

Sprawa C-817/19**Streszczenie wniosku o wydanie orzeczenia w trybie prejudycjalnym zgodnie z art. 98 § 1 regulaminu postępowania przed Trybunałem Sprawiedliwości****Data wpływu:**

31 października 2019 r.

Oznaczenie sądu odsyłającego:

Cour constitutionnelle (Belgia)

Data wydania postanowienia o wystąpieniu z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym:

17 października 2019 r.

Strona skarżąca:

ASBL „Ligue des droits humains”

I. Przedmiot skargi i stanowiska stron

- 1 Ustawodawca belgijski przyjął loi du 25 décembre 2016 relative au traitement des données des passagers (ustawę z dnia 25 grudnia 2016 r. o przetwarzaniu danych pasażerów, Moniteur belge z dnia 25 stycznia 2017 r., zwaną dalej również „ustawą PNR”) zasadniczo w celu dokonania transpozycji:
 - 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 (zwanej dalej również „dyrektywą PNR”)
 - dyrektywy Rady 2004/82/WE z dnia 29 kwietnia 2004 r. w sprawie zobowiązania przewoźników do przekazywania danych pasażerów (zwanej dalej również „dyrektywą API”).
- 2 Ustawa PNR nakłada na różne sektory przewozu osób o charakterze międzynarodowym (lotnictwo, kolej, międzynarodowe przewozy drogowe i morskie) oraz na operatorów turystycznych obowiązek przekazywania danych ich pasażerów do bazy danych zarządzanej przez SPF Intérieur (Service public fédéral, ministerstwo spraw wewnętrznych).

- 3 W tym celu ustawa tworzy w ramach SPF Intérieur „jednostkę ds. informacji o pasażerach” (art. 12–14), w której skład wchodzi w szczególności delegowani członkowie służb policyjnych, celnych, bezpieczeństwa państwa, wywiadu i bezpieczeństwa, do których zadań należy w szczególności gromadzenie, przechowywanie i przetwarzanie danych pasażerów przekazywanych przez przewoźników oraz operatorzy turystyczni.
- 4 „Baza danych pasażerów” zawiera z jednej strony dane dotyczące rezerwacji, a z drugiej strony dane dotyczące rejestracji i wejścia na pokład [dane zwane „API” (Advance Passenger Information) i dane zwane „PNR” (Passenger Name Record)] (art. 9).
- 5 Dane te są przetwarzane w szczególności dla celów poszukiwania, ścigania i wykonywania kar dotyczących przestępstw, o których mowa w ustawie, jak również zapobiegania poważnym zakłóceniom bezpieczeństwa publicznego w kontekście radykalizacji postaw prowadzącej do aktów przemocy, monitorowania działalności przez służby wywiadowcze i bezpieczeństwa, poprawy kontroli osób na granicach zewnętrznych oraz w celu zwalczania nielegalnej imigracji (art. 8).
- 6 Dane można przetwarzać w ramach wstępnej oceny pasażerów (przed ich wyjazdem lub przyjazdem) (art. 24–26) lub w ramach wyszukiwań ad hoc (art. 27).
- 7 Ustawa przewiduje, że dane pasażerów są przechowywane w bazie danych pasażerów przez okres nieprzekraczający pięciu lat od chwili ich rejestracji (art. 18–23).
- 8 ASBL „Ligue des droits humains” krytykuje ustawę w odniesieniu do siedmiu następujących aspektów:
 - zasady wykonania ustawy z dnia 25 grudnia 2016 r. (art. 3 ust. 2 i art. 7 ust. 3);
 - pojęcia „dokumentów tożsamości” i „dokumentów podróży” (art. 7 ust. 1 i 2);
 - dane, o których mowa (art. 4 pkt 9 i 9);
 - pojęcie „pasażera” (art. 4 pkt 10);
 - cele przetwarzania danych „PNR” (art. 8);
 - zarządzanie bazą danych pasażerów i przetwarzanie danych w ramach wstępnej oceny pasażerów i wyszukiwań ad hoc (art. 12–16 i 24–27 oraz art. 50 i 51);
 - okres przechowywania danych PNR (art. 18).
- 9 Wskazując na nieprawidłowości tej ustawy w tym względzie, wniosła ona do Cour constitutionnelle (trybunału konstytucyjnego) skargę o stwierdzenie jej nieważności opartą na dwóch zarzutach.

