interesu publicznego uznanego przez Unię oraz potrzeby zapewnienia ochrony praw i wolności innych osób w walce z przestępstwami terrorystycznymi i poważną przestępczością". W motywie tym dodano, że stosowanie dyrektywy „powinno być należycie uzasadnione; należy wprowadzić niezbędne gwarancje, aby zapewnić zgodność z prawem przechowywania, analizowania, przekazywania lub wykorzystywania danych PNR".

90 Ponadto art. 19 ust. 2 dyrektywy PNR nakłada na Komisję, w ramach przeglądu dyrektywy, obowiązek zwrócenia szczególnej uwagi na „przestrzeganie mających zastosowanie standardów ochrony danych osobowych", „konieczność i proporcjonalność zbierania i przetwarzania danych PNR w odniesieniu do każdego celu określonego w niniejszej dyrektywie", jak również na „długość okresu zatrzymania danych".

91 Należy zatem sprawdzić, czy dyrektywa PNR, zgodnie z wymogami wyrażonymi w szczególności w jej motywach oraz przepisach wskazanych w pkt 88–90 niniejszego wyroku, może być interpretowana w sposób, który zapewni pełne poszanowanie praw podstawowych zagwarantowanych w art. 7 i 8 karty, jak również zasady proporcjonalności, o której mowa w jej art. 52 ust. 1.

1. W przedmiocie wynikającej z dyrektywy PNR ingerencji w prawa podstawowe zagwarantowane w art. 7 i 8 karty

92 Artykuł 7 karty gwarantuje każdemu prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się, podczas gdy art. 8 ust. 1 karty wyraźnie przyznaje każdemu prawo do ochrony danych osobowych, które go dotyczą.

93 Jak wynika z art. 3 pkt 5 dyrektywy PNR oraz z wykazu znajdującego się w załączniku I do niej, na dane PNR, o których mowa w dyrektywie, składają się w szczególności, oprócz imienia i nazwiska pasażera lub pasażerów lotniczych – informacje niezbędne do dokonania rezerwacji, jak daty planowanej podróży i trasy podróży, informacje o biletach, grupy osób zarejestrowanych pod tym samym numerem rezerwacji, informacje kontaktowe pasażera lub pasażerów, informacje o płatnościach lub fakturowaniu, informacje o bagażu, jak również uwagi ogólne o pasażerach.

94 Jako że dane PNR zawierają więc informacje o konkretnych osobach fizycznych, a mianowicie o określonych pasażerach lotniczych, różne formy przetwarzania, jakimi mogą być poddane te dane, mają wpływ na podstawowe prawo do poszanowania życia prywatnego zagwarantowane w art. 7 karty [zob. podobnie opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 121, 122 i przytoczone tam orzecznictwo].

95 Ponadto przetwarzanie danych PNR, takie jak przewidziane w dyrektywie PNR, jest objęte także art. 8 karty z tego względu, że stanowi przetwarzanie danych osobowych w rozumieniu tego postanowienia i tym samym powinno spełniać wymogi ochrony danych w nim przewidziane [zob. podobnie opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 123 i przytoczone tam orzecznictwo].

96 Z utrwalonego orzecznictwa wynika tymczasem, że udostępnianie danych osobowych podmiotowi trzeciemu, takiemu jak organ publiczny, stanowi ingerencję w zagwarantowane w art. 7 i 8 karty prawa podstawowe niezależnie od tego, w jaki sposób te dane zostaną później wykorzystane. Tak samo rzecz się ma w przypadku przechowywania danych osobowych oraz

dostępu do nich z zamiarem ich wykorzystania przez organy publiczne. W tym względzie nie ma znaczenia, czy rozpatrywane informacje dotyczące życia prywatnego są danymi szczególnie chronionymi, czy nie, ani czy osoby, których dane dotyczą, ucierpiały z powodu ewentualnych niedogodności wynikających z tej ingerencji [opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 124, 126 i przytoczone tam orzecznictwo].

97 Co za tym idzie, zarówno przekazywanie danych PNR przez przewoźników lotniczych do JIP danego państwa członkowskiego, przewidziane w art. 1 ust. 1 lit. a) dyrektywy PNR w związku z jej art. 8, jak i uregulowanie warunków zmierzających do zatrzymywania tych danych celem ich wykorzystania oraz ich ewentualnego późniejszego przekazania właściwym organom tego państwa członkowskiego, JIP lub właściwym organom innych państw członkowskich, Europolowi lub nawet organom państw trzecich, na co zezwalają w szczególności art. 6, 7, 9 i 10–12 tej dyrektywy, stanowią ingerencje w prawa gwarantowane w art. 7 i 8 karty.

98 Jeśli chodzi o wagę tych ingerencji, należy zauważyć, po pierwsze, że na podstawie art. 1 ust. 1 lit. a) dyrektywy PNR w związku z jej art. 8 dyrektywa ta przewiduje systematyczne i ciągłe przekazywanie do JIP danych PNR wszystkich pasażerów odbywających loty pozaunijne, w rozumieniu art. 3 pkt 2 tej dyrektywy, odbywające się między państwami trzecimi i Unią. Jak podniósł rzecznik generalny w pkt 73 opinii, takie przekazywanie pociąga za sobą ogólny dostęp JIP do wszystkich przekazanych danych PNR, dotyczących wszystkich osób korzystających z usług transportu lotniczego, niezależnie od późniejszego wykorzystania tych danych.

99 Po drugie, art. 2 dyrektywy PNR przewiduje w ust. 1, że państwa członkowskie mogą zdecydować o zastosowaniu dyrektywy do lotów wewnątrzunijnych, w rozumieniu jej art. 3 pkt 3, oraz wskazuje w ust. 2, że w takim przypadku wszystkie przepisy dyrektywy „stosuje się do lotów wewnątrzunijnych, tak jakby były one lotami pozaunijnymi, oraz do danych PNR dotyczących lotów wewnątrzunijnych, tak jakby były one danymi PNR dotyczącymi lotów pozaunijnych”.

100 Po trzecie, nawet jeżeli niektóre dane PNR wymienione w załączniku I do dyrektywy PNR, takie jak wskazane w pkt 93 niniejszego wyroku, rozpatrywane oddzielnie, nie wydają się ujawniać istotnych informacji o życiu prywatnym danych osób, to jednak, rozpatrywane jako całość, mogą między innymi ujawniać pełną trasę podróży, nawyki turystyczne, relacje między dwoma osobami lub większą ich liczbą, a także informacje o sytuacji finansowej pasażerów lotniczych, ich zwyczajach żywieniowych lub stanie zdrowia, a nawet mogą dostarczać o tych pasażerach informacji szczególnie chronionych [zob. podobnie, opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 128].

101 Po czwarte, na podstawie art. 6 ust. 2 lit. a) i b) dyrektywy PNR, dane przekazane przez przewoźników lotniczych mają być przedmiotem nie tylko wstępnej oceny, dokonywanej przed planowanym przylotem lub wylotem pasażerów, ale także późniejszej oceny.

102 Jeśli chodzi o wstępną ocenę, z art. 6 ust. 2 lit. a) oraz art. 6 ust. 3 dyrektywy PNR wynika, że ocena ta jest dokonywana przez JIP państw członkowskich w sposób systematyczny i w sposób zautomatyzowany, a zatem ciągły, i niezależnie od tego, czy istnieje jakakolwiek przesłanka wskazująca na istnienie ryzyka zaangażowania danych osób w przestępstwa terrorystyczne lub poważną przestępczość. W tym celu wskazane przepisy przewidują, że dane PNR mogą być porównywane z „bazami danych, które mają znaczenie” oraz być przetwarzane według „wcześniej ustalonych kryteriów”.

103 W tym kontekście należy przypomnieć, że Trybunał orzekł już, iż zakres ingerencji wynikający ze zautomatyzowanych analiz danych PNR w prawa uznane w art. 7 i 8 karty zależy zasadniczo od określonych wcześniej modeli i kryteriów, a także baz danych, na których opiera się ten rodzaj przetwarzania danych [opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 172].

104 Jak zauważył tymczasem rzecznik generalny w pkt 78 opinii, przetwarzanie, o którym mowa w art. 6 ust. 3 lit. a) dyrektywy PNR, a mianowicie porównywanie danych PNR z „bazami danych, które mają znaczenie", może dostarczyć dodatkowych informacji o życiu prywatnym pasażerów lotniczych i pozwolić na wyciągnięcie w tym zakresie bardzo konkretnych wniosków.

105 Co do przetwarzania danych PNR w świetle „wcześniej ustalonych kryteriów", o którym mowa w art. 6 ust. 3 lit. b) dyrektywy PNR, prawdą jest, że art. 6 ust. 4 tej dyrektywy wymaga, by ocena pasażerów według tych kryteriów odbywała się w sposób niedyskryminacyjny, a zwłaszcza bez opierania się na cechach wskazanych w ostatnim zdaniu tego ust. 4. Poza tym przyjęte kryteria muszą być ukierunkowane, proporcjonalne i szczegółowe.

106 Niemniej Trybunał orzekł już, że w zakresie, w jakim zautomatyzowane analizy danych PNR są dokonywane na podstawie danych osobowych niezweryfikowanych oraz opierają się one na określonych wcześniej modelach i kryteriach, w sposób nieunikniony obarczone są pewnym marginesem błędu [zob. analogicznie opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 169]. W szczególności, jak podniósł co do istoty rzecznik generalny w pkt 78 opinii, z dokumentu roboczego Komisji [SWD(2020) 128 final] załączonego do jej sprawozdania z dnia 24 lipca 2020 r. dotyczącego przeglądu dyrektywy PNR wynika, że liczba pozytywnych wyników będących rezultatem zautomatyzowanego przetwarzania, o którym mowa w art. 6 ust. 3 lit. a) i b) dyrektywy, które okazały się błędne po indywidualnym sprawdzeniu za pomocą środków niezautomatyzowanych, jest dość znacząca i wynosiła w latach 2018–2019 co najmniej pięć osób na sześć zidentyfikowanych. To przetwarzanie prowadzi zatem do pogłębionej analizy danych PNR w stosunku do tychże osób.

107 Jeśli chodzi o późniejszą ocenę danych PNR, o której mowa w art. 6 ust. 2 lit. b) dyrektywy PNR, z tego przepisu wynika, że w okresie sześciu miesięcy następującym po przekazaniu danych PNR, o którym mowa w art. 12 ust. 2 tej dyrektywy, JIP jest zobowiązana, na wniosek właściwych organów, do przekazania im danych PNR oraz do przetwarzania ich w określonych przypadkach w celach zapobiegania przestępstwom terrorystycznym lub poważnej przestępczości.

108 Poza tym, nawet jeśli po upływie tego okresu sześciu miesięcy dane PNR są depersonalizowane poprzez maskowanie niektórych ich elementów, JIP, zgodnie z art. 12 ust. 3 dyrektywy PNR, może zostać zobowiązana, w następstwie odpowiedniego wniosku, do przekazania właściwym organom całości danych PNR w formie pozwalającej zidentyfikować daną osobę wtedy, gdy istnieje uzasadnienie, by uznać, że jest to niezbędne do celów określonych w art. 6 ust. 2 lit. b) tej dyrektywy, przy czym takie przekazanie jest uzależnione od zgody przyznawanej przez organ wymiaru sprawiedliwości lub „inny [właściwy] organ krajowy".

109 Po piąte, przewidując w swoim art. 12 ust. 1, bez jakiegokolwiek doprecyzowania, że dane PNR są zatrzymywane w bazie danych przez okres pięciu lat od przekazania ich do JIP w państwie członkowskim, na którego terytorium ma miejsce przylot lub z którego terytorium ma miejsce odlot, dyrektywa PNR pozwala – biorąc pod uwagę fakt, że całość danych PNR jest możliwa do ujawnienia w przypadku wskazanym w poprzednim punkcie, pomimo ich depersonalizacji poprzez maskowanie niektórych elementów danych po upływie pierwotnego okresu sześciu

miesięcy – na dysponowanie informacjami na temat życia prywatnego pasażerów lotniczych przez okres, który Trybunał zakwalifikował już jako szczególnie długi w swojej opinii 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r. (EU:C:2017:592, pkt 132).

110 Biorąc pod uwagę powszechność korzystania z transportu lotniczego, taki okres zatrzymywania skutkuje tym, że dla znacznej części populacji Unii jest prawdopodobne, iż jej dane PNR mogą być zatrzymywane, w sposób powtarzalny, w ramach systemu wprowadzonego dyrektywą PNR i tym samym dostępne na potrzeby analiz wykonywanych przez JIP i właściwe organy w toku wstępnych i późniejszych ocen przez okres znaczny, a nawet nieokreślony – w stosunku do osób, które podróżują samolotem częściej niż raz na pięć lat.

111 Mając na względzie całość powyższych rozważań, należy stwierdzić, że dyrektywa PNR przewiduje istotną ingerencję w prawa zagwarantowane w art. 7 i 8 karty, w szczególności z tego względu, że zmierza do stworzenia systemu ciągłego nadzoru, nieukierunkowanego i systematycznego, zakładającego zautomatyzowane przetwarzanie danych osobowych wszystkich osób korzystających z usług transportu lotniczego.

2. W przedmiocie uzasadnienia ingerencji wynikającej z dyrektywy PNR

112 Należy przypomnieć, że prawa podstawowe zagwarantowane w art. 7 i 8 karty nie stanowią prerogatyw o charakterze absolutnym, lecz należy je rozważać z uwzględnieniem ich funkcji społecznej [opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 136 i przytoczone tam orzecznictwo; wyrok z dnia 6 października 2020 r., Privacy International, C-623/17, EU:C:2020:790, pkt 63 i przytoczone tam orzecznictwo].

113 Zgodnie z art. 52 ust. 1 zdanie pierwsze karty wszelkie ograniczenia w korzystaniu z uznanych w niej praw i wolności muszą być przewidziane ustawą i szanować ich istotę. Zgodnie z art. 52 ust. 1 zdanie drugie karty, z zastrzeżeniem zasady proporcjonalności, 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. W tym względzie art. 8 ust. 2 karty wskazuje, że dane osobowe powinny w szczególności być przetwarzane „w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą”.

114 Należy przypomnieć, że wymóg, zgodnie z którym wszelkie ograniczenia korzystania z praw podstawowych muszą być przewidziane ustawą, oznacza, że podstawa prawna, która pozwala na ingerencję w te prawa, musi sama określać zakres ograniczenia wykonywania danego prawa, przy czym, z jednej strony, wymaganie to nie wyklucza, by to ograniczenie było sformułowane w sposób wystarczająco otwarty, tak aby można je było dostosować do zmieniających się sytuacji (zob. podobnie wyrok z dnia 26 kwietnia 2022 r., Polska/Parlament i Rada, C-401/19, EU:C:2022:297, pkt 64, 74 i przytoczone tam orzecznictwo), a z drugiej strony, Trybunał może, w stosownym przypadku, doprecyzować poprzez wykładnię konkretny zakres ograniczenia, z punktu widzenia zarówno samego brzmienia rozpatrywanych przepisów Unii, jak i ich ogólnej systematyki oraz celów, którym służą, zinterpretowanym w świetle praw podstawowych gwarantowanych w karcie.

115 Jeśli chodzi o poszanowanie zasady proporcjonalności, ochrona prawa podstawowego do poszanowania życia prywatnego na poziomie Unii, zgodnie z utrwalonym orzecznictwem Trybunału wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia mieściły się w ramach tego, co ściśle niezbędne. Ponadto nie można dążyć do celu interesu ogólnego bez

uwzględnienia okoliczności, że należy pogodzić go z prawami podstawowymi, których dotyczy środek, dokonując zbilansowanego wyważenia między celem interesu ogólnego z jednej strony, a rozpatrywanymi prawami z drugiej strony [opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 140; wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 52 i przytoczone tam orzecznictwo].

116 Konkretniej rzecz ujmując, możliwość uzasadnienia przez państwa członkowskie ograniczenia praw i obowiązków przewidzianych w art. 7 i 8 karty należy oceniać, badając wagę ingerencji, jaką stanowi takie ograniczenie, oraz sprawdzając, czy znaczenie celu interesu ogólnego, któremu służy to ograniczenie, pozostaje w relacji do tej wagi (zob. podobnie wyroki: z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 55 i przytoczone tam orzecznictwo; z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 53 i przytoczone tam orzecznictwo).

117 By zadośćuczynić wymogowi proporcjonalności, dane uregulowanie Unii powinno zawierać jasne i precyzyjne reguły dotyczące zakresu i sposobu stosowania rozpatrywanych środków, a także ustanawiać minimalne zabezpieczenia służące temu, aby osoby, których dane zostały przekazane, miały wystarczające gwarancje rzeczywistej ochrony swoich danych osobowych przed ryzykiem nadużyć. Powinno ono w szczególności wskazywać, w jakich okolicznościach i pod jakimi warunkami może zostać przyjęty środek przewidujący przetwarzanie takich danych, gwarantując w ten sposób, że ingerencja będzie ograniczona do tego, co ściśle konieczne. Konieczność posiadania takich gwarancji jest jeszcze bardziej istotna, gdy dane osobowe są przetwarzane w sposób zautomatyzowany. Te względy mają znaczenie w szczególności, gdy dane PNR mogą ujawniać informacje szczególnie chronione dotyczące pasażerów [opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 141; 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, pkt 132 i przytoczone tam orzecznictwo].

118 Zatem uregulowanie przewidujące zatrzymywanie danych osobowych powinno zawsze spełniać obiektywne kryteria wykazujące związek między danymi podlegającymi zatrzymaniu a zamierzonym celem [zob. podobnie opinia 1/15 (umowa PNR UE–Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 191 i przytoczone tam orzecznictwo; wyroki: z dnia 3 października 2019 r., A. i in., C-70/18, EU:C:2019:823, pkt 63; 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, pkt 133].

a) W przedmiocie poszanowania zasady legalności oraz istoty rozpatrywanych praw podstawowych

119 Ograniczenie w wykonywaniu praw podstawowych, o których mowa w art. 7 i 8 karty, wynikające z systemu wprowadzonego dyrektywą PNR zostało przewidziane aktem prawa Unii. Co do kwestii, czy zgodnie z orzecznictwem przypomnianym w pkt 114 niniejszego wyroku dyrektywa ta, jako akt prawa Unii zezwalający na ingerencję w przedmiotowe prawa, sama określa zakres ograniczenia wykonywania tych praw, należy zauważyć, że przepisy tej dyrektywy, tak samo jak załączniki I i II do niej, formułują, z jednej strony, listę danych PNR, a z drugiej strony, tworzą ramy przetwarzania tych danych, w szczególności określając cele i sposoby tego przetwarzania. Ponadto ta kwestia jest w znacznej mierze związana z poszanowaniem wymogu proporcjonalności, który został przypomniany w pkt 117 niniejszego wyroku (zob. podobnie wyrok z dnia 16 lipca 2020 r., Facebook Ireland i Schrems, C-311/18, EU:C:2020:559, pkt 180) i zostanie zbadany w pkt 125 i nast. niniejszego wyroku.

120 Co do poszanowania istoty praw podstawowych, o których mowa w art. 7 i 8 karty, jest prawdą, że dane PNR mogą, w odpowiednich przypadkach, zawierać bardzo konkretne informacje na temat życia prywatnego danej osoby. Jednakże w zakresie, w jakim, z jednej strony, charakter tych informacji jest ograniczony do niektórych aspektów życia prywatnego, dotyczących w szczególności podróży lotniczych danej osoby, a z drugiej strony, dyrektywa PNR wprost zabrania, w swoim art. 13 ust. 4, przetwarzania danych szczególnie chronionych w rozumieniu art. 9 ust. 1 RODO, dane, których dotyczy ta dyrektywa, nie pozwalają, same w sobie, ujawnić całokształtu życia prywatnego danej osoby. Co więcej, dyrektywa ta wyznacza, w swoim art. 1 ust. 2 w związku z art. 3 pkt 8 i 9 oraz załącznikiem II, cele przetwarzania omawianych danych. Wreszcie dyrektywa ta formułuje w art. 4–15 normy regulujące przekazywanie, przetwarzanie i zatrzymywanie wskazanych danych, jak również normy zmierzające do zapewnienia, w szczególności, bezpieczeństwa, poufności oraz integralności tych danych oraz ochrony przed nielegalnym dostępem do nich i ich nielegalnym przetwarzaniem. W związku z powyższym ingerencja, którą zakłada dyrektywa PNR, nie stanowi zagrożenia dla istoty praw podstawowych zagwarantowanych w art. 7 i 8 karty.

b) W zakresie celu interesu ogólnego oraz przydatności przetwarzania danych PNR w świetle tego celu

121 Co do kwestii, czy system wprowadzony dyrektywą PNR realizuje cel interesu ogólnego, z motywów 5, 6 i 15 tej dyrektywy wynika, że jej celem jest ochrona bezpieczeństwa wewnętrznego Unii oraz ochrona życia i bezpieczeństwa osób, przy jednoczesnym stworzeniu ram prawnych gwarantujących podwyższony poziom ochrony praw podstawowych pasażerów, w szczególności ich prawa do poszanowania życia prywatnego oraz ochrony danych osobowych podczas przetwarzania danych PNR przez właściwe organy.

122 W tym względzie art. 1 ust. 2 dyrektywy PNR stanowi, że dane PNR, gromadzone zgodnie z tą dyrektywą, mogą być przetwarzane wyłącznie w celach przewidzianych w art. 6 ust. 2 lit. a)–c) tej dyrektywy, to jest w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości oraz ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania. Cele te służą niewątpliwie interesowi ogólnemu Unii i mogą uzasadniać ingerencję, nawet istotną, w prawa podstawowe, o których mowa w art. 7 i 8 karty [zob. podobnie wyrok z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 42; opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 148, 149].

123 W zakresie przydatności systemu wprowadzonego dyrektywą PNR do realizowania założonych celów, należy stwierdzić, że o ile możliwość wyników „fałszywie negatywnych” oraz dość znaczna liczba wyników „fałszywie pozytywnych”, które – jak wspomniano w pkt 106 niniejszego wyroku – zostały uzyskane w latach 2018 i 2019 w następstwie przetwarzania zautomatyzowanego, przewidzianego przez tę dyrektywę, mogą ograniczać przydatność systemu, o tyle nie czynią systemu niezdatnym do realizowania celu zmierzającego do zwalczania przestępstw terrorystycznych i poważnej przestępczości. A zatem, jak wynika również z dokumentu roboczego Komisji wspomnianego w pkt 106 niniejszego wyroku, przetwarzanie zautomatyzowane dokonywane na mocy przedmiotowej dyrektywy pozwoliło już w sposób skuteczny zidentyfikować pasażerów lotniczych stanowiących ryzyko w ramach zwalczania przestępstw terrorystycznych i poważnej przestępczości.

124 Ponadto, biorąc pod uwagę odsetek błędów wynikających ze zautomatyzowanego przetwarzania danych PNR, a zwłaszcza utrzymującą się znaczną liczbę wyników „fałszywie pozytywnych”, przydatność systemu wprowadzonego dyrektywą PNR zależy zasadniczo od dobrego

funkcjonowania następczej weryfikacji wyników uzyskanych w ramach takiego przetwarzania – poprzez zastosowanie środków niezautomatyzowanych, co jest zadaniem, które dyrektywa wyznacza JIP. Przepisy, przewidziane w tym zakresie przez dyrektywę PNR, służą zatem realizacji wskazanych celów.

c) W przedmiocie koniecznego charakteru ingerencji wynikających z dyrektywy PNR

125 Zgodnie z orzecznictwem przypomnianym w pkt 115–118 niniejszego wyroku należy zbadać, czy ingerencja wynikająca z dyrektywy PNR ogranicza się do tego co ściśle niezbędne, a w szczególności, czy dyrektywa ta zawiera jasne i precyzyjne normy, które regulują zakres i sposób stosowania środków, jakie przewiduje, oraz czy system, który tworzy, nadal odpowiada obiektywnym kryteriom, określając związek między danymi PNR, które są ściśle powiązane z rezerwacją i realizacją podróży lotniczych a celami, którym ma służyć dyrektywa, a mianowicie zwalczaniem przestępstw terrorystycznych i poważnej przestępczości.

1) W przedmiocie danych pasażerów lotniczych wskazanych w dyrektywie PNR

126 Należy zbadać, czy wykazy danych znajdujące się w załączniku I do dyrektywy PNR, określają w sposób jasny i precyzyjny dane PNR, które przewoźnik lotniczy ma obowiązek ujawnić JIP.

127 Tytułem wstępu należy przypomnieć, że jak wynika, między innymi, z motywu 15 dyrektywy PNR, prawodawca Unii uznał, że wykaz danych PNR przekazywanych JIP należy sporządzać „w taki sposób, by czynił on zadość zarówno uzasadnionym potrzebom organów publicznych w związku z zapobieganiem przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywaniem, prowadzeniem postępowań przygotowawczych w ich sprawie i ich ściganiem, przyczyniając się tym samym do poprawy bezpieczeństwa wewnętrznego w Unii, jak również ochronie praw podstawowych, w szczególności prawa do prywatności i ochrony danych osobowych”. Zgodnie z tym samym motywem dane PNR „powinny zawierać wyłącznie informacje dotyczące rezerwacji i tras podróży danego pasażera, które umożliwią właściwym organom identyfikację pasażerów lotniczych stanowiących zagrożenie dla bezpieczeństwa wewnętrznego”. Ponadto dyrektywa PNR, w swoim art. 13 ust. 4 zdanie pierwsze, zabrania „przetwarzania danych PNR ujawniających rasę lub pochodzenie etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, stan zdrowia, życie seksualne lub orientację seksualną danej osoby”.

128 A zatem dane PNR gromadzone i ujawniane zgodnie z załącznikiem I do dyrektywy PNR powinny mieć bezpośredni związek z realizowanym lotem oraz danym pasażerem i muszą być ograniczone w ten sposób, by, z jednej strony, czynić zadość uzasadnionym potrzebom organów publicznych w przedmiocie zapobiegania i wykrywania przestępstw terrorystycznych i poważnej przestępczości, a także prowadzenia postępowań przygotowawczych i ścigania w tym zakresie, a z drugiej strony, by nie obejmować danych szczególnie chronionych.

129 Tymczasem rubryki 1–4, 7, 9, 11, 15, 17 i 19 załącznika I do dyrektywy PNR odpowiadają tym wymogom, podobnie jak wymogom jasności i precyzji, ponieważ zawierają informacje jednoznacznie możliwe do określenia i o oznaczonym zakresie, odnoszące się bezpośrednio do wykonanego lotu i danego pasażera. Jak podniósł rzecznik generalny w pkt 165 opinii, tak jest również w przypadku rubryk 10, 13, 14 i 16 pomimo ich otwartego brzmienia.

130 Z kolei rubryki 5, 6, 8, 12 i 18 wymagają wyjaśnienia w celu ich wykładni.

131 Co się tyczy rubryki 5, która zawiera „adres i dane kontaktowe (numer telefonu, adres e-mail)", ta rubryka nie precyzuje, czy adres i dane kontaktowe dotyczą jedynie pasażera lotniczego czy również osób trzecich dokonujących rezerwacji lotu dla tego pasażera, osób trzecich, za których pośrednictwem można się z nim skontaktować, czy wreszcie osób trzecich, które powinny zostać powiadomione w nagłym wypadku. Jednakże, jak zasadniczo wskazał rzecznik generalny w pkt 162 opinii, biorąc pod uwagę wymogi jasności i precyzji, ta rubryka nie może być interpretowana jako zezwalająca, w sposób dorozumiany, na zbieranie i przetwarzanie danych osobowych również tych osób trzecich. Tym samym brzmienie tej rubryki należy interpretować w ten sposób, że dotyczy ona jedynie adresu i danych kontaktowych, to jest numeru telefonu oraz adresu e-mail pasażera lotniczego, na którego nazwisko dokonywana jest rezerwacja.

132 W zakresie rubryki 6, która zawiera „wszystkie informacje o formie płatności, w tym adres na fakturze", musi być ona interpretowana tak, by spełniać wymagania jasności i precyzji, a zatem może dotyczyć jedynie informacji związanych z formą płatności i fakturą za bilet lotniczy, z pominięciem wszelkich innych informacji niemających bezpośredniego związku z lotem [zob. analogicznie opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 159].

133 Jeśli chodzi o rubrykę 8, która obejmuje „informacje dotyczące programów lojalnościowych", jak wskazał rzecznik generalny w pkt 164 opinii, powinna być ona interpretowana jako odnosząca się jedynie do danych związanych ze statusem danego pasażera w kontekście programów lojalnościowych danej linii lotniczej lub grupy linii lotniczych oraz do numeru identyfikacyjnego tego pasażera jako „często korzystającego z lotów". Rubryka 8 nie pozwala zatem na zbieranie informacji dotyczących transakcji, dzięki którym tenże status został przyznany.

134 Co się tyczy rubryki 12, zawiera ona „uwagi ogólne (w tym wszelkie dostępne informacje o osobach małoletnich bez opieki w wieku poniżej 18 lat, takie jak: imię i nazwisko, płeć, wiek, języki, którymi włada, imię i nazwisko oraz dane kontaktowe opiekuna w momencie odlotu i rodzaj więzi łączącej go z osobą małoletnią, imię i nazwisko oraz dane kontaktowe opiekuna w momencie lądowania i rodzaj więzi łączącej go z osobą małoletnią, przedstawiciel obecny przy odlocie i przylocie)".

135 W tym względzie należy od razu podnieść, że wyrażenie „uwagi ogólne" nie odpowiada wymogom jasności i precyzji, jako że nie zawiera, samo w sobie, żadnego ograniczenia, jeśli chodzi o charakter i zakres informacji, które mogą być gromadzone i ujawniane JIP na podstawie rubryki 12 [zob. podobnie opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 160], przy czym wykaz, który znajduje się w nawiasie, spełnia, jako taki, przedmiotowe wymogi.

136 Tym samym, aby zinterpretować rubrykę 12, przy zastosowaniu orzecznictwa przypomnianego w pkt 86 niniejszego wyroku, jako zgodną z wymogami jasności i precyzji, a szerzej, z art. 7 i 8 oraz art. 52 ust. 1 karty, należy uznać, że dopuszczalne jest zbieranie i ujawnienie jedynie informacji wprost wymienionych w tej rubryce, którymi są: imię i nazwisko, płeć osoby małoletniej, jej wiek, języki, którymi włada, imię i nazwisko oraz dane kontaktowe opiekuna w momencie odlotu i rodzaj więzi łączącej go z osobą małoletnią, imię i nazwisko oraz dane kontaktowe opiekuna w momencie lądowania i rodzaj więzi łączącej go z osobą małoletnią, przedstawiciel obecny przy odlocie i przylocie.

137 Z kolei rubryka 18 zawiera: „wszelkie zebrane dane pasażera przekazane przed podróżą (dane API) (w tym rodzaj, numer, kraj wydania i data ważności dokumentu tożsamości, obywatelstwo, nazwisko, imię, płeć, data urodzenia, linia lotnicza, numer lotu, data odlotu, data przylotu, port lotniczy odlotu, port lotniczy przylotu, godzina odlotu i godzina przylotu)".

138 Jak zauważył co do istoty rzecznik generalny w pkt 156–160 swojej opinii, z rubryki 18, wykładanej w świetle motywów 4 i 9 dyrektywy PNR, wynika, że informacje, do których się odnosi, są tożsame z danymi API wskazanymi w tej rubryce oraz w art. 3 ust. 2 dyrektywy API.

139 Również rubryka 18, pod warunkiem jej interpretacji jako zawierającej jedynie informacje wprost wskazane w niej oraz w art. 3 ust. 2 dyrektywy API, może zostać uznana za odpowiadającą wymogom jasności i precyzji [zob. analogicznie opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 161].

140 A zatem należy stwierdzić, że załącznik I do dyrektywy PNR, interpretowany zgodnie z motywami wskazanymi w szczególności w pkt 130–139 niniejszego wyroku, jest, jako całość, sformułowany w sposób wystarczająco jasny i precyzyjny, ograniczając zakres ingerencji w prawa podstawowe wyrażone w art. 7 i 8 karty.

2) W przedmiocie celów przetwarzania danych PNR

141 Jak wynika z art. 1 ust. 2 dyrektywy PNR, przetwarzanie danych PNR gromadzonych zgodnie z tą dyrektywą ma na celu zwalczanie „przestępstw terrorystycznych" i „poważnej przestępczości".

142 Co się tyczy kwestii, czy dyrektywa PNR zawiera w tej materii jasne i precyzyjne uregulowania, które ograniczają zastosowanie systemu utworzonego na jej podstawie do tego, co ściśle konieczne w zakresie wskazanych celów, należy zauważyć, z jednej strony, że pojęcie „przestępstwa terrorystyczne" zostało zdefiniowane w art. 3 pkt 8 tej dyrektywy poprzez odniesienie do „przestępstw określonych zgodnie z prawem krajowym, o których mowa w art. 1–4 decyzji ramowej [2002/475]".

143 Tymczasem poza tym, że ta decyzja ramowa określała w swoich art. 1–3 w sposób jasny i precyzyjny „przestępstwa terrorystyczne", „przestępstwa dotyczące grupy terrorystycznej" oraz „przestępstwa związane z działalnością terrorystyczną", które państwa członkowskie muszą penalizować jako przestępstwa karne na podstawie tejże decyzji ramowej, dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475 oraz zmieniająca decyzję Rady 2005/671/WSiSW (Dz.U. 2017, L 88, s. 6), w art. 3–14, również definiuje w sposób jasny i precyzyjny te same przestępstwa.

144 Z drugiej strony, art. 3 pkt 9 dyrektywy PNR zawiera definicję pojęcia „poważnej przestępczości", które oznacza „przestępstwa wymienione w załączniku II [do tej dyrektywy], które na mocy prawa krajowego państwa członkowskiego podlegają karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności o maksymalnym wymiarze co najmniej trzech lat".

145 Tymczasem przede wszystkim załącznik ten wymienia w sposób wyczerpujący różne kategorie przestępstw mogących stanowić „poważne przestępstwa", o których mowa w art. 3 pkt 9 dyrektywy PNR.

146 Następnie, biorąc pod uwagę specyfikę, jaką charakteryzują się, w chwili przyjęcia wspomnianej dyrektywy, systemy karne państw członkowskich, przy braku harmonizacji w zakresie przestępstw tam wskazanych, prawodawca Unii mógł ograniczyć się do określenia kategorii przestępstw, nie definiując ich elementów konstytutywnych, tym bardziej że te elementy są, w założeniu, wystarczająco określone przez prawo krajowe, do którego odsyła art. 3 pkt 9 dyrektywy PNR, jako że państwa członkowskie są zobowiązane do poszanowania zasady ustawowej określoności czynów zabronionych i kar jako składnika dzielonej z Unią wspólnej wartości państwa prawnego, o której mowa w art. 2 TUE (zob. analogicznie wyrok z dnia 16 lutego 2022 r., Węgry/Parlament i Rada, C-156/21, EU:C:2022:97, pkt 136, 160, 234), zasady, o której mowa również w art. 49 ust. 1 karty, a której państwa członkowskie są zobowiązane przestrzegać podczas wprowadzania w życie aktu Unii takiego jak dyrektywa PNR (zob. podobnie wyrok z dnia 10 listopada 2011 r., QB, C-405/10, EU:C:2011:722, pkt 48 i przytoczone tam orzecznictwo). Biorąc pod uwagę również zwyczajowe rozumienie wyrażeń, którymi posłużono się w przedmiotowym załączniku, należy uznać, że on sam określa w sposób wystarczająco jasny i precyzyjny przestępstwa mogące stanowić poważną przestępczość.

147 Jest prawdą, że pkt 7, 8, 10 i 16 załącznika II wymieniają bardzo ogólne kategorie przestępstw (oszustwo, pranie pieniędzy i fałszowanie pieniędzy, poważne przestępstwa przeciwko środowisku, nielegalny handel dobrami kultury), odnosząc się jednak do poszczególnych przestępstw z tych ogólnych kategorii. Celem zapewnienia wystarczającej precyzji wymaganej także przez art. 49 karty, punkty te powinny być interpretowane jako odnoszące się do tych przestępstw, tak jak są określone w prawie krajowym lub prawie Unii w tym zakresie. Te punkty, zinterpretowane w opisany sposób, mogą być uznane za spełniające wymogi jasności i precyzji.

148 Wreszcie należy przypomnieć, że zgodnie z zasadą proporcjonalności cel w postaci zwalczania poważnej przestępczości może uzasadniać istotną ingerencję w prawa podstawowe, zagwarantowane w art. 7 i 8 karty, którą zakłada dyrektywa PNR, przy czym inaczej rzecz się ma ze zwalczaniem przestępczości jako takiej, ponieważ taki cel może uzasadniać jedynie ingerencję, która nie jest istotna (zob. analogicznie wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 59 i przytoczone tam orzecznictwo). Rozpatrywana dyrektywa powinna zapewniać również, poprzez użycie jasnych i precyzyjnych norm, by system nią wprowadzony był stosowany jedynie do poważnych przestępstw, a nie do przestępstw zwyczajnych.