- 10 Zarzut pierwszy dotyczy zasadniczo art. 23 rozporządzenia (UE) 2016/679¹, art. 7, 8 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej „kartą”) oraz art. 8 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności (zwanej dalej „EKPC”).
- 11 Utrzymuje ona zasadniczo, że ingerencja w prawo do poszanowania życia prywatnego i w prawo do ochrony danych osobowych jest niedopuszczalna, ponieważ nie odpowiada kryteriom zgodności z prawem, konieczności i proporcjonalności.
- 12 Przede wszystkim ustawa PNR przyznaje szeroki zakres uznania władzy wykonawczej, którą zobowiązuje do określenia, w drodze rozporządzenia królewskiego, pewnych istotnych elementów z naruszeniem zasady legalności, która wymaga, aby ingerencja była przewidziana w ustawie, a w przypadku delegacji tego uprawnienia królowi, aby istotne elementy były przewidziane w ustawie w sposób wystarczająco dokładny i szczegółowy.
- Ponadto zaskarżona ustawa nie realizuje zgodnego z prawem celu. Przewiduje ona bowiem wstępną ocenę zwaną „pre-screening”, która polega na ocenie ryzyka, jakie stanowią pasażerowie przed przyjazdem, przejazdem lub opuszczeniem kraju.
- 13 Skarżąca kwestionuje następnie konieczność przyjęcia zaskarżonych środków dla realizacji celu, o którym mowa.
- Utrzymuje ona, że mapowanie danych, które znacznie mniej ingeruje w życie prywatne niż utworzenie bazy danych, mogłoby również umożliwić osiągnięcie zamierzonego celu.
- 14 Wreszcie podnosi ona, że zaskarżona ustawa nie realizuje zasady proporcjonalności, ponieważ dane są gromadzone przez operatorów w sposób jednakowy i uogólniony i przekazywane właściwym organom do celów przechowywania przez okres pięciu lat bez rozróżnienia, rozgraniczenia, ograniczenia lub wyjątku w zależności od zamierzonego celu.
- 15 Dokładniej rzecz ujmując, ustawa narusza zasadę proporcjonalności, w odniesieniu do (a) jej zakresu stosowania oraz kategorii danych, o których mowa, (b) do przetwarzania danych, które ustanawia; c) jej celów oraz d) okresu przechowywania danych.

¹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.U. 2016, L 119, s. 1 (zwane dalej również „RODO”).

- 16 Przede wszystkim zaskarżona ustawa określa w sposób bardzo szeroki gromadzone dane, które wykraczają w sposób oczywisty poza to, co jest ściśle niezbędne.
- 17 Skarżąca stwierdza, że wydaje się – choć ustawa nie jest jasna – iż pre-screening powinien być wykonywany w centralnej bazie danych JIP za pomocą określonych wcześniej kryteriów służących jako wskaźniki zagrożenia. Tymczasem ustawa PNR nie definiuje ani konkretnego charakteru baz danych wykorzystywanych do poszukiwania korelacji, ani sposobów tego poszukiwania. Ustawa PNR nie przewiduje też, że ta korelacja jest ograniczona do baz danych wykorzystywanych w związku ze zwalczaniem terroryzmu i poważnych przestępstw.
- 18 Skarżąca krytykuje także, że ustawa przewiduje wyszukiwania ad hoc, jednak nie precyzuje faktycznie dostępnych danych.
- 19 Skarżąca podważa również cele przetwarzania danych, które są zdecydowanie szersze niż te określone w dyrektywie PNR, takie jak zwalczanie nielegalnej imigracji, działalności, która może stanowić zagrożenie dla podstawowych interesów państwa, czy też walka z „radikalizacją postaw prowadzącą do aktów przemocy”, zdefiniowaną wyłącznie w okólniku.
- 20 Wreszcie skarżąca podważa wynoszący pięć lat okres przechowywania danych. Prawodawca nie uzasadnił w żaden sposób wyboru maksymalnego terminu dozwolonego przez dyrektywę PNR, który świadczy o nieproporcjonalnym charakterze środka.
- 21 Rada ministrów (która broni ustawy) podnosi tytułem głównym niedopuszczalność zarzutu pierwszego w zakresie, w jakim dotyczy on naruszenia art. 23 RODO, ponieważ zarówno z motywu 19 RODO, jak i z art. 1 dyrektywy PNR wynika jasno, że przetwarzanie danych PNR nie wchodzi w zakres RODO, lecz współpracy sądowej i policyjnej między państwami członkowskimi oraz dyrektywy (UE) 2016/680².
- 22 Ponadto utrzymuje ona, że zasada legalności nie została naruszona, ponieważ ustawa zawiera istotne elementy środków, które przewiduje, zaś upoważnienie dla króla jest wystarczająco precyzyjne. Zresztą według Europejskiego Trybunału Praw Człowieka wymóg zgodności z prawem w znaczeniu materialnym polega na tym, że akty regulacyjne muszą odpowiadać pojęciu „ustawy” w rozumieniu Europejskiej konwencji praw człowieka.