149 W tym względzie, jak podniósł rzecznik generalny w pkt 121 opinii, liczne przestępstwa wskazane w załączniku II do dyrektywy PNR, takie jak: handel ludźmi, wykorzystywanie seksualne dzieci i pornografia dziecięca, handel bronią i materiałami wybuchowymi, pranie brudnych pieniędzy, cyberprzestępczość, handel organami i tkankami ludzkimi, handel środkami odurzającymi i substancjami psychotropowymi, handel materiałami jądrowymi i radioaktywnymi, bezprawne zawładnięcie statkiem powietrznym lub statkiem, poważne przestępstwa podlegające jurysdykcji Międzynarodowego Trybunału Karnego, zabójstwo, gwałt, porwanie, porwanie dla okupu – są ze względu na swoją naturę w sposób niezaprzeczalny przestępstwami poważnymi.

150 Ponadto, o ile inne przestępstwa również wskazane w załączniku II trudniej jest, co do zasady, uznać za poważną przestępczość, z samego brzmienia art. 3 pkt 9 dyrektywy PNR wynika jednak, że przestępstwa te mogą być uznawane za poważne jedynie wtedy, gdy w danym państwie członkowskim podlegają karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności o maksymalnym wymiarze co najmniej trzech lat. Wymogi wynikające z tego przepisu, odnoszące się do charakteru i surowości stosowanej kary, mają na celu, co do zasady, ograniczyć zastosowanie systemu utworzonego na mocy dyrektywy

do przestępstw wystarczająco poważnych, by uzasadnić ingerencję w prawa podstawowe zagwarantowane w art. 7 i 8 karty, wynikającą z systemu ustanowionego na mocy tej samej dyrektywy.

151 Jednakże, wobec tego, że art. 3 pkt 9 dyrektywy PNR odnosi się nie do minimalnego, a do maksymalnego wymiaru kary, nie jest wykluczone, że dane PNR mogą być przetwarzane w celu zwalczania przestępstw, które, mimo że spełniają kryteria określone we wskazanym przepisie co do swojej wagi, stanowią – ze względu na specyfikę krajowego systemu karnego – nie przestępstwa poważne, a zwyczajne.

152 W związku z tym to do państw członkowskich należy zapewnienie, by system ustanowiony na podstawie dyrektywy PNR był rzeczywiście stosowany jedynie do zwalczania poważnej przestępczości oraz by nie obejmował zwyczajnych przestępstw.

3) W przedmiocie powiązania pomiędzy danymi PNR a celami przetwarzania tych danych

153 Jest prawdą, jak wskazał co do istoty rzecznik generalny w pkt 119 opinii, że brzmienie art. 3 pkt 8 oraz art. 3 pkt 9 dyrektywy PNR, w związku z jej załącznikiem II, nie odnosi się wprost do kryterium mogącego zawęzić zakres stosowania tej dyrektywy jedynie do tych przestępstw, które ze względu na swój charakter mogą mieć, choćby nie w sposób bezpośredni, obiektywny związek z podróżami lotniczymi i tym samym z kategoriami danych przekazywanych, przetwarzanych i zatrzymywanych na podstawie wspomnianej dyrektywy.

154 Jednakże, jak zauważył rzecznik generalny w pkt 121 opinii, niektóre przestępstwa wskazane w załączniku II do dyrektywy PNR, takie jak handel ludźmi, handel środkami odurzającymi lub bronią, ułatwienie nielegalnego wjazdu i pobytu czy bezprawne zawładnięcie statkiem powietrznym mogą mieć ze względu na swój charakter bezpośredni związek z przewozem lotniczym pasażerów. Podobnie rzecz się ma z niektórymi przestępstwami terrorystycznymi, takimi jak spowodowanie rozległych zniszczeń systemu transportowego czy przygotowanie do zajęcia statku powietrznego, które zostały wymienione w art. 1 ust. 1 lit. d) i e) decyzji ramowej 2002/475, a do których odsyła art. 3 pkt 8 dyrektywy PNR, a także podejmowanie, organizowanie lub ułatwianie podróżowania w celach terrorystycznych, o których to przestępstwach mowa w art. 9 i 10 dyrektywy 2017/541.

155 W tym kontekście należy przypomnieć, że Komisja uzasadniła swój wniosek z dnia 2 lutego 2011 r. dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie wykorzystania danych dotyczących przelotu pasażera w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania [COM(2011) 32 wersja ostateczna], na którym została oparta dyrektywa PNR, podkreślając, iż „ataki terrorystyczne na Stany Zjednoczone w 2001 r., powstrzymany atak terrorystyczny w sierpniu 2006 r., zmierzający do wysadzenia szeregu samolotów zmierzających ze Zjednoczonego Królestwa do Stanów Zjednoczonych, oraz próba ataku terrorystycznego na pokładzie samolotu z Amsterdamu do Detroit w grudniu 2009 r. ukazały możliwości terrorystów, jeżeli chodzi o przygotowanie ataków wymierzonych w samoloty odbywające przeloty międzynarodowe, w dowolnym państwie” oraz że „większość działań terrorystycznych ma charakter transgraniczny i wiąże się z podróżami międzynarodowymi, między innymi do obozów szkoleniowych zlokalizowanych poza UE”. Ponadto, aby umotywować konieczność analizy danych PNR celem zwalczania poważnej przestępczości, Komisja przywołała, tytułem przykładów, przypadek handlarzy ludźmi, którzy posługiwali się fałszywymi dokumentami, aby dokonać odprawy na lot, oraz przypadek siatki handlarzy ludźmi i narkotykami, która celem sprowadzenia

narkotyków do szeregu miejsc w Europie wykorzystywała osoby, które same były ofiarami handlu ludźmi i nabywała bilety lotnicze dla tych osób przy użyciu skradzionych kart kredytowych. Te przypadki dotyczyły przestępstw mających bezpośredni związek z lotniczym przewozem pasażerów, jako że chodziło o czyny skierowane przeciwko tymże przewozom oraz o czyny popełniane podczas podróży samolotem lub czyny, do których taka podróż się przyczyniała.

156 Poza tym należy stwierdzić, że nawet jeśli przestępstwa nie mają takiego bezpośredniego związku z lotniczym przewozem pasażerów, mogą mieć w danych okolicznościach pośredni związek z tym przewozem. Dzieje się tak w szczególności wtedy, gdy transport lotniczy służy jako środek do przygotowania takich przestępstw lub do uniknięcia skutków karnych ich popełnienia. Z kolei przestępstwa całkowicie pozbawione obiektywnego związku, choćby pośredniego, z lotniczym przewozem pasażerów nie mogą uzasadniać zastosowania systemu wprowadzonego dyrektywą PNR.

157 W związku z powyższym art. 3 pkt 8 i 9 omawianej dyrektywy, w związku z jej załącznikiem II oraz w świetle wymogów wynikających z art. 7 i 8 oraz art. 52 ust. 1 karty, wymaga, by państwa członkowskie czuwały nad tym, by w szczególności w trakcie indywidualnej oceny przeprowadzanej w sposób niezautomatyzowany, o której mowa w art. 6 ust. 5 owej dyrektywy, stosowanie systemu ustanowionego na jej mocy ograniczało się do przestępstw terrorystycznych i poważnych przestępstw, które mają obiektywny, choćby i pośredni, związek z lotniczym przewozem pasażerów.

4) W przedmiocie pasażerów lotniczych i konkretnych lotów

158 System wprowadzony dyrektywą PNR obejmuje dane wszystkich osób, które spełniają definicję „pasażera” w rozumieniu art. 3 pkt 4 tej dyrektywy i odbywają loty wchodzące w jej zakres stosowania.

159 Zgodnie z art. 8 ust. 1 wspomnianej dyrektywy dane te są przekazywane JIP państwa członkowskiego, na którego terytorium nastąpi przylot lub z którego terytorium nastąpi odlot, niezależnie od jakichkolwiek przesłanek pozwalających na uznanie, że określeni pasażerowie mogą stanowić ryzyko związane z przestępstwami terrorystycznymi lub poważną przestępczością. Dane w ten sposób przekazane są poddawane zautomatyzowanemu przetwarzaniu w ramach wstępnej oceny na mocy art. 6 ust. 2 lit. a) i art. 6 ust. 3 dyrektywy PNR, a ocena ta ma na celu, jak wynika z motywu 7 tej dyrektywy, identyfikację osób, które przed dokonaniem takiego sprawdzenia nie były podejrzewane o udział w przestępstwach terrorystycznych lub w poważnej przestępczości i które powinny być poddane dalszemu sprawdzeniu przez właściwe organy.

160 W szczególności z art. 1 ust. 1 lit. a) oraz art. 2 dyrektywy PNR wynika, że rozróżnia ona pasażerów odbywających loty pozaunijne, wykonywane pomiędzy Unią i państwami trzecimi oraz odbywających loty wewnątrzunijne, wykonywane pomiędzy różnymi państwami członkowskimi.

161 Jeśli chodzi o pasażerów lotów pozaunijnych, należy przypomnieć, że w odniesieniu do pasażerów odbywających loty między Unią i Kanadą Trybunał orzekł już, że zautomatyzowane przetwarzanie danych przed przybyciem pasażerów do Kanady ułatwia i przyspiesza kontrole, zwłaszcza na granicach. Ponadto wyłączenie określonych kategorii osób lub określonych stref pochodzenia mogłoby stanowić przeszkodę dla realizacji celu zautomatyzowanego przetwarzania danych PNR, którym jest zidentyfikowanie, poprzez weryfikację tych danych, osób mogących stanowić

zagrożenie dla bezpieczeństwa publicznego wśród ogółu pasażerów lotniczych, oraz mogłoby umożliwić obejście tego sprawdzenia [zob. podobnie opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 187].

162 Te ustalenia mogą tymczasem zostać zastosowane mutatis mutandis do sytuacji pasażerów odbywających loty między Unią i wszystkimi innymi państwami trzecimi, których państwa członkowskie mają obowiązek poddać systemowi stworzonemu przez dyrektywę PNR, zgodnie z art. 1 ust. 1 lit. a) tej dyrektywy, w związku z jej art. 3 pkt 2 i 4. A zatem przetwarzanie i wstępna ocena danych PNR pasażerów lotniczych przybywających do Unii i ją opuszczających nie może być ograniczona do określonego kręgu pasażerów lotniczych, biorąc pod uwagę charakter zagrożeń dla porządku publicznego mogący wynikać z przestępstw terrorystycznych i poważnej przestępczości, które mają obiektywny związek, choćby pośredni, z lotniczym przewozem pasażerów między Unią i państwami trzecimi. Należy zatem stwierdzić, że konieczny związek między tymi danymi i celem w postaci walki ze wskazanymi przestępstwami istnieje, co oznacza, że dyrektywa PNR nie wykracza poza to, co ściśle konieczne tylko dlatego, że nakłada na państwa członkowskie obowiązek systematycznego przekazywania i wstępnej oceny danych PNR wszystkich pasażerów.

163 Jeśli chodzi o pasażerów odbywających loty między różnymi państwami członkowskimi Unii, art. 2 ust. 1 dyrektywy PNR, w związku z jej motywem 10, wprowadza jedynie w odniesieniu do państw członkowskich możliwość rozszerzenia stosowania systemu wprowadzonego dyrektywą na loty wewnątrzunijne.

164 Zatem prawodawca Unii nie zamierzał nałożyć na państwa członkowskie obowiązku objęcia systemem wprowadzonym dyrektywą PNR lotów wewnątrzunijnych, ale, jak wynika z art. 19 ust. 3 tej dyrektywy, pozostawił im decyzję w zakresie takiego rozszerzenia, zakładając, że powinna być ona poprzedzona szczegółową oceną jej skutków prawnych, w szczególności wpływu na prawa podstawowe zainteresowanych osób.

165 W tym względzie należy zauważyć, że, wskazując, iż sprawozdanie z przeglądu Komisji, o którym mowa w art. 19 ust. 1 dyrektywy PNR „zawiera również przegląd konieczności, proporcjonalności i skuteczności włączenia do zakresu stosowania niniejszej dyrektywy obowiązkowego zbierania i przekazywania danych PNR w odniesieniu do wszystkich lub wybranych lotów wewnątrzunijnych” oraz, że w związku z tym musi brać pod uwagę „doświadczenia państw członkowskich, zwłaszcza tych, które stosują niniejszą dyrektywę do lotów wewnątrzunijnych zgodnie z art. 2”, art. 19 ust. 3 tej dyrektywy potwierdza, że według prawodawcy Unii system wprowadzony dyrektywą PNR nie musi być koniecznie rozszerzony na loty wewnątrzunijne.

166 Z tych samych powodów art. 2 ust. 3 dyrektywy PNR wskazuje, że państwa członkowskie mogą zdecydować o zastosowaniu tej dyrektywy tylko do niektórych lotów wewnątrzunijnych, jeśli uznają to za konieczne dla realizacji jej celów, przy czym mogą zmienić zakres tych lotów w każdym czasie.

167 W każdym razie uprawnienie państw członkowskich do rozszerzenia zastosowania systemu wprowadzonego dyrektywą PNR na loty wewnątrzunijne musi odbywać się, jak wynika z jej motywu 22, z pełnym poszanowaniem praw podstawowych gwarantowanych w art. 7 i 8 karty. W tym względzie, skoro zgodnie z motywem 19 wspomnianej dyrektywy to do państw członkowskich należy ocena zagrożeń związanych z przestępstwami terrorystycznymi i poważną

przestępczością, to jednak korzystanie z tego uprawnienia zakłada, że podczas przedmiotowej oceny państwa członkowskie stwierdzą istnienie zagrożenia związanego z takimi przestępstwami, które może uzasadniać zastosowanie owej dyrektywy również do lotów wewnątrzunijnych.

168 A zatem państwo członkowskie, które chce skorzystać z uprawnienia przewidzianego w art. 2 dyrektywy PNR, czy to w zakresie wszystkich lotów wewnątrzunijnych na podstawie art. 2 ust. 2, czy też jedynie w zakresie niektórych takich lotów na podstawie art. 2 ust. 3, nie jest zwolnione ze sprawdzenia, czy zastosowanie dyrektywy do wszystkich lub niektórych lotów wewnątrzunijnych jest rzeczywiście niezbędne i proporcjonalne do realizacji celu, o którym mowa w art. 1 ust. 2 tej dyrektywy.

169 Biorąc pod uwagę motywy 5–7, 10 i 22 dyrektywy PNR, takie państwo członkowskie musi zbadać, czy przetwarzanie, o którym mowa w tej dyrektywie, w zakresie danych PNR pasażerów odbywających loty wewnątrzunijne (wszystkie albo tylko niektóre) jest ściśle konieczne, w świetle powagi ingerencji w prawa podstawowe zagwarantowane w art. 7 i 8 karty, dla zapewnienia bezpieczeństwa wewnętrznego Unii lub co najmniej tego państwa członkowskiego oraz dla ochrony życia i bezpieczeństwa ludzi.

170 W odniesieniu w szczególności do zagrożeń związanych z przestępstwami terrorystycznymi, z orzecznictwa Trybunału wynika, że do działalności terrorystycznej zaliczają się czyny mogące poważnie zdestabilizować fundamentalne struktury konstytucyjne, polityczne, ekonomiczne lub społeczne kraju, w szczególności bezpośrednio zagrozić społeczeństwu, ludności lub państwu jako takiemu oraz że pierwszorzędnym interesem każdego państwa członkowskiego jest zapobieganie i ściganie takiej działalności w celu ochrony podstawowych funkcji państwa i podstawowych interesów społeczeństwa ze względu na ochronę bezpieczeństwa narodowego. Takie zagrożenia różnią się – ze względu na swoją specyfikę, wagę i szczególny charakter składających się na nie okoliczności – od ogólnego i stałego ryzyka poważnych przestępstw (zob. podobnie wyroki: 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, pkt 135, 136; z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 61, 62).

171 Zatem w sytuacji, w której zostanie stwierdzone, na podstawie oceny dokonanej przez państwo członkowskie, że istnieją wystarczająco konkretne okoliczności do uznania, że to państwo stoi w obliczu zagrożenia terrorystycznego, które okazuje się rzeczywiste i aktualne lub możliwe do przewidzenia, zastosowanie przez to państwo przez ograniczony okres dyrektywy PNR, na mocy jej art. 2 ust. 1, do wszystkich lotów wewnątrzunijnych rozpoczynających się lub kończących w tym państwie, nie wydaje się wykraczać poza to, co ściśle konieczne. Istnienie takiego zagrożenia samo w sobie może ustanawiać związek pomiędzy, z jednej strony, przetwarzaniem określonych danych oraz, z drugiej strony, zwalczaniem terroryzmu (zob. analogicznie 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, pkt 137).

172 Decyzja o zastosowaniu dyrektywy PNR powinna podlegać skutecznej kontroli sądu lub niezależnego organu administracyjnego, którego decyzja wywiera wiążący skutek, w celu weryfikacji występowania jednej z takich sytuacji oraz poszanowania warunków i gwarancji, jakie należy przewidzieć. Okres stosowania dyrektywy PNR powinien być również ograniczony do tego, co ściśle konieczne, jednak z możliwością przedłużenia w przypadku utrzymywania się tego zagrożenia (zob. analogicznie wyroki: 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, pkt 168; z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 58).

173 Natomiast w przypadku braku rzeczywistego i aktualnego lub możliwego do przewidzenia zagrożenia terrorystycznego, z którym zmaga się dane państwo członkowskie, niezróżnicowane zastosowanie systemu wprowadzonego dyrektywą PNR nie tylko do lotów pozaunijnych, ale także do wszystkich lotów wewnątrzunijnych nie może być uznane za ograniczone do tego, co ściśle konieczne.

174 W takiej sytuacji zastosowanie systemu wprowadzonego dyrektywą PNR do niektórych lotów wewnątrzunijnych powinno być ograniczone do przekazywania i przetwarzania danych PNR dotyczących lotów związanych w szczególności z niektórymi trasami lotniczymi lub planami podróży, lub niektórymi lotniskami, w odniesieniu do których istnieją przesłanki mogące uzasadnić takie zastosowanie. To do danego państwa członkowskiego należy, w takiej sytuacji, wybór lotów wewnątrzunijnych, zgodnie z wynikami oceny, którą ma obowiązek przeprowadzić w oparciu o wymogi wskazane w pkt 163–169 niniejszego wyroku oraz regularne ich przeglądanie pod kątem zmian okoliczności uzasadniających ten wybór, celem zapewnienia, że stosowanie systemu wprowadzonego przez wspomnianą dyrektywę do lotów wewnątrzunijnych jest nadal ograniczone do tego, co ściśle konieczne.