² Dyrektywa 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 uchyłająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. 2016, L 119, s. 89) (zwana dalej „dyrektywą 2016/680”).

Ustawa PNR ma na celu zapewnienie bezpieczeństwa publicznego, umożliwiając nie tylko ściganie przestępstw terrorystycznych lub poważnej przestępczości, ale także zapobieganie tym przestępstwom poprzez przeprowadzenie wstępnej analizy zgromadzonych danych. Trybunał Sprawiedliwości przyznał, że cele te są zgodne z prawem w rozumieniu art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej zarówno w wyroku z dnia 8 kwietnia 2014 r., *Digital Rights Ireland i in.*, C-293/12 i C-594/12, EU:C:2014:238, jak i w opinii 1/15 (umowa PNR UE-Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592.

- 23 Rada ministrów uważa, że zaskarżone środki są proporcjonalne.
- 24 W odniesieniu do utworzenia bazy danych „pasażerów” rada ministrów podnosi, że strona skarżąca poprzestaje na stwierdzeniu, bez wykazania jego słuszności, iż mapowanie danych mogłoby umożliwić osiągnięcie zamierzonego celu i stanowiłoby mniejszą ingerencję w prawo do poszanowania życia prywatnego. Dodaje ona, że zwykle mapowanie nie jest wystarczające do dokonania wstępnej oceny mającej na celu określenie zagrożeń dla bezpieczeństwa. Utworzenie bazy danych jest zresztą zgodne z wymogami motywu 25 dyrektywy PNR, który wzywa do przechowywania danych w okresie koniecznym do osiągnięcia zamierzonych celów.
- 25 W odniesieniu do korelacji między różnymi bazami danych rada ministrów przypomina, że art. 24 i 25 ustawy PNR dokonują transpozycji art. 6 dyrektywy PNR. Ponadto z prac przygotowawczych wynika, że ustawodawca nie ma na celu dokonania korelacji między bazą danych „pasażerów” a wszystkimi bazami danych, do których właściwe organy mają dostęp, lecz wyłącznie między bazą danych „pasażerów” a bazami danych, które odpowiadają celom realizowanym przez zaskarżoną ustawę. Środki te są zgodne z wnioskami płynącymi z opinii 1/15 Trybunału Sprawiedliwości, ponieważ art. 6 ust. 3 dyrektywy PNR nie wyjaśnia także, jakie bazy danych mogą być skorelowane. Swobodne uznanie nie jest również niezgodne z zasadą legalności zgodnie z wykładnią dokonaną przez Europejski Trybunał Praw Człowieka.

Ponadto cel ustawy nie mógłby zostać osiągnięty, gdyby podróżni znali z wyprzedzeniem kryteria, na podstawie których dojdzie do skojarzenia danych, ponieważ mogliby oni w związku z tym dostosować swoje zachowanie. Artykuł 16 zaskarżonej ustawy wskazuje ponadto wyraźnie, że pre-screeningu należy dokonywać w bazie danych „pasażerów”, co jest więc zgodne z zasadą legalności.
- 26 Co się tyczy okresu przechowywania danych, rada ministrów uważa, że określenie pięcioletniego okresu ich przechowywania, który odpowiada zresztą minimalnemu okresowi przedawnienia ścigania wykroczeń i mniej poważnych przestępstw, nie jest nieracjonalne.

Okres przechowywania tych danych, który jest zgodny z okresem przewidzianym w dyrektywie PNR, nie jest zatem w żaden sposób nieproporcjonalny.

- 27 Zarzut drugi, podniesiony posiłkowo, dotyczy zasadniczo naruszenia przepisów art. 3 ust. 2 TFUE w związku z art. 45 karty.
- 28 Skarżąca twierdzi, że art. 3 ust. 1, art. 8 ust. 2 i rozdział 11 zawierający art. 28–31 ustawy PNR są sprzeczne ze swobodnym przepływem osób w zakresie, w jakim odnoszą się one nie tylko do przewozów pozaunijnych, lecz również do przewozów wewnątrzunijnych (w tym do przesiadek). Strona skarżąca uważa, innymi słowy, że rozszerzając system „PNR” na loty wewnątrzunijne zaskarżone przepisy w sposób pośredni przywracają kontrole graniczne, które są sprzeczne ze swobodą przepływu osób.
- 29 Rada ministrów uważa, że zaskarżona ustawa nie przywraca żadnej kontroli granicznej i nie narusza w żaden sposób swobody przepływu osób. Dyrektywa PNR nie ma zastosowania do nielegalnej imigracji, a zaskarżona ustawa dokonuje transpozycji nie tylko dyrektywy PNR, ale także dyrektywy API.

Zarzut w brzmieniu, w jakim został sformułowany dotyczy wyłącznie art. 3 ust. 1 i art. 8 ust. 2, a także rozdziału 11 zaskarżonej ustawy. Tymczasem z definicji pojęcia „granic zewnętrznych” wynika, że ustawa PNR dotyczy wyłącznie kontroli pozaunijnych. Ponadto ustawa PNR dokonuje transpozycji dyrektywy 2004/82/WE, a więc nie można jej interpretować w ten sposób, że wprowadza ona kontrolę graniczną w strefie Schengen.

Dalszym tytułem posiłkowym, motyw 10 dyrektywy PNR przewiduje wyraźnie możliwość rozszerzenia wykorzystywania danych „PNR” na loty wewnątrzunijne, co świadczy o tym, że środek ten nie jest sam w sobie sprzeczny ze swobodą przepływu ani z rozporządzeniem (WE) nr 562/2006.

II. Ramy prawne

Europejska konwencja praw człowieka

- 30 Artykuł 8 stanowi:
- „1. Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji.
2. Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób”.

Prawo Unii*Karta praw podstawowych Unii Europejskiej*

- 31 Artykuł 7 karty („Poszanowanie życia prywatnego i rodzinnego”) stanowi:
- „Każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się”.
- 32 Artykuł 8 karty („Ochrona danych osobowych”) stanowi:
- „1. Każdy ma prawo do ochrony danych osobowych, które go dotyczą.
2. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania.
3. Przestrzeganie tych zasad podlega kontroli niezależnego organu”.
- 33 Artykuł 52 ust. 1 karty stanowi:
- „Wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w niniejszej Karcie muszą być przewidziane ustawą i szanować istotę tych praw i wolności. 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”.

Ogólne rozporządzenie o ochronie danych (RODO)

- 34 Artykuł 2 ust. 2 lit. d) stanowi:
- „2. Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych:
- [...]
- d) przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom”.
- 35 Artykuł 23 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;
- e) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu;
- f) ochronie niezależności sądów i postępowania sądowego;
- g) zapobieganiu naruszeniom zasad etyki w zawodach regulowanych, prowadzeniu postępowań w takich sprawach, ich wykrywaniu oraz ściganiu;
- h) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a)–e) oraz g);
- i) ochronie osoby, której dane dotyczą, lub praw i wolności innych osób;
- j) egzekucji roszczeń cywilnoprawnych.

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”.

Dyrektywa PNR

36 Artykuł 3 ma następujące brzmienie:

„Na potrzeby niniejszej dyrektywy stosuje się następujące definicje:

[...]

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;”.

37 Artykuł 4 stanowi:

„Jednostka do spraw informacji o pasażerach

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 (zwanej dalej »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.

[...]”.

38 Artykuł 6 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; oraz

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

[...]”.

39 Artykuł 12 stanowi:

„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 do 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 jakiegokolwiek 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”.

40 W załączniku I do dyrektywy PNR, zatytułowanym „Dane dotyczące przelotu pasażera zbierane przez przewoźników lotniczych” wymieniono w szczególności:

„[...]”

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)

[...]

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)

[...]”.

Dyrektywa API

41 Artykuł 1 stanowi:

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

Prawo belgijskie

42 Właściwe przepisy **ustawy PNR** (w brzmieniu zmienionym ustawami z dnia 15 i 30 lipca 2018 r. oraz ustawą z dnia 2 maja 2019 r.) są następujące:

„ROZDZIAŁ 2. Zakres stosowania

Art. 3. § 1. Niniejsza ustawa określa obowiązki przewoźników i operatorów turystycznych związane z przekazywaniem danych pasażerów udających się na terytorium kraju, przybywającym z niego lub przez nie przejeżdżającym.

§ 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 właściwego organu ds. kontroli przetwarzania danych osobowych. [...]

ROZDZIAŁ 3. Definicje

Art. 4. Do celów stosowania niniejszej ustawy i rozporządzeń wykonawczych do niej, przyjmuje się następujące definicje:

[...]