175 Z powyższych rozważań wynika, że powyższa wykładnia art. 2 i art. 3 pkt 4 dyrektywy PNR, w świetle art. 7 i 8 oraz art. 52 ust. 1 karty, jest w stanie zapewnić, że rozpatrywane przepisy mieszczą się w granicach tego, co ściśle konieczne.

5) W przedmiocie wstępnej oceny danych PNR za pomocą zautomatyzowanego przetwarzania

176 Zgodnie z art. 6 ust. 2 lit. a) dyrektywy PNR wstępna ocena ma na celu identyfikację osób, które wymagają dalszego sprawdzenia przez właściwe organy, o których mowa w art. 7 tej dyrektywy, ze względu na możliwość udziału takich osób w przestępstwach terrorystycznych lub w poważnej przestępczości.

177 Ta wstępna ocena przebiega dwuetapowo. W ramach pierwszego etapu JIP danego państwa członkowskiego przeprowadza, zgodnie z art. 6 ust. 3 dyrektywy PNR, zautomatyzowane przetwarzanie danych PNR, zestawiając je z bazami danych lub wcześniej ustalonymi kryteriami. W drugim etapie, w przypadku gdy to zautomatyzowane przetwarzanie da wynik pozytywny (*hit*), jednostka ta przeprowadza, na podstawie art. 6 ust. 5 tej dyrektywy, indywidualną ocenę w sposób niezautomatyzowany w celu ustalenia, czy właściwe organy, o których mowa w art. 7 wspomnianej dyrektywy, powinny podjąć działania zgodnie z prawem krajowym (*match*).

178 Tymczasem, jak zostało przypomniane w pkt 106 niniejszego wyroku, zautomatyzowane przetwarzanie wiąże się zawsze ze znacznym odsetkiem błędów, jako że jest dokonywane na podstawie niezweryfikowanych danych osobowych oraz opiera się ono na ustalonych wcześniej kryteriach.

179 W związku z tym, biorąc pod uwagę konieczność, o której mowa w motywie czwartym preambuły karty, wzmocnienia ochrony praw podstawowych w obliczu rozwoju naukowego i technologicznego, należy zapewnić, na co wskazuje również motyw 20 i art. 7 ust. 6 dyrektywy PNR, by żadna decyzja, która miałaby negatywne skutki prawne dla danej osoby lub znacząco wpływałaby na jej sytuację, nie była podjęta przez właściwe organy wyłącznie na podstawie automatycznego przetwarzania danych PNR. Ponadto, zgodnie z art. 6 ust. 6 tej dyrektywy, JIP może przekazać dane PNR takim organom jedynie po przeprowadzeniu indywidualnej oceny w sposób niezautomatyzowany. Wreszcie, poza tą weryfikacją przeprowadzaną przez JIP oraz same właściwe organy, zgodność z prawem całokształtu przetwarzania zautomatyzowanego

powinna być kontrolowana przez inspektora ochrony danych oraz krajowy organ nadzorczy, zgodnie z art. 6 ust. 7 oraz art. 15 ust. 3 lit. b) wspomnianej dyrektywy, jak również przez sądy krajowe w ramach sądowych środków ochrony prawnej, o których mowa w art. 13 ust. 1 tej samej dyrektywy.

180 Jak podniósł rzecznik generalny w pkt 207 opinii, krajowy organ nadzorczy, inspektor ochrony danych oraz JIP muszą mieć zapewnione środki materialne i osobowe niezbędne do realizowania kontroli, która została im powierzona na mocy dyrektywy PNR. Ponadto jest istotne, by przepisy krajowe dokonujące transpozycji tej dyrektywy do prawa wewnętrznego i upoważniające do zautomatyzowanego przetwarzania przewidzianego przez ową dyrektywę, ustanowiły jasne i precyzyjne zasady regulujące określanie baz danych oraz kryteria oceny, bez możliwości posługiwania się, w celach wstępnej oceny, metodami nieprzewidzianymi wprost w art. 6 ust. 2 wspomnianej dyrektywy.

181 Poza tym z art. 6 ust. 9 dyrektywy PNR wynika, że skutki wstępnej oceny pasażerów, o której mowa w art. 6 ust. 2 lit. a) tej dyrektywy, nie naruszają określonego w dyrektywie 2004/38 prawa osób, którym przysługuje prawo do swobodnego przemieszczania się, do wjazdu na terytorium danego państwa członkowskiego, oraz muszą być ponadto zgodne z rozporządzeniem nr 562/2006. A zatem system wprowadzony dyrektywą PNR nie pozwala właściwym organom na ograniczanie tego prawa ponad to, co zostało przewidziane w dyrektywie 2004/38 oraz rozporządzeniu nr 562/2006.

i) W przedmiocie zestawiania danych PNR z bazami danych

182 Jak stanowi art. 6 ust. 3 lit. a) dyrektywy PNR, dokonując sprawdzenia, o którym mowa w art. 6 ust. 2 lit. a) tej dyrektywy, JIP „może" porównać dane PNR z „bazami danych, które mają znaczenie" dla zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, „w tym z bazami danych o osobach lub przedmiotach poszukiwanych lub objętych wpisem, zgodnie z przepisami unijnymi, międzynarodowymi i krajowymi mającymi zastosowanie do takich baz danych".

183 O ile z samego brzmienia art. 6 ust. 3 lit. a) dyrektywy PNR, a w szczególności z wyrażenia „w tym", wynika, że bazy danych o osobach lub przedmiotach poszukiwanych lub objętych wpisem należą do „baz danych, które mają znaczenie", o których mowa w tym przepisie, o tyle przepis ten nie wskazuje innych baz danych, które mogą również być uznane za „mające znaczenie" w świetle celów realizowanych przez dyrektywę. Jak bowiem zauważył rzecznik generalny w pkt 217 opinii, omawiany przepis nie wskazuje wprost charakteru danych, które mogą być zawarte w takich bazach, oraz ich związku z przedmiotowymi celami ani nie mówi o tym, czy dane PNR muszą być porównywane jedynie z bazami danych prowadzonymi przez organy publiczne, czy też mogą być porównywane również z bazami danych prowadzonymi przez podmioty prywatne.

184 W związku z powyższym art. 6 ust. 3 lit. a) dyrektywy PNR może być, prima facie, interpretowany w ten sposób, że dane PNR mogą być wykorzystywane jako proste kryteria badania w celu przeprowadzania analiz różnych baz danych, w tym baz danych, które służby wywiadowcze i bezpieczeństwa państw członkowskich prowadzą i wykorzystują w celach innych niż te wskazane w tej dyrektywie, oraz że takie analizy mogą przyjąć formę eksploracji danych (*data mining*). Tymczasem możliwość przeprowadzania takich analiz i porównywania danych PNR z takimi bazami danych może prowadzić do powstania wśród pasażerów transportu lotniczego poczucia, że ich życie prywatne podlega pewnej formie nadzoru. Mimo że wstępna ocena przewidziana

w rozpatrywanym przepisie dotyczy ograniczonego zbioru danych, jakimi są dane PNR, powyższa wykładnia owego art. 6 ust. 3 lit. a) nie może zostać utrzymana, jako że mogłaby prowadzić do nieproporcjonalnego wykorzystywania tych danych, umożliwiając ustalenie precyzyjnego profilu osób zainteresowanych tylko dlatego, że mają one zamiar podróżować samolotem.

185 A zatem, zgodnie z orzecznictwem przypomnianym w pkt 86 i 87 niniejszego wyroku, art. 6 ust. 3 lit. a) dyrektywy PNR należy interpretować w sposób zapewniający pełne poszanowanie praw podstawowych, o których mowa w art. 7 i 8 karty.

186 W tym względzie z motywów 7 i 15 dyrektywy PNR wynika, że zautomatyzowane przetwarzanie przewidziane w art. 6 ust. 3 lit. a) tej dyrektywy musi być ograniczone do tego, co ściśle konieczne w celu zwalczania przestępstw terrorystycznych i poważnej przestępczości, przy zachowaniu wysokiego poziomu ochrony praw podstawowych.

187 Poza tym, jak zasadniczo wskazała Komisja w odpowiedzi na pytanie Trybunału, brzmienie tego przepisu, zgodnie z którym JIP „może" porównywać dane PNR z bazami danych, o których w nim mowa, pozwala JIP na wybór sposobu przetwarzania ograniczonego do tego, co ściśle konieczne w danej sytuacji. W świetle niezbędnego przestrzegania wymogów jasności i precyzji wymaganego celem zapewnienia ochrony praw podstawowych, o których mowa w art. 7 i 8 karty, JIP jest zobowiązana do ograniczenia zautomatyzowanego przetwarzania przewidzianego w art. 6 ust. 3 lit. a) dyrektywy PNR jedynie do tych baz danych, które na podstawie tego przepisu można zidentyfikować. W tym względzie, o ile zawarte w tym przepisie odniesienie do „baz mających znaczenie" nie poddaje się wykładni precyzującej w sposób wystarczająco jasny i konkretny te bazy danych, o tyle rzecz się ma inaczej w odniesieniu do „baz danych o osobach lub przedmiotach poszukiwanych lub objętych wpisem, zgodnie z przepisami unijnymi, międzynarodowymi i krajowymi mającymi zastosowanie do takich baz danych".

188 A zatem, jak zasadniczo wskazał rzecznik generalny w pkt 219 opinii, art. 6 ust. 3 lit. a) dyrektywy PNR powinien być, w świetle praw podstawowych, interpretowany w ten sposób, że tylko te ostatnie bazy danych mogą być porównywane przez JIP z danymi PNR.

189 Jeśli chodzi o wymogi, które muszą spełniać te bazy danych, należy podnieść, że zgodnie z art. 6 ust. 4 dyrektywy PNR wstępna ocena przeprowadzana w świetle wcześniej ustalonych kryteriów powinna, na podstawie art. 6 ust. 3 lit. b) tej dyrektywy, być realizowana w sposób niedyskryminacyjny, a przedmiotowe kryteria muszą być ukierunkowane, proporcjonalne i szczegółowe oraz poddawane regularnym przeglądom przez JIP we współpracy z właściwymi organami, o których mowa w art. 7 wspomnianej dyrektywy. Skoro, odnosząc się do art. 6 ust. 3 lit. b) tej samej dyrektywy, brzmienie jej art. 6 ust. 4 dotyczy wyłącznie przetwarzania danych PNR według wcześniej ustalonych kryteriów, ten ostatni przepis powinien być interpretowany w świetle art. 7, 8 i 21 karty w ten sposób, że wymogi, które zawiera, muszą mieć zastosowanie mutatis mutandis do porównywania tych danych z bazami danych wskazanymi w poprzednim punkcie niniejszego wyroku, tym bardziej że te wymogi są co do zasady tożsame z tymi przyjętymi do zestawiania danych PNR z bazami danych przez orzecznictwo wynikające z opinii 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r. (EU:C:2017:592, pkt 172).

190 W tym względzie należy uściślić, że z wymogu dotyczącego niedyskryminacyjnego charakteru tych baz danych wynika w szczególności, że zamieszczenie w bazach danych o osobach lub przedmiotach poszukiwanych lub objętych wpisem powinno być oparte na obiektywnych

i niedyskryminacyjnych przesłankach ustalonych przez przepisy krajowe, międzynarodowe lub unijne, mające zastosowanie do takich baz danych (zob. analogicznie wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 78).

191 Poza tym, aby spełnić wymóg dotyczący ukierunkowanego, proporcjonalnego i szczegółowego charakteru wcześniej ustalonych kryteriów, bazy danych, o których mowa w pkt 188 niniejszego wyroku, powinny być użytkowane w związku ze zwalczaniem przestępstw terrorystycznych i poważnej przestępczości oraz mieć obiektywny związek, choćby pośredni, z lotniczym przewozem pasażerów.

192 Ponadto bazy danych wykorzystywane na podstawie art. 6 ust. 3 lit. a) dyrektywy PNR powinny, biorąc pod uwagę motywy wskazane w pkt 183 i 184 niniejszego wyroku, być prowadzone przez właściwe organy, o których mowa w art. 7 tej dyrektywy lub, w zakresie baz danych Unii oraz międzynarodowych baz danych, być wykorzystywane przez te organy w ramach ich zadania zwalczania przestępstw terrorystycznych i poważnej przestępczości. Tak jest w przypadku baz danych o osobach lub przedmiotach poszukiwanych lub objętych wpisem, zgodnie z przepisami unijnymi, międzynarodowymi i krajowymi mającymi zastosowanie do takich baz danych.

ii) W przedmiocie przetwarzania danych PNR według wcześniej ustalonych kryteriów

193 Artykuł 6 ust. 3 lit. b) dyrektywy PNR przewiduje, że JIP mogą przetwarzać dane PNR także według wcześniej ustalonych kryteriów. Z art. 6 ust. 2 lit. a) tej dyrektywy wynika, że wstępna ocena, a tym samym przetwarzanie danych PNR według wcześniej ustalonych kryteriów zmierza zasadniczo do zidentyfikowania osób, które mogą być zaangażowane w przestępstwa terrorystyczne lub poważną przestępczość.

194 Jeśli chodzi o kryteria, których JIP może używać w tym celu, trzeba zauważyć, że zgodnie z art. 6 ust. 3 lit. b) dyrektywy PNR kryteria te powinny być „wcześniej ustalone". Jak wskazał rzecznik generalny w pkt 228 opinii, wymóg ten stoi na przeszkodzie wykorzystywaniu technologii sztucznej inteligencji w ramach systemu uczenia maszynowego (*machine learning*), który może, bez interwencji i udziału ludzi, zmieniać proces oceny, a w szczególności kryteria oceny, na których opiera się rezultat zastosowania takiego procesu, jak i wagę tych kryteriów.

195 Należy dodać, że odwołanie się do takich technologii stwarzałoby ryzyko pozbawienia skuteczności indywidualnej oceny pozytywnych wyników, a także kontroli legalności wymaganej przez przepisy dyrektywy PNR. Jak wskazał bowiem rzecznik generalny w pkt 228 opinii, biorąc pod uwagę brak przejrzystości związanej z działaniem technologii sztucznej inteligencji, może okazać się niemożliwe zrozumienie przyczyny, dla której dany program wskazał wynik pozytywny. W tych warunkach posługiwanie się takimi technologiami mogłoby pozbawić zainteresowane osoby również prawa do skutecznego środka ochrony prawnej, o którym mowa w art. 47 karty i które zgodnie z motywem 28 dyrektywy PNR ma być zagwarantowane na wysokim poziomie, w szczególności celem kwestionowania niedyskryminacyjnego charakteru uzyskanych wyników.

196 Jeśli chodzi następnie o wymogi wynikające z art. 6 ust. 4 dyrektywy PNR, przepis ten wskazuje w zdaniu pierwszym, że wstępna ocena według wcześniej ustalonych kryteriów odbywa się w sposób niedyskryminacyjny i precyzyjny, a w zdaniu czwartym doprecyzowuje, iż kryteria te w żadnym przypadku nie mogą opierać się na rasie ani pochodzeniu etnicznym, na poglądach politycznych, przekonaniach religijnych lub światopoglądowych, przynależności do związków zawodowych, stanie zdrowia, życiu seksualnym ani orientacji seksualnej danej osoby.

197 Także państwa członkowskie nie mogą przyjąć jako wcześniej ustalonych kryteriów takich, które opierają się na cechach wskazanych w poprzednim punkcie niniejszego wyroku i których użycie może być źródłem dyskryminacji. Z brzmienia art. 6 ust. 4 zdanie czwarte dyrektywy PNR, zgodnie z którym wcześniej ustalone kryteria nie mogą „w żadnym przypadku" opierać się na tych cechach, wynika w tym względzie, że przepis ten dotyczy zarówno dyskryminacji bezpośredniej, jak i pośredniej. Wykładnię tę potwierdza art. 21 ust. 1 karty, który zabrania „wszelkiej" dyskryminacji opartej na tych cechach i w świetle którego należy interpretować wyżej wskazany przepis dyrektywy PNR. W związku z tym wcześniej ustalone kryteria muszą być określone tak, by, poza neutralnym sposobem ich sformułowania, ich zastosowanie nie mogło postawić w gorszej sytuacji w szczególności osób posiadających chronione cechy.

198 Co do wymogów, by wcześniej ustalone kryteria były ukierunkowane, proporcjonalne i szczegółowe, co przewiduje art. 6 ust. 4 zdanie drugie dyrektywy PNR, z tych wymogów wynika, że kryteria używane do celów wstępnej oceny powinny być sformułowane w taki sposób, by ukierunkować je ściśle na osoby, wobec których może istnieć racjonalne podejrzenie ich udziału w przestępstwach terrorystycznych lub poważnej przestępczości, o których mowa w tej dyrektywie. Taką wykładnię potwierdza brzmienie art. 6 ust. 2 lit. a) owej dyrektywy, w którym położono akcent na „możliwość" udziału tych osób w przestępstwach terrorystycznych lub w poważnej przestępczości. Z tych samych powodów w motywie 7 tej dyrektywy wskazano, że ustalanie i stosowanie kryteriów dokonywania oceny należy ograniczyć do przestępstw terrorystycznych i poważnej przestępczości, „w przypadku których stosowanie takich kryteriów jest właściwe".

199 Celem wyłonienia w ten sposób osób, o których mowa wyżej i biorąc pod uwagę ryzyko dyskryminacji, która może wyniknąć z zastosowania kryteriów opartych na cechach wskazanych w art. 6 ust. 4 zdanie czwarte dyrektywy PNR, JIP i właściwe organy nie mogą zasadniczo opierać się na tych cechach. Natomiast, jak podniósł rząd niemiecki w czasie rozprawy, mogą one brać między innymi pod uwagę szczególne elementy w zachowaniu osób związane z przygotowaniem i realizacją podróży lotniczych, które mogą, zgodnie z doświadczeniem i wnioskami wypracowanymi przez właściwe organy, wskazywać, że osoby te działają w sposób mogący ujawnić ich zaangażowanie w przestępstwa terrorystyczne lub poważną przestępczość.

200 W tym kontekście, co zauważyła Komisja w swojej odpowiedzi na pytanie Trybunału, wcześniej ustalone kryteria powinny być określone z uwzględnieniem zarówno elementów „obciążających", jak i „odciążających", co może przyczynić się do większej wiarygodności tych kryteriów oraz w szczególności zapewnić, że będą one proporcjonalne, jak tego wymaga art. 6 ust. 4 zdanie drugie dyrektywy PNR.