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;

[...]

ROZDZIAŁ 5. Cele przetwarzania danych

Art. 8. § 1. Dane pasażerów są przetwarzane w celu:

1) poszukiwania i ścigania, w tym wykonywania kar lub środków ograniczenia wolności dotyczących przestępstw, o których mowa [w] Code d’Instruction criminelle (kodeksie postępowania karnego);

2) poszukiwania i ścigania, w tym wykonywania kar lub środków ograniczenia wolności, dotyczących przestępstw, o których mowa [w] Code pénal (kodeksie karnym);

3) zapobiegania poważnym zakłóceniom bezpieczeństwa publicznego w ramach radykalizacji postaw prowadzącej do aktów przemocy poprzez monitorowanie zjawisk i ugrupowań zgodnie z art. 44/5 § 1 pkt 2) i 3) oraz § 2 loi du 5 août 1992 sur la fonction de police (ustawy z dnia 5 sierpnia 1992 r. o policji);

4) monitorowania działalności, o której mowa w art. 7 pkt 1) i 3) 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) poszukiwania i ścigania przestępstw, o których mowa w [różnych ustawach].

§ 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.

ROZDZIAŁ 6. – Dane pasażerów

Art. 9. § 1. Jeśli chodzi o dane dotyczące rezerwacji, dane pasażerów obejmują co najwyżej:

1) numer rezerwacji PNR;

2) datę rezerwacji/wystawienia biletu;

- 3) daty planowanej podróży;
- 4) nazwiska, imiona i datę urodzenia;
- 5) adres i dane kontaktowe (numer telefonu, adres e-mail);
- 6) wszystkie informacje o formie płatności, w tym adres na fakturze;
- 7) kompletną trasę podróży dla danego pasażera;
- 8) informacje dotyczące „podróżnych zarejestrowanych”, czyli stałych klientów;
- 9) biuro podróży;
- 10) dane o statusie podróży pasażera, w tym potwierdzenia, stan odprawy biletowo-bagażowej, dane typu: pasażer nie stawiał 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 oraz płeć małoletniego, jego 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, datę wystawienia biletu i bilety w jedną stronę, informację o automatycznie skalkulowanej taryfie;
- 14) numer miejsca na pokładzie i inne informacje o miejscu;
- 15) informacje o wspólnej obsłudze połączeń;
- 16) wszelkie informacje o bagażu;
- 17) liczbę oraz imiona i nazwiska innych podróżnych wymienionych w PNR;
- 18) wszelkie wstępne dane pasażera przekazane przed podróżą (dane API), które zostały zgromadzone, wymienione w § 2;
- 19) wszystkie dotychczasowe zmiany danych PNR wymienionych w pkt 1–18.

§ 2. W odniesieniu do danych dotyczących rejestracji i wejścia na pokład, danymi wstępnymi, o których mowa w § 1 pkt 18) są:

- 1) rodzaj dokumentu podróży;
- 2) numer dokumentu;

- 3) obywatelstwo;
- 4) kraj wydania dokumentu;
- 5) data ważności dokumentu;
- 6) nazwisko, imię, płeć, data urodzenia;
- 7) przewoźnik/operator turystyczny;
- 8) numer przewozu;
- 9) data wyjazdu, data przyjazdu;
- 10) miejsce wyjazdu, miejsce przyjazdu;
- 11) godzina wyjazdu, godzina przyjazdu;
- 12) całkowita liczba przewożonych pasażerów;
- 13) numer miejsca;
- 14) numer rezerwacji PNR;
- 15) liczba, ciężar i identyfikacja bagażu;
- 16) przejście graniczne wjazdu na terytorium kraju.

[...]

ROZDZIAŁ 7. Jednostka do spraw informacji o pasażerach

Art. 12. W ramach Service Public Fédéral Intérieur tworzy się Jednostkę do spraw informacji o pasażerach.

Art. 13. § 1. JIP odpowiada za:

- 1) gromadzenie, przechowywanie i przetwarzanie danych przewożonych pasażerów przez przewoźników lub operatorów turystycznych oraz zarządzanie bazą danych pasażerów;
- 2) wymianę zarówno danych pasażerów, jak i rezultatów ich przetwarzania z JIP innych państw członkowskich Unii Europejskiej, z Europolem, oraz z państwami trzecimi, zgodnie z rozdziałem 12.

§ 2. Bez uszczerbku dla innych przepisów ustawowych JIP nie może wykorzystywać danych przechowywanych na mocy rozdziału 9 dla celów innych niż cele określone w art. 8.

Art. 14. § 1. JIP składa się z:

1) Urzędnika [...] odpowiedzialnego za:

- a) organizację i funkcjonowanie JIP;
- b) kontrolę przestrzegania przez przewoźników i operatorów turystycznych obowiązków określonych w rozdziale 4;
- c) zarządzanie i wykorzystanie bazy danych pasażerów;
- d) przetwarzanie danych pasażerów;
- e) poszanowanie zgodności z prawem i prawidłowości przetwarzania danych, o których mowa w rozdziale 10;

[...].

2) delegowanych członków pochodzących z następujących [...] służb:

- a) służby policji [...];
- b) służby bezpieczeństwa państwa [...];
- c) ogólne służby wywiadowcze i bezpieczeństwa [...];
- d) organy celne [...]

[...].

ROZDZIAŁ 8. Baza danych pasażerów

Art. 15. § 1. Niniejszym ustanawia się bazę danych pasażerów zarządzaną przez Service Public Fédéral Intérieur, w której rejestrowane są dane pasażerów.

[...].

§ 4. Przetwarzanie danych pasażerów na mocy niniejszej ustawy podlega przepisom ustawy o ochronie danych. Właściwy organ kontroli przetwarzania danych osobowych wykonuje uprawnienia przewidziane w ustawie o ochronie życia prywatnego. [...]

[...]

ROZDZIAŁ 9. Okres przechowywania

Art. 18. Dane pasażerów są przechowywane w bazie danych pasażerów przez okres co najwyżej pięciu lat od chwili ich zarejestrowania. Po upływie tego okresu dane te są usuwane.

[...]

ROZDZIAŁ 10. Przetwarzanie danych

Sekcja I. Przetwarzanie danych pasażerów w ramach wstępnej oceny pasażerów

Art. 24. § 1. Dane pasażerów są przetwarzane w celu dokonania wstępnej oceny pasażerów przed ich przyjazdem, ich odjazdem lub ich planowanym przejazdem przez terytorium kraju w celu ustalenia, które osoby powinny podlegać bardziej szczegółowemu badaniu.

[metody wstępnej oceny]

Art. 25. [...]

§ 2. Ocena pasażerów przed ich przyjazdem, przejazdem lub wyjazdem w świetle określonych wcześniej kryteriów jest przeprowadzona w sposób niedyskryminujący. Kryteria te nie mogą odnosić się do tożsamości jednostki i muszą być ukierunkowane, proporcjonalne i szczególne.

§ 3. Kryteria te nie mogą być oparte na danych ujawniających pochodzenie rasowe lub etniczne osoby, jej przekonania religijne lub filozoficzne, opinie polityczne, przynależność do związków zawodowych, stan zdrowia, życie seksualne lub orientację seksualną.

[...]

Sekcja 2. - Przetwarzanie danych w ramach wyszukiwań ad hoc

Art. 27. Dane pasażerów są wykorzystywane z zamiarem przeprowadzenia wyszukiwań ad hoc dla celów, o których mowa w art. 8 § 1 pkt 1), 2), 4) i 5) oraz na warunkach przewidzianych w art. 46f kodeksu postępowania karnego lub w art. 16/3 ustawy z dnia 30 listopada 1998 r. organicznej o służbach wywiadowczych i bezpieczeństwa) lub w art. 281 § 4 loi générale sur les douanes et accises (ogólnej ustawy o cłach i akcyzie), ujednoliconej w dniu 18 lipca 1977 r.

ROZDZIAŁ 11. Przetwarzanie danych pasażerów z zamiarem ulepszenia kontroli na granicach zewnętrznych i zwalczania nielegalnej imigracji

Art. 28. § 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.

[...]

Art. 29. § 1. [...]

§ 2. Przekazywane są wyłącznie dane [API] 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, o których mowa w art. 14 § 1 pkt 2) lit. a), natychmiast po wpisaniu ich do bazy 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 urzędu ds. cudzoziemców niezwłocznie po ich zarejestrowaniu w bazie danych pasażerów. Urząd ten przechowuje dane w tymczasowym pliku i usuwa je w ciągu 24 godzin po przekazaniu.

[...].

Art. 31. W ciągu 24 godzin po zakończeniu przewozu, o którym mowa w art. 4 pkt 3)–6), przewoźnicy i operatorzy turystyczni usuwają wszelkie dane pasażerów, o których mowa w art. 9 § 1 pkt 18) [...].

[...]