201 Wreszcie, zgodnie z art. 6 ust. 4 zdanie trzecie tej dyrektywy, wcześniej ustalone kryteria winny być poddawane regularnym przeglądom. W ramach przeglądu kryteria te muszą być aktualizowane stosownie do zmiany warunków uzasadniających ich uwzględnianie w toku wstępnej oceny, pozwalających w szczególności na dostosowywanie się do zmian w zwalczaniu przestępstw terrorystycznych i poważnej przestępczości, o których mowa w pkt 157 niniejszego wyroku [zob. analogicznie wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 82]. W trakcie przeglądu należy w szczególności wziąć pod uwagę doświadczenie nabyte w ramach stosowania wcześniej ustalonych kryteriów, celem ograniczenia w jak największym stopniu liczby rezultatów „fałszywie pozytywnych" i zachowania ściśle niezbędnego charakteru zastosowania tych kryteriów.

iii) W przedmiocie gwarancji towarzyszących zautomatyzowanemu przetwarzaniu danych PNR

202 Poszanowanie wymogów, którym art. 6 ust. 4 dyrektywy PNR poddaje zautomatyzowane przetwarzanie danych PNR, jest konieczne nie tylko w ramach określania i przeglądu baz danych oraz wcześniej ustalonych kryteriów, które przewiduje ten przepis, ale także, na co zwraca uwagę rzecznik generalny w pkt 230 opinii, w trakcie całego procesu przetwarzania danych.

203 Jeśli chodzi w szczególności o wcześniej ustalone kryteria, należy na wstępie wskazać, że JIP ma obowiązek, na co wskazuje motyw 7 dyrektywy PNR, określenia kryteriów dokonywania oceny w sposób ograniczający do minimum liczbę osób niewinnych błędnie zidentyfikowanych przez system wprowadzony przez tę dyrektywę, a ponadto JIP powinna, zgodnie z art. 6 ust. 5 i 6 wspomnianej dyrektywy, przeprowadzić w sposób niezautomatyzowany indywidualną ocenę każdego wyniku pozytywnego celem ograniczenia w jak największym stopniu liczby rezultatów „fałszywie pozytywnych". Poza tym JIP, niezależnie od tego, że musi ustalić kryteria oceny w sposób niedyskryminacyjny, ma także obowiązek przeprowadzania oceny celem wyeliminowania ewentualnych dyskryminujących wyników. JIP powinna przestrzegać tego samego obowiązku oceny podczas zestawiania danych PNR z bazami danych.

204 JIP musi również powstrzymać się od przekazywania wyników zautomatyzowanego przetwarzania właściwym organom, o których mowa w art. 7 dyrektywy PNR, jeśli po przeprowadzeniu oceny indywidualnej nie dysponuje, w świetle uwag sformułowanych w pkt 198 niniejszego wyroku, uzasadnionym podejrzeniem udziału w przestępstwach terrorystycznych lub poważnej przestępczości osób zidentyfikowanych w trakcie zautomatyzowanego przetwarzania danych lub jeśli istnieją elementy wskazujące, że to przetwarzanie prowadzi do dyskryminujących wyników.

205 Co się tyczy weryfikacji, którą musi przeprowadzić w tym celu JIP, z art. 6 ust. 5 i 6 dyrektywy PNR, w związku z jej motywami 20 i 21 wynika, że państwa członkowskie powinny ustanowić jasne i precyzyjne zasady określające ramy analizy przeprowadzanej przez pracowników odpowiedzialnych za indywidualną ocenę, celem zapewnienia pełnego poszanowania praw podstawowych, o których mowa w art. 7, 8 i 21 karty oraz w szczególności wprowadzić w JIP spójną praktykę administracyjną będącą w zgodzie z zasadą niedyskryminacji.

206 W szczególności, biorąc pod uwagę dość znaczną liczbę wyników „fałszywie pozytywnych" wspomnianą w pkt 106 niniejszego wyroku, państwa członkowskie mają obowiązek zapewnienia, by JIP określała w sposób jasny i precyzyjny obiektywne kryteria oceny pozwalające jej pracownikom zweryfikować, po pierwsze, czy i w jakim stopniu wynik pozytywny (*hit*) dotyczy w istocie jednostki, która może być zaangażowana w przestępstwa terrorystyczne lub poważną przestępczość, o jakich mowa w pkt 157 niniejszego wyroku, i w związku z tym winna być poddana pogłębionej analizie przez właściwe organy wskazane w art. 7 dyrektywy PNR oraz, po drugie, niedyskryminacyjny charakter zautomatyzowanego przetwarzania przewidzianego tą dyrektywą, a zwłaszcza wcześniej ustalonych kryteriów oraz wykorzystywanych baz danych.

207 W tym kontekście państwa członkowskie mają obowiązek czuwania nad tym, by, zgodnie z art. 13 ust. 5 dyrektywy PNR, w związku z jej motywem 37, JIP rejestrowała i dokumentowała każde przetwarzanie danych PNR dokonywane w ramach wstępnej oceny, w tym w ramach indywidualnego sprawdzania za pomocą niezautomatyzowanych środków, w celu weryfikacji jego legalności oraz autokontroli.

208 Następnie właściwe organy nie mogą podjąć, na podstawie art. 7 ust. 6 zdanie pierwsze dyrektywy PNR żadnych decyzji, które miałyby negatywne skutki prawne dla danej osoby lub znacząco wpływałyby na jej sytuację, wyłącznie na podstawie automatycznego przetwarzania danych PNR, co oznacza, że w ramach wstępnej oceny muszą wziąć pod uwagę wynik indywidualnej oceny przeprowadzanej przez JIP za pomocą środków niezautomatyzowanych, a w odpowiednich przypadkach zmienić wynik uzyskany za pomocą przetwarzania zautomatyzowanego. Artykuł 7 ust. 6 zdanie drugie tej dyrektywy wskazuje, że takie decyzje nie mogą mieć charakteru dyskryminacyjnego.

209 W tym kontekście właściwe organy muszą zapewnić zgodność z prawem zarówno takiego przetwarzania zautomatyzowanego, w tym ich niedyskryminacyjnego charakteru, jak i oceny indywidualnej.

210 W szczególności właściwe organy powinny zagwarantować, by osoba zainteresowana w toku procedury administracyjnej mogła zrozumieć działanie zastosowanych kryteriów wstępnej oceny i programów stosujących te kryteria, bez konieczności poznawania tych kryteriów i programów jako takich, w sposób pozwalający jej na podjęcie w sposób w pełni świadomy decyzji, czy skorzysta z prawa do sądowego środka ochrony prawnej zagwarantowanego w art. 13 ust. 1 dyrektywy PNR w celu zaskarżenia, w odpowiednim przypadku, nielegalnego i dyskryminacyjnego charakteru przedmiotowych kryteriów (zob. analogicznie wyrok z dnia 24 listopada 2020 r., Minister van Buitenlandse Zaken, C-225/19 i C-226/19, EU:C:2020:951, pkt 43 i przytoczone tam orzecznictwo). To samo tyczy się kryteriów oceny, o których mowa w pkt 206 niniejszego wyroku.

211 Wreszcie, w ramach sądowego środka ochrony prawnej, o którym mowa w art. 13 ust. 1 dyrektywy PNR, zarówno sąd dokonujący kontroli legalności decyzji wydanej przez właściwe organy, jak i osoba zainteresowana, z wyłączeniem przypadków zagrożenia bezpieczeństwa narodowego, powinny mieć możliwość zapoznania się z całością zarówno motywów, jak i odnośnych dowodów, na podstawie których decyzja ta została wydana (zob. analogicznie wyrok z dnia 4 czerwca 2013 r., ZZ, C-300/11, EU:C:2013:363, pkt 54–59), w tym z wcześniej ustalonymi kryteriami oceny oraz działaniem programów stosujących te kryteria.

212 Poza tym, zgodnie odpowiednio z art. 6 ust. 7 i art. 15 ust. 3 lit. b) dyrektywy PNR, na inspektorze ochrony danych i krajowym organie nadzorczym spoczywa obowiązek zapewnienia kontroli legalności zautomatyzowanego przetwarzania danych wykonywanego przez JIP w ramach wstępnej oceny, kontroli, która dotyczy w szczególności niedyskryminacyjnego charakteru tego przetwarzania. O ile pierwszy ze wskazanych przepisów wskazuje, że inspektor ochrony danych ma dostęp do wszystkich danych przetwarzanych przez JIP, dostęp ten musi koniecznie rozciągać się na wcześniej ustalone kryteria oraz bazy danych używane przez JIP celem zapewnienia skuteczności i wysokiego poziomu ochrony danych, który to obowiązek spoczywa na tym organie zgodnie z motywem 37 dyrektywy. Podobnie postępowania, inspekcje i audyty, przeprowadzane przez krajowy organ nadzorczy na podstawie drugiego ze wskazanych przepisów, także mogą dotyczyć tych wcześniej ustalonych kryteriów i baz danych.

213 Z całokształtu powyższych rozważań wynika, że przepisy dyrektywy PNR regulujące wstępną ocenę danych PNR na podstawie art. 6 ust. 2 lit. a) tej dyrektywy poddają się wykładni zgodnej z art. 7, 8 i 21 karty, ograniczając się do tego, co ściśle konieczne.

6) W przedmiocie przekazywania i późniejszej oceny danych PNR

214 Zgodnie z art. 6 ust. 2 lit. b) dyrektywy PNR dane PNR na wniosek właściwych organów mogą być przekazywane tym ostatnim oraz być przedmiotem oceny następującej po planowanym przylocie do państwa członkowskiego lub planowanym z niego wylocie.

215 Jeśli chodzi o warunki, w których takie przekazanie i ocena mogą zostać przeprowadzone, z brzmienia wskazanego przepisu wynika, że JIP może przetwarzać dane PNR w celu odpowiadania „na podstawie oceny każdego indywidualnego przypadku" na „należycie uzasadniony i oparty na wystarczających podstawach wniosek" właściwych organów zmierzający do tego, by dane zostały im przekazane i były przetwarzane „w określonych przypadkach w celach zapobiegania przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania". Poza tym, jeśli wniosek jest składany później niż sześć miesięcy po pierwszym przekazaniu danych PNR do JIP, to jest po okresie, po którym całość danych PNR jest poddawana depersonalizacji poprzez maskowanie ich niektórych elementów, zgodnie z art. 12 ust. 2 tej dyrektywy, jej art. 12 ust. 3 stanowi, że przekazanie całości danych PNR i tym samym ich wersji niezdepersonalizowanej może być zatwierdzone jedynie przy spełnieniu dwóch warunków – po pierwsze, musi istnieć uzasadnienie, by uznać, że jest to niezbędne do celów określonych w art. 6 ust. 2 lit. b) wspomnianej dyrektywy, a po drugie, musi zostać przyznana zgoda w tym zakresie przez organ wymiaru sprawiedliwości lub inny właściwy na mocy prawa krajowego organ krajowy.

216 W tym względzie, z brzmienia art. 6 ust. 2 lit. b) dyrektywy PNR wynika przede wszystkim, że JIP nie może dokonywać systematycznego przekazywania i następczej oceny danych PNR wszystkich pasażerów lotniczych, a jedynie może odpowiadać „na podstawie oceny każdego indywidualnego przypadku" na wnioski dotyczące przetwarzania danych „w określonych przypadkach". Ze względu na to, że przepis ten odnosi się do określonych przypadków, przetwarzanie to nie musi się ograniczać do danych PNR jednego pasażera lotniczego, ale może, jak wskazała Komisja w swojej odpowiedzi na pytanie Trybunału, dotyczyć większej liczby osób, pod warunkiem, że osoby te mają pewną liczbę cech wspólnych pozwalającą uznać je za stanowiące „określony przypadek" w celu przekazania danych i ich oceny.

217 Co się tyczy, następnie, przesłanek materialnych, które muszą zaistnieć, by dane PNR pasażerów lotniczych mogły być przedmiotem przekazania i późniejszej oceny, o ile art. 6 ust. 2 lit. b) oraz art. 12 ust. 3 lit. a) dyrektywy PNR odnoszą się odpowiednio do „wystarczających podstaw" oraz „uzasadnienia", nie precyzując wprost charakteru tychże, o tyle z brzmienia pierwszego z tych przepisów, który odnosi się do celów wskazanych w art. 1 ust. 2 wspomnianej dyrektywy, wynika, że przekazanie danych PNR i późniejsza ich ocena mogą zostać dokonane jedynie w celu weryfikacji istnienia przesłanek co do możliwości zaangażowania określonych osób w przestępstwa terrorystyczne lub poważną przestępczość, które mają, co wynika również z pkt 157 niniejszego wyroku, obiektywny, choćby pośredni, związek z przewozem lotniczym pasażerów.

218 Tymczasem w ramach systemu wprowadzonego dyrektywą PNR przekazywanie i przetwarzanie danych PNR na podstawie art. 6 ust. 2 lit. b) tej dyrektywy dotyczy danych osobowych, które były już przedmiotem wstępnej oceny przed planowanym przylotem danej osoby do określonego państwa członkowskiego lub jej wylotem z niego. Poza tym wniosek w zakresie późniejszej oceny danych może obejmować w szczególności osoby, których dane PNR nie zostały przekazane właściwym organom w następstwie wstępnej oceny, pod warunkiem że nie ujawniła ona elementów wskazujących na to, że osoby te mogły być zaangażowane w przestępstwa

terrorystyczne lub poważną przestępczość, które mają obiektywny związek, choćby pośredni, z lotniczym przewozem pasażerów. W tym przypadku przekazanie i przetwarzanie rzeczonych danych w celu późniejszej oceny muszą być oparte na nowych okolicznościach uzasadniających takie użycie danych [zob. podobnie opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 200 i przytoczone tam orzecznictwo].

219 Co do charakteru okoliczności mogących uzasadnić takie przekazanie i przetwarzanie danych PNR w celu ich późniejszej oceny, z utrwalonego orzecznictwa wynika, że jeśli powszechnego dostępu do zatrzymanych danych, niezależnie od jakiegokolwiek związku, nawet pośredniego, z realizowanym celem, nie można uważać za ograniczony do tego, co ściśle konieczne, rozpatrywane przepisy – czy to unijne, czy krajowe mające na celu transpozycję tej dyrektywy – winny opierać się na obiektywnych kryteriach umożliwiających określenie okoliczności i warunków przyznania dostępu właściwym organom do omawianych danych. W tym względzie, biorąc pod uwagę cel polegający na zwalczaniu poważnej przestępczości, dostęp ten może co do zasady zostać przyznany jedynie w odniesieniu do danych dotyczących osób podejrzewanych o planowanie, popełnianie czy też popełnienie już poważnego przestępstwa bądź też zaangażowanych w taki czy inny sposób w takie przestępstwo. Niemniej jednak w szczególnych sytuacjach, takich jak te, w których istotne interesy związane z bezpieczeństwem narodowym, obroną czy też bezpieczeństwem publicznym są zagrożone wskutek działań terrorystycznych, dostęp do danych dotyczących innych osób może zostać przyznany również wówczas, gdy istnieją obiektywne elementy pozwalające uznać, że dane te mogłyby w konkretnym przypadku rzeczywiście przyczynić się do zwalczania takich działań [wyroki: z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej), C-746/18, EU:C:2021:152, pkt 50 i przytoczone tam orzecznictwo; z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 105].

220 Pojęcia „wystarczających podstaw” i „uzasadnienia”, o których mowa, odpowiednio, w art. 6 ust. 2 lit. b) oraz art. 12 ust. 3 lit. a) dyrektywy PNR, winny być interpretowane w świetle art. 7 i 8 karty, jako odnoszące się do obiektywnych przesłanek, na których można oprzeć racjonalne podejrzenie zaangażowania danej osoby, w taki lub inny sposób, w poważną przestępczość, która ma związek, choćby pośredni, z lotniczym przewozem pasażerów, podczas gdy w przypadku przestępstw terrorystycznych, w których taki związek występuje, sformułowany wyżej wymóg jest spełniony, jeśli istnieją obiektywne przesłanki pozwalające uznać, że dane PNR mogą w konkretnym przypadku skutecznie przyczynić się do zwalczania takich przestępstw.

221 Wreszcie, w kwestii warunków proceduralnych, którym podlegają przekazanie i przetwarzanie danych PNR w celach późniejszej oceny, art. 12 ust. 3 lit. b) dyrektywy PNR wymaga, by w przypadku gdy wniosek jest złożony później niż sześć miesięcy po przekazaniu danych do JIP, a zatem po tym, gdy zgodnie z ust. 2 tego artykułu dane te zostały zdepersonalizowane poprzez maskowanie elementów, o których mowa w tymże ustępie, przekazanie wszystkich danych PNR i tym samym ich wersji niezdepersonalizowanej było zatwierdzone przez organ wymiaru sprawiedliwości lub inny właściwy organ krajowy. A zatem to do tych organów należy zbadanie całości uzasadnienia wniosku oraz w szczególności weryfikacja, czy dowody przedstawione na jego poparcie spełniają materialną przesłankę w postaci istnienia „wystarczających podstaw”, o których mowa w poprzednim punkcie niniejszego wyroku.

222 Jest prawdą, że w przypadku gdy wniosek o przekazanie i o późniejszą ocenę danych PNR jest kierowany przed upływem przedmiotowego okresu sześciu miesięcy od przekazania danych, art. 6 ust. 2 lit. b) dyrektywy PNR nie przewiduje wprost takiego warunku proceduralnego. Jednakże wykładnia tego ostatniego przepisu musi brać pod uwagę motyw 25 tej dyrektywy,

z którego wynika, że przewidując omawiany warunek proceduralny, prawodawca Unii zamierzał „zapewnić jak najwyższy poziom ochrony danych" w zakresie dostępu do danych PNR w formie pozwalającej na bezpośrednią identyfikację osoby zainteresowanej. Tymczasem każdy wniosek o udostępnienie i późniejszą ocenę wiąże się z dostępem do tych danych, niezależnie od tego, czy został złożony przed upływem okresu sześciu miesięcy po przekazaniu danych PNR do JIP, czy też po jego upływie.

223 W celu zapewnienia w praktyce pełnego poszanowania praw podstawowych w ramach systemu wprowadzonego dyrektywą PNR, a zwłaszcza warunków, o których mowa w pkt 218 oraz 219 niniejszego wyroku, niezbędne jest, by przekazanie danych PNR w celach późniejszej oceny było co do zasady, z wyjątkiem należycie uzasadnionych pilnych przypadków, uzależnione od uprzedniej kontroli sądu lub niezależnego organu administracyjnego, a decyzja tego sądu lub organu była wydawana na uzasadniony wniosek właściwych organów, złożony w szczególności w ramach postępowań mających na celu zapobieganie, wykrywanie lub ściganie przestępstw. W pilnych i należycie uzasadnionych przypadkach rzeczona kontrola powinna zostać przeprowadzona w krótkim czasie [zob. podobnie opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 202 i przytoczone tam orzecznictwo; wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 110].

224 W związku z powyższym wymóg uprzedniej kontroli wniosków o przekazanie danych PNR składanych po upływie okresu sześciu miesięcy po przekazaniu danych do JIP, o którym mowa w art. 12 ust. 3 lit. b) dyrektywy PNR, powinien być stosowany, mutatis mutandis, również do przypadków, w których wniosek o przekazanie danych jest składany przed upływem tego okresu.

225 Ponadto, chociaż art. 12 ust. 3 lit. b) dyrektywy PNR nie wskazuje wprost wymogów, jakie musi spełniać organ odpowiedzialny za uprzednią kontrolę, z utrwalonego orzecznictwa wynika, że celem zapewnienia, by ingerencja w prawa podstawowe zagwarantowane w art. 7 i 8 karty, wynikająca z dostępu do danych osobowych, była ograniczona do tego, co ściśle konieczne, wspomniany organ powinien dysponować wszelkimi uprawnieniami i gwarancjami niezbędnymi do pogodzenia poszczególnych wchodzących w grę interesów i praw. Jeśli chodzi w szczególności o dochodzenie w sprawach karnych, taka kontrola wymaga, aby ten sąd lub organ był w stanie zapewnić właściwą równowagę pomiędzy z jednej strony uzasadnionymi 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 (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 107 i przytoczone tam orzecznictwo).

226 W związku z tym taki organ musi posiadać status pozwalający mu działać w wykonywaniu swoich obowiązków w sposób obiektywny i bezstronny i w tym celu powinien on pozostawać poza jakimkolwiek wpływem z zewnątrz. Dla spełnienia tego wymogu niezależności niezbędne jest, by organ ten miał status strony trzeciej w stosunku do organu wnoszącego o udzielenie dostępu do danych, tak aby ten pierwszy był w stanie przeprowadzić kontrolę poza jakimkolwiek wpływem z zewnątrz. W szczególności w dziedzinie prawa karnego wymóg niezależności oznacza, że organ odpowiedzialny za tę uprzednią kontrolę, po pierwsze, nie jest zaangażowany w prowadzenie danego dochodzenia karnego, a po drugie, zajmuje neutralną pozycję wobec stron postępowania karnego (zob. podobnie wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 108 i przytoczone tam orzecznictwo).

227 A zatem przepisy dyrektywy PNR regulujące przekazanie i późniejszą ocenę danych PNR, na podstawie art. 6 ust. 2 lit. b) tej dyrektywy, poddają się wykładni zgodnej z art. 7, 8 oraz art. 52 ust. 1 karty, ograniczając się do tego, co ściśle konieczne.

228 Mając na względzie całokształt powyższych rozważań, jako że wykładnia dyrektywy PNR w świetle art. 7, 8, 21 oraz art. 52 ust. 1 karty zapewnia zgodność tej dyrektywy ze wskazanymi postanowieniami karty, analiza pytań od drugiego do czwartego oraz pytania szóstego nie doprowadziła do żadnych ustaleń, które mogłyby mieć wpływ na ważność owej dyrektywy.

C. W przedmiocie pytania piątego

229 W pytaniu piątym sąd odsyłający dąży do ustalenia, czy art. 6 dyrektywy PNR, w związku z art. 7 i 8 oraz art. 52 ust. 1 karty, należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu, które zezwala na przetwarzanie danych PNR, gromadzonych zgodnie z tą dyrektywą, do celów monitorowania działalności będącej przedmiotem zainteresowania służb wywiadowczych i bezpieczeństwa.

230 Z wniosku o wydanie orzeczenia w trybie prejudycjalnym wynika, że sąd odsyłający w pytaniu piątym porusza w szczególności kwestię działań Sûreté de l'État (służby bezpieczeństwa państwa, Belgia) oraz Service général du renseignement et de sécurité (ogólnych służb wywiadowczych i bezpieczeństwa, Belgia) w ramach ich zadań dotyczących ochrony bezpieczeństwa narodowego.

231 W tym względzie, celem przestrzegania zasad legalności i proporcjonalności, o których mowa w art. 52 ust. 1 karty, prawodawca Unii sformułował jasne i precyzyjne zasady regulujące cele działań przewidzianych w dyrektywie PNR, które zakładają ingerencję w prawa podstawowe zagwarantowane w art. 7 i 8 karty.

232 Otóż art. 1 ust. 2 dyrektywy PNR wskazuje wprost, że dane PNR gromadzone zgodnie z tą dyrektywą mogą być przetwarzane „wyłącznie w celach zapobiegania przestępstwom terrorystycznym i poważnej przestępczości oraz ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, jak przewidziano w art. 6 ust. 2 lit. a), b) i c) [wspomnianej dyrektywy]". Ten ostatni przepis potwierdza zasadę wyrażoną w art. 1 ust. 2, odnosząc się systematycznie do pojęć „przestępstw terrorystycznych" oraz „poważnej przestępczości".

233 Z brzmienia przedmiotowych przepisów wynika jasno, że zawarty w nich wykaz celów realizowanych przez przetwarzanie danych PNR na podstawie dyrektywy PNR ma charakter wyczerpujący.

234 Wykładnia ta znajduje potwierdzenie w szczególności w motywie 11 dyrektywy PNR, zgodnie z którym przetwarzanie danych PNR powinno być proporcjonalne do „szczególnych celów dotyczących bezpieczeństwa", którym służy ta dyrektywa, oraz w jej art. 7 ust. 4, zgodnie z którym dane PNR oraz wyniki przetwarzania tych danych, otrzymane od JIP, mogą być poddane dalszemu przetwarzaniu „wyłącznie do określonych celów, jakimi są zapobieganie przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywanie, prowadzenie postępowań przygotowawczych w ich sprawie lub ich ściganie".

235 Poza tym wyczerpujący charakter celów wskazanych w art. 1 ust. 2 dyrektywy PNR implikuje, że dane PNR nie mogą być zatrzymywane w pojedynczej bazie danych, z której można by korzystać dla realizacji zarówno tych, jak i innych celów. Przechowywanie danych w takiej bazie pociągałoby za sobą ryzyko, że zostaną one użyte w celach innych niż wskazane w owym art. 1 ust. 2.

236 W niniejszym przypadku w zakresie, w jakim zdaniem sądu odsyłającego rozpatrywane w postępowaniu głównym uregulowania krajowe dopuszcza, jako cel przetwarzania danych, monitorowanie działalności będącej przedmiotem zainteresowania służb wywiadowczych i bezpieczeństwa, włączając ten cel w zapobieganie przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywanie, prowadzenie postępowań przygotowawczych w ich sprawie i ich ściganie, uregulowanie to może naruszać wyczerpujący charakter wykazu celów realizowanych przez przetwarzanie danych PNR na podstawie dyrektywy PNR, czego ustalenie należy do sądu odsyłającego.

237 W związku z powyższym na pytanie piąte należy odpowiedzieć w ten sposób, że art. 6 dyrektywy PNR, w związku z art. 7 i 8 oraz art. 52 ust. 1 karty, należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu, które zezwala na przetwarzanie danych PNR, gromadzonych zgodnie z tą dyrektywą, do celów innych niż wprost wskazane w art. 1 ust. 2 owej dyrektywy.

D. W przedmiocie pytania siódmego

238 Poprzez pytanie siódme sąd odsyłający dąży zasadniczo do ustalenia, czy art. 12 ust. 3 lit. b) dyrektywy PNR należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu, zgodnie z którym organ ustanowiony jako JIP ma jednocześnie status właściwego organu krajowego uprawnionego do udzielania zgody na ujawnienie danych PNR po upływie okresu sześciu miesięcy od przekazania danych PNR do JIP.

239 Tytułem wstępu należy zauważyć, że rząd belgijski wyraża wątpliwości co do tego, czy Trybunał jest właściwy do udzielenia odpowiedzi na tak sformułowane przez sąd odsyłający pytanie, jako że tylko ten ostatni sąd jest uprawniony do interpretacji przepisów krajowych, a w szczególności oceniania wymogów wynikających z ustawy z dnia 25 grudnia 2016 r. w świetle art. 12 ust. 3 lit. b) dyrektywy PNR.

240 W tym względzie wystarczy wskazać, że poprzez przedmiotowe pytanie sąd odsyłający zwraca się o wykładnię przepisu prawa Unii. Poza tym, w ramach procedury wprowadzonej na podstawie art. 267 TFUE, wykładnia przepisów prawa krajowego należy do sądów państw członkowskich, a nie do Trybunału; do tego ostatniego nie należy zatem orzekanie w przedmiocie zgodności norm prawa krajowego z postanowieniami prawa Unii, przy czym zadaniem Trybunału jest dostarczenie sądowi krajowemu wszystkich elementów wykładni prawa Unii, które mogą mu być pomocne w dokonaniu oceny zgodności norm prawa krajowego z uregulowaniami Unii (wyrok z dnia 30 kwietnia 2020 r., CTT – Correios de Portugal, C-661/18, EU:C:2020:335, pkt 28 i przytoczone tam orzecznictwo). A zatem Trybunał jest uprawniony do udzielenia odpowiedzi na pytanie siódme.

241 Co do istoty sprawy należy wskazać, że brzmienie art. 12 ust. 3 lit. b) dyrektywy PNR, który mówi w swoich ppkt (i) i (ii), odpowiednio, o „organie wymiaru sprawiedliwości” oraz „innym organie krajowym, który zgodnie z prawem krajowym jest właściwy do ustalenia, czy warunki ujawnienia zostały spełnione”, stawia na równi oba organy, co wynika ze spójnika „lub” użytego między tymi

podpunktami. Wyrażenie „inny organ krajowy”, jak ponadto wynika, stanowi alternatywę dla organu sądowego, a tym samym ten pierwszy organ powinien prezentować poziom niezależności i bezstronności porównywalny z tym drugim.

242 Taki wniosek znajduje poparcie w celu dyrektywy PNR wskazanym w jej motywie 25, by zapewnić jak najwyższy poziom ochrony danych w zakresie dostępu do pełnych danych PNR, które umożliwiają bezpośrednie zidentyfikowanie osoby, której dane dotyczą. W tym samym motywie wskazano, że taki dostęp po upływie okresu sześciu miesięcy od przekazania danych PNR do JIP może być przyznany wyłącznie po spełnieniu bardzo restrykcyjnych warunków.

243 Słuszność tego podejścia potwierdza również geneza dyrektywy PNR. Otóż, pomimo że projekt dyrektywy, leżący u jej źródła, o którym wspomniano w pkt 155 niniejszego wyroku, początkowo przewidywał tylko, że „dostęp do wszystkich danych PNR jest dozwolony jedynie przez jednostkę do spraw informacji o pasażerach”, w ostatecznej wersji art. 12 ust. 3 lit. b) dyrektywy przyjętej przez prawodawcę Unii zrównano organ sądowy i „inny organ krajowy” właściwy do ustalenia, czy warunki ujawnienia wszystkich danych PNR zostały spełnione, oraz do zatwierdzenia takiego ujawnienia.

244 Przede wszystkim zaś, zgodnie z utrwalonym orzecznictwem przypomnianym w pkt 223, 225 i 226 niniejszego wyroku, podstawowe znaczenie ma to, aby dostęp właściwych organów 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. Wymóg niezależności, który powinien spełniać organ odpowiedzialny za przeprowadzenie uprzedniej kontroli, wymaga, aby organ ten miał status strony trzeciej w stosunku do organu wnoszącego o udzielenie dostępu do danych, tak aby ten pierwszy był w stanie przeprowadzić tę kontrolę w sposób obiektywny i bezstronny, poza jakimkolwiek wpływem z zewnątrz. W szczególności w dziedzinie prawa karnego wymóg niezależności oznacza, że organ odpowiedzialny za tę uprzednią kontrolę, po pierwsze, nie jest zaangażowany w prowadzenie omawianego dochodzenia karnego, a po drugie, zajmuje neutralną pozycję wobec stron postępowania karnego.

245 Tymczasem, jak podniósł rzecznik generalny w pkt 271 opinii, art. 4 dyrektywy PNR przewiduje w ust. 1 i 3, że JIP, ustanowiona lub wyznaczona w każdym państwie członkowskim, jest organem właściwym do zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie lub ich ścigania oraz że jej pracownicy mogą być oddelegowani z właściwych organów, o których mowa w art. 7 tej dyrektywy, a zatem JIP wydaje się w sposób jednoznaczny powiązana z tymi organami. JIP może również dokonać, na podstawie art. 6 ust. 2 lit. b) wspomnianej dyrektywy, przetwarzania danych PNR i przekazać jego wyniki rzeczonym organom. Mając na względzie powyższe, JIP nie może być uznana za posiadającą status strony trzeciej w stosunku do tych organów i tym samym za wystarczająco niezależną i bezstronną do przeprowadzania uprzedniej kontroli, o której mowa w poprzednim punkcie niniejszego wyroku, oraz do ustalania, czy warunki ujawnienia wszystkich danych PNR, o których mowa w art. 12 ust. 3 lit. b) wspomnianej dyrektywy, zostały spełnione.

246 Poza tym fakt, że ten ostatni przepis wymaga w swoim ppkt (ii), w przypadku zgody na ujawnienie wszystkich danych udzielonej przez „inny organ krajowy”, „poinformowania inspektora ochrony danych w JIP oraz dokonania przez tego inspektora ochrony danych weryfikacji ex post”, a taki wymóg nie istnieje w przypadku udzielania zgody przez organ wymiaru sprawiedliwości, nie może podważyć tej oceny. Zgodnie z utrwalonym orzecznictwem późniejsza kontrola, taka jak ta

przeprowadzana przez inspektora ochrony danych, nie pozwala bowiem osiągnąć celu uprzedniej kontroli, polegającego na uniemożliwieniu udzielania zezwoleń na dostęp do rozpatrywanych danych, który wykracza poza granice tego, co ściśle konieczne (zob. podobnie wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 110 i przytoczone tam orzecznictwo).

247 Biorąc pod uwagę całokształt powyższych rozważań, na pytanie siódme należy odpowiedzieć w ten sposób, że art. 12 ust. 3 lit. b) dyrektywy PNR należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu, zgodnie z którym organ ustanowiony jako JIP ma jednocześnie status właściwego organu krajowego uprawnionego do udzielania zgody na ujawnienie danych PNR po upływie okresu sześciu miesięcy od przekazania danych PNR do JIP.

E. W przedmiocie pytania ósmego

248 Poprzez pytanie ósme sąd odsyłający dąży zasadniczo do ustalenia, czy art. 12 dyrektywy PNR, w związku z art. 7 i 8 oraz art. 52 ust. 1 karty, należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu, które przewiduje ogólny okres zatrzymywania danych wynoszący pięć lat, nie dokonując rozróżnienia stosownie do tego, czy dani pasażerowie stanowią zagrożenie lub nie stanowią zagrożenia w zakresie przestępstw terrorystycznych lub poważnej przestępczości.

249 Należy przypomnieć, że zgodnie z art. 12 ust. 1 i 4 dyrektywy PNR JIP państwa członkowskiego, na którego terytorium ma miejsce przylot lub z którego terytorium ma miejsce odlot, zatrzymuje dane PNR dostarczone przez przewoźników lotniczych w bazie danych przez okres pięciu lat następujących po przekazaniu tych danych oraz usuwa te dane w sposób trwały po upływie tego okresu pięciu lat.

250 Jak wspomniano w motywie 25 dyrektywy PNR, dane PNR „powinny być zatrzymywane na okres niezbędny i proporcjonalny do celów, jakimi są zapobieganie przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywanie, prowadzenie postępowań przygotowawczych w ich sprawie i ich ściganie”.

251 A zatem zatrzymanie danych PNR na podstawie art. 12 ust. 1 dyrektywy PNR nie może być uzasadnione bez obiektywnego związku pomiędzy tym zatrzymaniem i celami realizowanymi przez przedmiotową dyrektywę, a mianowicie zwalczaniem przestępstw terrorystycznych lub poważnej przestępczości, które mają obiektywny związek, choćby pośredni, z lotniczym przewozem pasażerów.

252 W tym względzie, co wynika również z motywu 25 dyrektywy PNR, należy dokonać rozróżnienia pomiędzy pierwotnym okresem zatrzymania wynoszącym sześć miesięcy, o którym mowa w art. 12 ust. 2 tej dyrektywy, oraz okresem późniejszym, o którym mowa w jej art. 12 ust. 3.

253 Wykładnia art. 12 ust. 1 dyrektywy PNR powinna brać pod uwagę przepisy znajdujące się w ust. 2 i 3 tego artykułu, które regulują system zatrzymywania i dostępu do przechowywanych danych PNR po upływie pierwotnego okresu zatrzymania wynoszącego sześć miesięcy. Jak wynika z motywu 25 tej dyrektywy, przepisy te odzwierciedlają, z jednej strony, cel w postaci zapewnienia „zatrzymywania danych PNR przez wystarczająco długi okres, aby możliwe było ich analizowanie i wykorzystywanie w postępowaniach przygotowawczych”, co może zostać dokonane w pierwotnym sześciomiesięcznym okresie zatrzymania. Z drugiej strony, służą one, zgodnie z tym samym motywem 25, „zapobieganiu ich nieproporcjonalnemu wykorzystywaniu” poprzez

ich maskowanie oraz „zapewnieniu jak najwyższego poziomu ochrony danych", zezwalając na dostęp do tych danych w formie pozwalającej na bezpośrednie zidentyfikowanie osoby, której dane dotyczą „wyłącznie po spełnieniu bardzo restrykcyjnych i ściśle określonych warunków", „po upływie początkowego okresu zatrzymania", biorąc pod uwagę fakt, że im dłuższy okres zatrzymania danych PNR, tym ingerencja z niego wynikająca jest poważniejsza.

254 Tymczasem rozróżnienie pomiędzy pierwotnym, sześciomiesięcznym okresem zatrzymania, o którym mowa w art. 12 ust. 2 dyrektywy PNR, i okresem późniejszym, o którym mowa w art. 12 ust. 3 tej dyrektywy, ma zastosowanie również do poszanowania koniecznego wymogu wskazanego w pkt 251 niniejszego wyroku.

255 Biorąc pod uwagę cele dyrektywy PNR oraz potrzeby postępowań przygotowawczych i ścigania przestępstw terrorystycznych, jak i poważnej przestępczości, należy stwierdzić, że zatrzymanie przez pierwotny okres sześciu miesięcy danych PNR wszystkich pasażerów lotniczych podlegających systemowi wprowadzonemu tą dyrektywą, niezależnie od tego, czy istnieje jakakolwiek przesłanka wskazująca na ich zaangażowanie w przestępstwa terrorystyczne lub poważną przestępczość, nie wydaje się, co do zasady, wykraczać poza to, co ściśle konieczne, jako że pozwala na dokonanie niezbędnych sprawdzeń celem zidentyfikowania osób, które nie były podejrzane o udział w przestępstwach terrorystycznych lub poważnej przestępczości.