ROZDZIAŁ 15. Przepisy zmieniające

Sekcja I. Zmiana kodeksu postępowania karnego

Art. 50. W kodeksie postępowania karnego dodaje się art. 46f, który ma następujące brzmienie:

“Art. 46f. Ścigając zbrodnie i przestępstwa, o których mowa w art. 8 § 1 pkt 1, 2 i 5 ustawy z dnia 25 grudnia 2016 r. o przetwarzaniu danych pasażerów, prokurator królewski może, w drodze pisemnego i umotywowanego postanowienia, powierzyć funkcjonariuszowi policji sądowej zwrócenie się do JIP o udzielenie informacji o danych pasażerów zgodnie z art. 27 ustawy z dnia 25 grudnia 2016 r. o przetwarzaniu danych pasażerów).

[...]

Sekcja 2. Zmiana ustawy organicznej z dnia 30 listopada 1998 r. o służbach wywiadowczych i bezpieczeństwa

Art. 51. W rozdziale III sekcji I podsekcja 2 ustawy organicznej z dnia 30 listopada 1998 r. o służbach wywiadowczych i bezpieczeństwa dodaje się art. 16/3, który ma następujące brzmienie:

„Art. 16/3. § 1. Służby wywiadowcze i bezpieczeństwa mogą, w celu wykonywania swoich zadań, podjąć należycie uzasadnioną decyzję o uzyskaniu dostępu do danych pasażerów, o których mowa w art. 27 ustawy z dnia 25 grudnia 2016 r. o przetwarzaniu danych pasażerów [...]”.

III. Ocena Cour constitutionnelle

- 43 Cour constitutionnelle precyzuje przede wszystkim, że skarga zostanie rozpoznana z uwzględnieniem zmian w ustawie z dnia 25 grudnia 2016 r., które zostały wprowadzone ustawami z dnia 15 i 30 lipca 2018 r. oraz ustawą z dnia 2 maja 2019 r.
- 44 Cour constitutionnelle ogranicza ponadto zakres skargi o stwierdzenie nieważności poprzez określenie, że zarzut pierwszy jest skierowany wyłącznie przeciwko art. 3 ust. 2, art. 4 pkt 9 i 10, art. 7–9, art. 12–16, art. 18, art. 24–27, art. 50 i 51 ustawy oraz że zarzut drugi jest skierowany przeciwko art. 3 ust. 1, art. 8 ust. 2 oraz art. 28–31 ustawy.

1. W przedmiocie dopuszczalności zarzutu pierwszego: czy art. 23 RODO znajduje zastosowanie do ustawy PNR?

- 45 Sąd odsyłający przypomina, że ochrona, jaką oferuje RODO, jest oparta na art. 16 ust. 2 TFUE zaś, co do zasady, przetwarzanie danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar nie jest objęte RODO, lecz dyrektywą 2016/680. W dyrektywie tej ustanowiono szczególne zasady odnoszące się do ochrony osób fizycznych w odniesieniu do przetwarzania 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 poszanowaniem szczególnego charakteru tych czynności.
- 46 Ustawa PNR reguluje gromadzenie i przekazywanie danych PNR, tworzenie bazy danych pasażerów zarządzanej przez JIP, cele przetwarzania tej bazy danych oraz dostęp do niej. Dokonuje ona zasadniczo transpozycji dyrektywy PNR, lecz jej treść wykracza poza transpozycję tej dyrektywy.
- 47 Powołując się na opinię 1/15 (umowa PNR UE-Kanada) z dnia 26 lipca 2017 r. (EU:C:2017:592), sąd odsyłający stwierdza, że przepisy regulujące gromadzenie, przekazywanie i przetwarzanie danych „PNR” mogą być objęte ochroną danych (art. 16 TFUE) jak i współpracą policyjną (art. 87 TFUE).

Podnosi on również, że w motywie 5 dyrektywy PNR wskazano, iż cele tej dyrektywy obejmują „między innymi, zapewnienie bezpieczeństwa ogólnego, ochronę życia i bezpieczeństwa osób oraz stworzenie ram prawnych służących ochronie danych PNR w związku z ich przetwarzaniem przez właściwe organy”.

Motyw 38 tej dyrektywy wskazuje jednak, że celami dyrektywy są „przekazywanie danych PNR przez przewoźników lotniczych i przetwarzanie tych danych w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania”, co mogłoby nadać tym celom charakter przeważający nad celem ochrony danych.

Sąd ten stwierdza ponadto, że prawo krajowe nie wyklucza całości ustawy PNR z zakresu zastosowania art. 23 RODO.