256 Jeśli chodzi z kolei o późniejszy okres, o którym mowa w art. 12 ust. 3 dyrektywy PNR, zatrzymywanie danych PNR wszystkich pasażerów lotniczych podlegających systemowi wprowadzonemu tą dyrektywą, poza tym że, ze względu na znaczną liczbę danych, które mogą być zatrzymywane w sposób ciągły, grozi nieproporcjonalnym ich wykorzystaniem i nadużyciem (zob. analogicznie 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, pkt 119), jest sprzeczne z wymogiem sformułowanym w motywie 25 dyrektywy, zgodnie z którym te dane powinny być zatrzymywane na okres niezbędny i proporcjonalny do zamierzonych celów, biorąc pod uwagę, że prawodawca Unii chciał zapewnić jak najwyższy poziom ochrony danych PNR, które pozwalają na bezpośrednią identyfikację osób zainteresowanych.

257 Tak więc, jeśli chodzi o pasażerów lotniczych, co do których ani podczas wstępnej oceny, o której mowa w art. 6 ust. 2 lit. a) dyrektywy PNR, ani podczas ewentualnych sprawdzeń dokonywanych w okresie sześciu miesięcy, o którym mowa w art. 12 ust. 2 tej dyrektywy, ani w innych okolicznościach nie wykryto istnienia jakichkolwiek obiektywnych przesłanek wskazujących na to, że mogą stanowić ryzyko w zakresie przestępstw terrorystycznych lub poważnej przestępczości, które mają obiektywny związek, choćby pośredni, z lotniczym przewozem pasażerów, nie wydaje się, by istniał, w takich okolicznościach, związek, nawet pośredni, między danymi PNR tych pasażerów i celem realizowanym przez przedmiotową dyrektywę, który uzasadniałby zatrzymanie tych danych [zob. analogicznie opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 204, 205].

258 Trwałe przechowywanie danych PNR ogółu pasażerów lotniczych po upływie pierwotnego okresu sześciu miesięcy nie wydaje się być zatem ograniczone do tego, co ściśle konieczne [zob. analogicznie opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 206].

259 Jednakże w zakresie, w jakim w poszczególnych wypadkach zostaną zidentyfikowane obiektywne elementy, takie jak dane PNR pasażerów, które były źródłem potwierdzonego wyniku pozytywnego, pozwalające na uznanie, że określeni pasażerowie mogliby stanowić zagrożenie

w zakresie przestępstw terrorystycznych lub poważnej przestępczości, przechowywanie ich danych PNR wydaje się dopuszczalne po upływie tego pierwotnego okresu [zob. analogicznie opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 207 i przytoczone tam orzecznictwo].

260 W takim przypadku identyfikacja wskazanych obiektywnych elementów pozwoli bowiem na stworzenie związku pomiędzy celami realizowanymi przez przetwarzanie danych na podstawie dyrektywy PNR, tak że zatrzymanie danych PNR dotyczących rzeczonych pasażerów będzie uzasadnione przez maksymalny okres dopuszczony dyrektywą, to jest przez okres pięciu lat.

261 W niniejszej sprawie w zakresie, w jakim uregulowanie rozpatrywane w postępowaniu głównym przewiduje generalny, pięcioletni okres zatrzymania danych PNR, mający zastosowanie do wszystkich pasażerów, w tym takich, co do których ani podczas wstępnej oceny, o której mowa w art. 6 ust. 2 lit. a) dyrektywy PNR, ani podczas ewentualnych sprawdzeń dokonywanych w pierwotnym okresie sześciu miesięcy, ani w innych okolicznościach nie wykryto istnienia jakichkolwiek obiektywnych przesłanek wskazujących na to, że mogą stanowić ryzyko w zakresie przestępstw terrorystycznych lub poważnej przestępczości, uregulowanie to może naruszać art. 12 ust. 1 tej dyrektywy, w związku z art. 7 i 8 oraz art. 52 ust. 1 karty, o ile nie można poddać go wykładni zgodnej z tymi postanowieniami karty, czego ustalenie należy do sądu odsyłającego.

262 Biorąc pod uwagę powyższe rozważania, na pytanie ósme należy odpowiedzieć w ten sposób, że art. 12 ust. 1 dyrektywy PNR, w związku z art. 7 i 8 oraz art. 52 ust. 1 karty, należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu, które przewiduje ogólny okres zatrzymywania danych wynoszący pięć lat, mający zastosowanie bez rozróżnienia do wszystkich pasażerów, w tym do takich, co do których ani podczas wstępnej oceny, o której mowa w art. 6 ust. 2 lit. a) tej dyrektywy, ani podczas ewentualnych sprawdzeń dokonywanych w okresie sześciu miesięcy, o którym mowa w art. 12 ust. 2 wspomnianej dyrektywy, ani w innych okolicznościach nie wykryto istnienia jakichkolwiek obiektywnych przesłanek wskazujących na to, że mogą stanowić ryzyko w zakresie przestępstw terrorystycznych lub poważnej przestępczości, które mają obiektywny związek, choćby pośredni, z lotniczym przewozem pasażerów.

F. W przedmiocie pytania dziewiątego lit. a)

263 Poprzez pytanie dziewiąte lit. a) sąd odsyłający dąży zasadniczo do ustalenia, czy dyrektywa API jest ważna w świetle art. 3 ust. 2 TUE oraz art. 45 karty, wychodząc z założenia, że ustanowione w niej obowiązki mają zastosowanie do lotów wewnątrzunijnych.

264 Jak wskazał rzecznik generalny w pkt 277 opinii oraz jak zauważyły Rada, Komisja i większa liczba rządów państw członkowskich, to założenie jest błędne.

265 Otóż art. 3 ust. 1 dyrektywy API przewiduje, że państwa członkowskie mają obowiązek podjąć niezbędne kroki do ustanowienia zobowiązania dla przewoźników do przesyłania na wniosek organów odpowiedzialnych za przeprowadzanie kontroli osób na granicach zewnętrznych, przed końcem kontroli, informacji dotyczących pasażerów, których będą wprowadzać przez autoryzowane przejścia graniczne, przez które te osoby wchodzą na terytorium państwa członkowskiego. Dane te są przekazywane, zgodnie z art. 6 ust. 1 tej dyrektywy, do organów odpowiedzialnych za przeprowadzanie kontroli osób na granicach zewnętrznych, przez które pasażer wchodzi na przedmiotowe terytorium oraz są przetwarzane w warunkach przewidzianych przez ten ostatni przepis.

266 Ze wskazanych przepisów, w związku z art. 2 lit. a), b) i d) dyrektywy API, w których zdefiniowano pojęcia, odpowiednio, „przewoźnika", „granic zewnętrznych" i „przejścia granicznego", jasno bowiem wynika, że dyrektywa ta nakłada na przewoźników lotniczych obowiązek przekazywania danych, o których mowa w art. 3 ust. 2, organom odpowiedzialnym za przeprowadzanie kontroli na granicach zewnętrznych jedynie w przypadkach lotów przewożących pasażerów przez autoryzowane przejścia graniczne celem przekroczenia przez nich granic zewnętrznych państw członkowskich z państwami trzecimi i przewiduje przetwarzanie danych dotyczące tych lotów.

267 Dyrektywa ta nie nakłada zaś żadnego obowiązku dotyczącego danych pasażerów korzystających z lotów, podczas których przekraczane są jedynie granice wewnętrzne między państwami członkowskimi.

268 Należy dodać, że dyrektywa PNR, obejmując w ramach danych PNR, co wynika z jej motywu 9 oraz jej art. 8 ust. 2, dane wskazane w art. 3 ust. 2 dyrektywy API, zbierane zgodnie z tą dyrektywą i zatrzymywane przez niektórych przewoźników lotniczych i przyznająca państwom członkowskim uprawnienie do zastosowania dyrektywy PNR, zgodnie z jej art. 2, do lotów wewnątrzunijnych, które definiuje, nie zmieniła ani brzmienia dyrektywy API, ani ograniczeń w niej przewidzianych.

269 Mając na uwadze powyższe, na pytanie dziewiąte lit. a) należy odpowiedzieć w ten sposób, że dyrektywę API należy intepretować w ten sposób, że nie ma ona zastosowania do lotów wewnątrzunijnych.

G. W przedmiocie pytania dziewiątego lit. b)

270 Chociaż w pytaniu dziewiątym lit. b) sąd odsyłający odnosi się do dyrektywy API, w związku z art. 3 ust. 2 TUE oraz art. 45 karty, z wniosku o wydanie orzeczenia w trybie prejudycjalnym wynika, że sąd ten pyta o zgodność systemu przekazywania danych pasażerów wprowadzonego ustawą z dnia 25 grudnia 2016 r. ze swobodnym przepływem osób oraz zniesieniem kontroli na granicach wewnętrznych przewidzianym przez prawo Unii w zakresie, w jakim system ten stosuje się nie tylko do przewozów powietrznych, ale także kolejowych, lądowych, a nawet morskich rozpoczynających się lub kończących w Belgii, wykonywanych w obrębie Unii, bez przekraczania granic zewnętrznych z państwami trzecimi.

271 Jak wynika z pkt 265– 269 niniejszego wyroku, dyrektywa API, która nie ma zastosowania do lotów wewnątrzunijnych i nie nakłada obowiązku przekazywania i przetwarzania danych pasażerów podróżujących drogą lotniczą lub innym środkiem transportu w obrębie Unii, bez przekraczania granic zewnętrznych z państwami trzecimi, nie jest właściwym aktem, by odpowiedzieć na to pytanie.

272 Jednakże pomimo że zgodnie z art. 67 ust. 2 TFUE Unia zapewnia brak kontroli osób na granicach wewnętrznych, art. 2 dyrektywy PNR, na którym ustawodawca belgijski oparł przyjęcie ustawy z dnia 25 grudnia 2016 r. będącej przedmiotem postępowania głównego, jak wynika z wniosku o wydanie orzeczenia w trybie prejudycjalnym, upoważnia państwa członkowskie do stosowania dyrektywy PNR do lotów wewnątrzunijnych.

273 W tych warunkach, celem udzielenia sądowi odsyłającemu użytecznej odpowiedzi, należy przeformułować pytanie dziewiąte lit. b) tak, by zasadniczo zmierzało do ustalenia, czy prawo Unii, a w szczególności art. 2 dyrektywy PNR, w związku z art. 3 ust. 2 TUE, art. 67 ust. 2 TFUE oraz art. 45 karty, należy interpretować w ten sposób, że stoi na przeszkodzie uregulowaniu

krajowemu, które wprowadza system przekazywania przez przewoźników i operatorów turystycznych oraz przetwarzania przez właściwe organy danych PNR dotyczących lotów i przewozów odbywających się innymi środkami transportu wewnątrz Unii, rozpoczynających się lub kończących w państwie członkowskim, w którym przyjęto to uregulowanie, lub przebiegających przez to państwo członkowskie.

274 Przede wszystkim, art. 45 karty dotyczy swobody przemieszczania się osób, która stanowi jedną z podstawowych swobód rynku wewnętrznego [zob. podobnie wyrok z dnia 22 czerwca 2021 r., Ordre des barreaux francophones et germanophone i in. (Środki zapobiegawcze mające na celu zapewnienie wydalenia), C-718/19, EU:C:2021:505, pkt 54].

275 Artykuł ten gwarantuje w swoim ust. 1 każdemu obywatelowi Unii prawo do swobodnego przemieszczania się i przebywania na terytorium państw członkowskich, to jest prawo, które zgodnie z wyjaśnieniami dotyczącymi karty praw podstawowych (Dz.U. 2007, C 303, s. 17) jest tożsame z tym zapewnionym w art. 20 ust. 2 akapit pierwszy lit. a) TFUE i jest wykonywane, zgodnie z art. 20 ust. 2 akapit drugi TFUE oraz art. 52 ust. 2 karty, na warunkach i w granicach określonych przez traktaty i środki przyjęte w ich wykonaniu.

276 Następnie, zgodnie z art. 3 ust. 2 TUE, Unia zapewnia swoim obywatelom przestrzeń wolności, bezpieczeństwa i sprawiedliwości bez granic wewnętrznych, w której zagwarantowana jest swoboda przepływu osób, w powiązaniu z właściwymi środkami w odniesieniu do kontroli granic zewnętrznych, jak również zapobiegania i zwalczania przestępczości. Z kolei, zgodnie z art. 67 ust. 2 TFUE, Unia zapewnia brak kontroli osób na granicach wewnętrznych i rozwija wspólną politykę, w szczególności w dziedzinie kontroli granic zewnętrznych.

277 Zgodnie z utrwalonym orzecznictwem Trybunału przepis prawa krajowego, który stawia w mniej korzystnej sytuacji niektórych obywateli państwa członkowskiego z tego tylko powodu, że korzystają oni ze swobody przemieszczania się i pobytu w innym państwie członkowskim, stanowi ograniczenie swobód gwarantowanych zgodnie z art. 45 ust. 1 karty każdemu obywatelowi Unii (zob. podobnie, w odniesieniu do art. 21 ust. 1 TFUE, wyroki: z dnia 8 czerwca 2017 r., Freitag, C-541/15, EU:C:2017:432, pkt 35 i przytoczone tam orzecznictwo; z dnia 19 listopada 2020 r., ZW, C-454/19, EU:C:2020:947, pkt 30).

278 Tymczasem uregulowanie krajowe rozpatrywane w postępowaniu głównym, które obejmuje systemem wprowadzonym dyrektywą PNR nie tylko loty pozaunijne, ale także, na podstawie art. 2 ust. 1 tej dyrektywy, loty wewnątrzunijne oraz, mimo że nie jest to przewidziane w tym przepisie, przewozy w ramach Unii dokonywane za pomocą innych środków transportu, skutkuje systematycznym i ciągłym przetwarzaniem danych PNR każdego pasażera przemieszczającego się w ten sposób wewnątrz Unii, korzystającego ze swobody przepływu osób.

279 Jak stwierdzono w pkt 98–111 niniejszego wyroku, przetwarzanie danych pasażerów lotów pozaunijnych i wewnątrzunijnych wynikające z systemu wprowadzonego dyrektywą PNR skutkuje istotną ingerencją w prawa podstawowe osób zainteresowanych zagwarantowane w art. 7 i 8 karty. Waga tej ingerencji jest jeszcze większa w przypadku rozszerzenia zastosowania systemu na inne środki transportu wewnątrz Unii. Taka ingerencja może, z powodów opisanych w tychże punktach wyroku, zniechęcać, a tym samym powstrzymywać przed korzystaniem ze swobody przemieszczania się, w rozumieniu art. 45 karty, obywateli państw członkowskich, w których przyjęto takie uregulowanie, a ogólniej rzecz ujmując, obywateli Unii

przemieszczających się takimi środkami transportu wewnątrz Unii, którzy wyjeżdżają z lub przybywają do tych państw członkowskich, a zatem rzeczone uregulowanie ogranicza omawiane prawo podstawowe.

280 Zgodnie z utrwalonym orzecznictwem ograniczenie w swobodnym przemieszczaniu się osób może być uzasadnione jedynie wtedy, gdy jest oparte na obiektywnych względach i jest proporcjonalne do uzasadnionego celu realizowanego przez prawo krajowe. Środek jest proporcjonalny, gdy pozostając zdatnym do osiągnięcia zamierzonego celu, nie wykracza poza to, co jest konieczne do jego osiągnięcia (zob. podobnie wyrok z dnia 5 czerwca 2018 r., Coman i in., C-673/16, EU:C:2018:385, pkt 41 i przytoczone tam orzecznictwo).

281 Należy dodać, że środek krajowy, który może utrudniać korzystanie ze swobody przemieszczania się osób, tylko wtedy może być uzasadniony, gdy jest zgodny z gwarantowanymi w karcie prawami podstawowymi, nad których przestrzeganiem czuwa Trybunał (wyrok z dnia 14 grudnia 2021 r., Stolichna obshtina, rayon „Pancharevo", C-490/20, EU:C:2021:1008, pkt 58 i przytoczone tam orzecznictwo).

282 W szczególności, zgodnie z orzecznictwem przywołanym w pkt 115 i 116 niniejszego wyroku, nie można dążyć do celu interesu ogólnego bez uwzględnienia okoliczności, że należy pogodzić go z prawami podstawowymi, których dotyczy środek, dokonując zbilansowanego wyważenia między celem interesu ogólnego z jednej strony a rozpatrywanymi prawami z drugiej strony. Tak więc możliwość uzasadnienia przez państwa członkowskie ograniczenia prawa podstawowego gwarantowanego przez art. 45 ust. 1 karty powinna być oceniana z uwzględnieniem wagi ingerencji, którą zakłada takie ograniczenie, oraz przy sprawdzeniu, czy znaczenie celu interesu ogólnego realizowanego przez to ograniczenie ma związek z tą wagą.

283 Jak przypomniano w pkt 122 niniejszego wyroku, cel w postaci zwalczania przestępstw terrorystycznych i poważnej przestępczości realizowany przez dyrektywę PNR stanowi niewątpliwie cel interesu ogólnego Unii.

284 Jeśli chodzi o kwestię ustalenia, czy uregulowanie krajowe przyjęte celem dokonania transpozycji dyrektywy PNR, które rozszerza system wprowadzony tą dyrektywą na loty wewnątrzunijne oraz na inne środki transportu wewnątrz Unii, jest zdatne do realizacji zamierzonego celu, z informacji zawartych w aktach sprawy, którymi dysponuje Trybunał, wynika, że wykorzystanie danych PNR pozwala zidentyfikować osoby, które nie były podejrzane o udział w przestępstwach terrorystycznych i poważnej przestępczości, a które powinny być poddane pogłębionemu sprawdzeniu, tak więc takie uregulowanie wydaje się odpowiednie do osiągnięcia celu zwalczania przestępstw terrorystycznych i poważnej przestępczości.

285 Co do niezbędnego charakteru takiego uregulowania korzystanie przez państwa członkowskie z uprawnienia przewidzianego w art. 2 ust. 1 dyrektywy PNR, w związku z art. 7 i 8 karty, musi ograniczać się do tego co ściśle konieczne do realizacji celu w świetle wymogów opisanych w pkt 163–174 niniejszego wyroku.

286 Wymogi te mają zastosowanie tym bardziej do przypadków, w których system wprowadzony dyrektywą PNR jest stosowany do innych środków transportu wewnątrz Unii.

287 Jak wynika z informacji zawartych we wniosku o wydanie orzeczenia w trybie prejudycjalnym, uregulowanie krajowe rozpatrywane w postępowaniu głównym dokonuje jednoczesnej transpozycji dyrektywy PNR, dyrektywy API i częściowo dyrektywy 2010/65. W tym celu

przewiduje zastosowanie systemu przewidzianego w dyrektywie PNR do wszystkich lotów wewnątrzunijnych, przewozów kolejowych, lądowych i morskich odbywających się wewnątrz Unii, które rozpoczynają się lub kończą w Belgii, lub przebiegają przez Belgię, i objęcie nim także operatorów turystycznych, przy czym realizuje także inne cele niż jedynie zwalczanie przestępstw terrorystycznych i poważnej przestępczości. Zgodnie z tymi samymi informacjami wydaje się, że wszystkie dane zbierane w ramach systemu ustanowionego omawianym uregulowaniem krajowym są gromadzone przez JIP w jednej bazie danych obejmującej dane PNR, w tym dane, o których mowa w art. 3 ust. 2 dyrektywy API, wszystkich pasażerów przewozów objętych tym uregulowaniem.

288 W tym względzie w zakresie, w jakim sąd odsyłający odniósł się do celu ulepszenia kontroli na granicach i walki z nielegalną imigracją w pytaniu dziewiątym lit. b), czyli celu zamierzonego przez dyrektywę API, należy przypomnieć, że jak wynika z pkt 233, 234 oraz 237 niniejszego wyroku, wykaz celów realizowanych przez przetwarzanie danych PNR na mocy dyrektywy PNR ma charakter wyczerpujący, w związku z czym ustawa krajowa zezwalająca na przetwarzanie danych PNR gromadzonych zgodnie z tą dyrektywą do celów innych niż w niej przewidziane, a mianowicie do celu ulepszenia kontroli na granicach wewnętrznych i walki z nielegalną imigracją, jest sprzeczna z art. 6 dyrektywy PNR w związku z postanowieniami karty.

289 Ponadto, jak wynika z pkt 235 niniejszego wyroku, państwa członkowskie nie mogą tworzyć jednej bazy danych zawierającej zarówno dane PNR zbierane na podstawie dyrektywy PNR i dotyczące lotów pozaunijnych i wewnątrzunijnych, jak i dane pasażerów innych środków transportu oraz dane, o których mowa w art. 3 ust. 2 dyrektywy API, zwłaszcza jeśli ta baza danych może służyć nie tylko do celów wskazanych w art. 1 ust. 2 dyrektywy PNR, ale także do innych celów.

290 Wreszcie i w każdym razie, jak podniósł rzecznik generalny w pkt 281 opinii, art. 28–31 ustawy z dnia 25 grudnia 2016 r. mogą być zgodne z prawem Unii, w szczególności art. 67 ust. 2 TFUE, jedynie pod warunkiem, że będą interpretowane i stosowane jako obejmujące jedynie przekazywanie i przetwarzanie danych API pasażerów przekraczających granice zewnętrzne Belgii z państwami trzecimi. A zatem środek, za pomocą którego państwo członkowskie rozszerzyłoby stosowanie przepisów dyrektywy API w celu ulepszenia kontroli na granicach zewnętrznych i walki z nielegalną imigracją na loty wewnątrzunijne i a fortiori na inne środki przewozu, który rozpoczyna się, kończy, lub przebiega przez to państwo członkowskie, w szczególności w zakresie obowiązku przekazywania danych pasażerów, o których mowa w art. 3 ust. 1 tej dyrektywy, byłby równoznaczny z zezwoleniem właściwym organom na sprawdzanie w sposób systematyczny, czy pasażerowie przekraczający granice wewnętrzne tego państwa członkowskiego mogą otrzymać zezwolenie na wejście na jego terytorium lub jego opuszczenie, a tym samym wywoływałby skutek tożsamy z kontrolami przeprowadzanymi na granicach zewnętrznych z państwami trzecimi.

291 W świetle całokształtu powyższych rozważań na pytanie dziewiąte lit. b) należy odpowiedzieć w ten sposób, że prawo Unii, a zwłaszcza art. 2 dyrektywy PNR, w związku z art. 3 ust. 2 TUE, art. 67 ust. 2 TFUE oraz art. 45 karty, należy intepretować w ten sposób, że stoi ono na przeszkodzie:

– uregulowaniu krajowemu, które przewiduje, przy braku rzeczywistego i aktualnego lub dającego się przewidzieć zagrożenia terrorystycznego, z którym zmaga się państwo członkowskie, system przekazywania przez przewoźników lotniczych i operatorów podróży, a także przetwarzania przez właściwe organy, danych PNR dotyczących wszystkich lotów wewnątrzunijnych i przewozów realizowanych innymi środkami transportu wewnątrz Unii,

które rozpoczynają się, kończą lub przebiegają przez to państwo członkowskie, w celu zwalczania przestępstw terrorystycznych i poważnej przestępczości. W takim przypadku stosowanie systemu wprowadzonego dyrektywą PNR powinno być ograniczone do przekazywania i przetwarzania danych PNR lotów lub innych przewozów dotyczących, w szczególności, niektórych połączeń lub planów podróży, lub niektórych lotnisk, dworców lub portów morskich, co do których istnieją przesłanki uzasadniające takie stosowanie. To do danego państwa członkowskiego należy wybór lotów wewnątrzunijnych lub przewozów odbywających się za pomocą innych środków transportu wewnątrz Unii, dla których takie przesłanki istnieją, oraz dokonywanie regularnego przeglądu takiego stosowania, w zależności od zmiany warunków, które uzasadniają ich wybór, celem zapewnienia, że zastosowanie przedmiotowego systemu do takich lotów lub takich innych przewozów jest cały czas ograniczone do tego, co ściśle konieczne, i

– uregulowaniu krajowemu przewidującemu zastosowanie wspomnianego systemu przekazywania i przetwarzania danych do celów ulepszenia kontroli na granicach i zwalczania nielegalnej imigracji.

H. W przedmiocie pytania dziesiątego

292 Poprzez pytanie dziesiąte sąd odsyłający dąży zasadniczo do ustalenia, czy prawo Unii należy interpretować w ten sposób, że sąd krajowy mógłby ograniczyć w czasie skutki stwierdzenia niezgodności z prawem, którego ma on dokonać na podstawie prawa krajowego, uregulowania krajowego nakładającego na przewoźników lotniczych, kolejowych i lądowych, a także operatorów podróży obowiązek przekazywania danych PNR i przewidującego przetwarzanie i zatrzymanie tych danych niezgodne z przepisami dyrektywy PNR, w związku z art. 3 ust. 2 TUE, art. 67 ust. 2 TFUE, art. 7, 8 i 45 oraz art. 52 ust. 1 karty.

293 Zasada pierwszeństwa prawa Unii ustanawia prymat prawa Unii nad prawem państw członkowskich. Zasada ta nakłada zatem na wszystkie organy państw członkowskich obowiązek zapewnienia pełnej skuteczności różnych norm prawa Unii, a prawo państw członkowskich nie może mieć wpływu na skuteczność przyznaną tym różnym normom na terytorium wspomnianych państw. Zgodnie z tą zasadą w razie niemożności dokonania wykładni uregulowania krajowego w sposób zgodny z wymogami określonymi w prawie Unii, sąd krajowy, do którego należy w ramach jego kompetencji stosowanie przepisów prawa Unii, jest zobowiązany zapewnić pełną ich skuteczność, w razie potrzeby powstrzymując się od stosowania, z własnej inicjatywy, wszelkich sprzecznych z nimi przepisów prawa krajowego, także późniejszych, bez konieczności żądania uprzedniego uchylenia tych przepisów w drodze ustawodawczej lub w jakimkolwiek innym trybie konstytucyjnym ani bez konieczności oczekiwania na takie uchylenie (wyroki: z dnia 15 lipca 1964 r., Costa, 6/64, EU:C:1964:66, s. 1159 i 1160; 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, pkt 214, 215; z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 118).

294 Jedynie Trybunał może, w drodze wyjątku oraz kierując się nadrzędnymi względami pewności prawa, tymczasowo zawiesić wywierany przez prawo Unii skutek w postaci uchylenia przepisów prawa krajowego sprzecznych z prawem Unii. Takie ograniczenie w czasie skutków wykładni prawa Unii dokonanej przez Trybunał może zostać orzeczone jedynie w samym wyroku, w którym Trybunał rozstrzyga w przedmiocie wykładni, o którą się do niego zwrócono. Do naruszenia pierwszeństwa i jednolitego stosowania prawa Unii doszłoby, gdyby sądy krajowe były

uprawnione do przyznania, choćby tymczasowo, przepisom krajowym pierwszeństwa przed prawem Unii, z którym te przepisy są sprzeczne (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 119 i przytoczone tam orzecznictwo).

295 W przeciwieństwie do pominięcia obowiązku proceduralnego takiego jak uprzednia ocena oddziaływania przedsięwzięcia w szczególnej dziedzinie ochrony środowiska w sprawie, w której zapadł wyrok z dnia 29 lipca 2019 r., Inter-Environnement Wallonie i Bond Beter Leefmilieu Vlaanderen (C-411/17, EU:C:2019:622, pkt 175, 176, 179, 181) i w której Trybunał zaakceptował tymczasowe zawieszenie skutku uchylenia przepisów, naruszenie norm dyrektywy PNR, w związku z art. 7, 8 i 45 oraz art. 52 ust. 1 karty nie może być przedmiotem konwalidacji w drodze procedury analogicznej do tej, dokonanej w przywołanej sprawie. Utrzymanie bowiem w mocy skutków uregulowania krajowego, takiego jak ustawa z dnia 25 grudnia 2016 r., oznaczałoby, że nadal nakłada ono na przewoźników lotniczych i innych przewoźników oraz operatorów podróży obowiązki sprzeczne z prawem Unii i pociągające za sobą istotną ingerencję w prawa podstawowe osób, których dane są przekazywane, zatrzymywane i przetwarzane, a także ograniczenie swobody przemieszczania się osób, które wykracza poza to, co niezbędne (zob. analogicznie wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 122 i przytoczone tam orzecznictwo).

296 W związku z tym sąd odsyłający nie może ograniczyć w czasie skutków stwierdzenia niezgodności z prawem, którego ma on dokonać na podstawie prawa krajowego, w odniesieniu do uregulowania krajowego rozpatrywanego w postępowaniu głównym (zob. analogicznie wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 123 i przytoczone tam orzecznictwo).

297 Wreszcie, jako że sąd odsyłający pyta o wpływ stwierdzenia ewentualnej niezgodności ustawy z dnia 25 grudnia 2016 r. z przepisami dyrektywy PNR, w związku z postanowieniami karty, na dopuszczalność i możliwość wykorzystania w ramach postępowań karnych dowodów i informacji uzyskanych za pomocą danych przekazanych przez określonych przewoźników i operatorów podróży, wystarczy przywołać odpowiednie orzecznictwo Trybunału, w szczególności zasady przywołane w pkt 41–44 wyroku z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej) (C-746/18, EU:C:2021:152), z którego wynika, że zgodnie z zasadą autonomii proceduralnej państw członkowskich kwestia tej dopuszczalności należy do prawa krajowego, z zastrzeżeniem poszanowania w szczególności zasad równoważności i skuteczności (zob. analogicznie wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 127).

298 W świetle powyższych rozważań odpowiedź na pytanie dziesiąte brzmi następująco: prawo Unii należy interpretować w ten sposób, że stoi ono na przeszkodzie temu, by sąd krajowy mógł ograniczyć w czasie skutki stwierdzenia niezgodności z prawem, którego ma on dokonać na podstawie prawa krajowego, uregulowania krajowego nakładającego na przewoźników lotniczych, kolejowych i lądowych, a także operatorów podróży obowiązek przekazywania danych PNR i przewidującego przetwarzanie i zatrzymanie tych danych niezgodne z przepisami dyrektywy PNR, w związku z art. 3 ust. 2 TUE, art. 67 ust. 2 TFUE, art. 7, 8 i 45 oraz art. 52 ust. 1 karty. Kwestia dopuszczalności dowodów uzyskanych w przedmiotowy sposób należy, zgodnie z zasadą autonomii proceduralnej państw członkowskich, do prawa krajowego, z zastrzeżeniem poszanowania w szczególności zasad równoważności i skuteczności.

IV. W przedmiocie kosztów

299 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 2 ust. 2 lit. d) oraz art. 23 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych) należy interpretować w ten sposób, iż rozporządzenie to ma zastosowanie do przetwarzania danych osobowych przewidzianego przez uregulowanie krajowe dokonujące transpozycji do prawa krajowego jednocześnie przepisów dyrektywy Rady 2004/82/WE z dnia 29 kwietnia 2004 r. w sprawie zobowiązania przewoźników do przekazywania danych pasażerów, dyrektywy Parlamentu Europejskiego i Rady 2010/65/UE z dnia 20 października 2010 r. w sprawie formalności sprawozdawczych dla statków wchodzących do lub wychodzących z portów państw członkowskich i uchylającej dyrektywę 2002/6/WE oraz dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, w zakresie, po pierwsze, przetwarzania danych dokonywanego przez podmioty prywatne, a po drugie, dokonywanego przez organy publiczne przetwarzania danych objętego dyrektywą 2004/82, dyrektywą 2010/65 lub obiema tymi dyrektywami. Rozporządzenie to nie ma natomiast zastosowania do przewidzianego przez to uregulowanie przetwarzania danych objętego jedynie dyrektywą 2016/681, które jest dokonywane przez jednostkę do spraw informacji o pasażerach (JIP) lub właściwe organy w celach wskazanych w art. 1 ust. 2 tej dyrektywy.**

2) **Jako że wykładnia dyrektywy 2016/681, w świetle art. 7, 8 i 21 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej, zapewnia zgodność tej dyrektywy ze wskazanymi postanowieniami karty, analiza pytań od drugiego do czwartego oraz pytania szóstego nie doprowadziła do żadnych ustaleń, które mogłyby mieć wpływ na ważność owej dyrektywy.**

3) **Artykuł 6 dyrektywy 2016/681, w związku z art. 7 i 8 oraz art. 52 ust. 1 karty praw podstawowych, należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu, które zezwala na przetwarzanie danych dotyczących przelotu pasażera (danych PNR), gromadzonych zgodnie z tą dyrektywą, do celów innych niż wprost wskazane w art. 1 ust. 2 owej dyrektywy.**

4) **Artykuł 12 ust. 3 lit. b) dyrektywy 2016/681 należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu, zgodnie z którym organ ustanowiony jako jednostka do spraw informacji o pasażerach (JIP) ma jednocześnie status właściwego organu krajowego uprawnionego do udzielania zgody na ujawnienie danych PNR po upływie okresu sześciu miesięcy od przekazania tych danych do JIP.**

5) Artykuł 12 ust. 1 dyrektywy 2016/681, w związku z art. 7 i 8 oraz art. 52 ust. 1 karty praw podstawowych, należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu, które przewiduje ogólny okres zatrzymywania danych wynoszący pięć lat, mający zastosowanie bez rozróżnienia do wszystkich pasażerów, w tym do takich, co do których ani podczas wstępnej oceny, o której mowa w art. 6 ust. 2 lit. a) tej dyrektywy, ani podczas ewentualnych sprawdzeń dokonywanych w okresie sześciu miesięcy, o którym mowa w art. 12 ust. 2 wspomnianej dyrektywy, ani w innych okolicznościach nie wykryto istnienia jakichkolwiek obiektywnych przesłanek wskazujących na to, że mogą stanowić ryzyko w zakresie przestępstw terrorystycznych lub poważnej przestępczości, które mają obiektywny związek, choćby pośredni, z lotniczym przewozem pasażerów.

6) Dyrektywę 2004/82 należy interpretować w ten sposób, że nie ma ona zastosowania do lotów regularnych lub nieregularnych, obsługiwanych przez przewoźnika lotniczego, odbywających się z terytorium państwa członkowskiego, z zaplanowanym lądowaniem na terytorium co najmniej jednego państwa członkowskiego, bez postojów na terytorium państw trzecich (lotów wewnątrzunijnych).

7) Prawo Unii, w szczególności art. 2 dyrektywy 2016/681, w związku z art. 3 ust. 2 TUE, art. 67 ust. 2 TFUE oraz art. 45 karty praw podstawowych należy interpretować w ten sposób, że stoi ono na przeszkodzie:

– uregulowaniu krajowemu, które przewiduje, przy braku rzeczywistego i aktualnego lub dającego się przewidzieć zagrożenia terrorystycznego, z którym zmaga się państwo członkowskie, system przekazywania przez przewoźników lotniczych i operatorów podróży, a także przetwarzania przez właściwe organy, danych PNR dotyczących wszystkich lotów wewnątrzunijnych i przewozów realizowanych innymi środkami transportu wewnątrz Unii, które rozpoczynają się, kończą lub przebiegają przez to państwo członkowskie, w celu zwalczania przestępstw terrorystycznych i poważnej przestępczości. W takim przypadku stosowanie systemu wprowadzonego dyrektywą 2016/681 powinno być ograniczone do przekazywania i przetwarzania danych PNR lotów lub innych przewozów dotyczących, w szczególności, niektórych połączeń lub planów podróży, lub niektórych lotnisk, dworców lub portów morskich, co do których istnieją przesłanki uzasadniające takie stosowanie. To do danego państwa członkowskiego należy wybór lotów wewnątrzunijnych lub przewozów odbywających się za pomocą innych środków transportu wewnątrz Unii, dla których takie przesłanki istnieją, oraz dokonywanie regularnego przeglądu takiego stosowania, w zależności od zmiany warunków, które uzasadniają ich wybór, celem zapewnienia, że zastosowanie przedmiotowego systemu do takich lotów lub takich innych przewozów jest cały czas ograniczone do tego, co ściśle konieczne, i

– uregulowaniu krajowemu przewidującemu zastosowanie wspomnianego systemu przekazywania i przetwarzania danych do celów ulepszenia kontroli na granicach i zwalczania nielegalnej imigracji.

8) Prawo Unii należy interpretować w ten sposób, że stoi ono na przeszkodzie temu, by sąd krajowy mógł ograniczyć w czasie skutki stwierdzenia niezgodności z prawem, którego ma on dokonać na podstawie prawa krajowego, uregulowania krajowego nakładającego na przewoźników lotniczych, kolejowych i lądowych, a także operatorów podróży obowiązek przekazywania danych PNR i przewidującego przetwarzanie i zatrzymanie

tych danych niezgodne z przepisami dyrektywy PNR, w związku z art. 3 ust. 2 TUE, art. 67 ust. 2 TFUE, art. 7, 8 i 45 oraz art. 52 ust. 1 karty. Kwestia dopuszczalności dowodów uzyskanych w przedmiotowy sposób należy, zgodnie z zasadą autonomii proceduralnej państw członkowskich, do prawa krajowego, z zastrzeżeniem poszanowania w szczególności zasad równoważności i skuteczności.

Podpisy