- 48 Cour constitutionnelle doszedł zatem do wniosku, że w celu ustalenia, czy wymogi art. 23 RODO mają zastosowanie do ustawy PNR, która dokonuje transpozycji, między innymi i zasadniczo, dyrektywy PNR, należy zwrócić się do Trybunału z pierwszym pytaniem prejudycjalnym.

2. Co do istoty zarzutu pierwszego

Cour constitutionnelle bada następnie istotę zarzutu w siedmiu aspektach, o których mowa w pkt 8 niniejszego streszczenia. Sąd odsyłający uważa, że dwa pierwsze podniesione zastrzeżenia dotyczące „sposobu wykonania” i pojęć „dokumentów tożsamości” i „dokumentu podróży” są pozbawione podstaw. Kontynuuje on analizę pięciu pozostałych zastrzeżeń i wyraża wątpliwości co do interpretacji pewnych przepisów dyrektywy PNR oraz ich ważności z punktu widzenia karty.

W przedmiocie danych, o których mowa (art. 4 pkt 9 i art. 9 ustawy PNR)

- 49 Strona skarżąca uważa, że bardzo szeroki zakres stosowania dotyczący danych pasażerów, o których mowa w art. 4 pkt 9 i art. 9 ustawy PNR, jest w oczywisty sposób nieproporcjonalny z punktu widzenia realizowanego celu. Jej zdaniem odnośne dane mogłyby prowadzić do ujawnienia szczególnie chronionych danych, takich jak przynależność do związków zawodowych, przekonania osobiste oraz relacje osobiste lub zawodowe.
- 50 Sąd odsyłający przypomina, że ingerencja władz publicznych w korzystanie z prawa do poszanowania życia prywatnego musi nie tylko opierać się na wystarczająco precyzyjnym przepisie ustawowym, ale musi także odpowiadać nadrzędnej potrzebie społecznej w społeczeństwie demokratycznym i być proporcjonalna do zamierzonego zgodnego z prawem celu. Ustawodawca posiada w tej dziedzinie zakres uznania, który nie jest jednak nieograniczony: aby przepis był zgodny z prawem do poszanowania życia prywatnego, ustawodawca musi ustanowić słuszną równowagę między wszystkimi wchodzącymi w grę prawami i interesami.

W opinii 1/15 (umowa PNR UE-Kanada) z dnia 26 lipca 2017 r. (EU:C:2017:592) Trybunał przypominał, że ingerencja w prawo do ochrony danych osobowych

powinna być ograniczona do tego, co „rzeczywiście konieczne” (zob. pkt 140 i 141).

- 51 Cour constitutionnelle zwraca uwagę, że ustawa PNR ma na celu zapewnienie bezpieczeństwa publicznego, wprowadzając przekazywanie danych pasażerów i ich wykorzystanie w ramach zwalczania przestępstw terrorystycznych i poważnych przestępstw międzynarodowych. Takie cele stanowią cele interesu ogólnego, które mogą uzasadniać ingerencje w prawo do poszanowania życia prywatnego oraz w prawo do ochrony danych osobowych (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). Trybunał Sprawiedliwości potwierdził zresztą, że takie cele interesu ogólnego mogą uzasadniać przekazywanie i przetwarzanie danych dotyczących przelotu pasażera [opinia 1/15 (umowa PNR UE-Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 148 i 149].

- 52 Sąd odsyłający bada następnie, czy te ingerencje są wystarczająco precyzyjne, proporcjonalne i ograniczone do tego, co „ściśle niezbędne”, z uwzględnieniem zakresu danych, o których mowa w ustawie PNR.

Gromadzenie danych pasażerów, o których mowa w ustawie PNR, jest obwarowane gwarancjami dotyczącymi treści tych danych. Dane te są bowiem określone w sposób wyczerpujący w art. 9 ustawy PNR. Chodzi o informacje bezpośrednio związane z podróżą, w ramach której następuje przewóz wchodzący w zakres stosowania ustawy PNR, co do zasady znane już przewoźnikom i operatorom turystycznym. Ponadto dane te odpowiadają załącznikowi I do wytycznych Organizacji Międzynarodowego Lotnictwa Cywilnego (ICAO). Mają one zatem znaczenie z punktu widzenia celów, do których dąży ustawa PNR.

Ponadto art. 10 i 11 ustawy PNR, które nie zostały zaskarżone, stanowią, że dane pasażerów nie mogą dotyczyć pochodzenia rasowego lub etnicznego osoby, jej przekonań religijnych lub filozoficznych, jej poglądów politycznych, jej przynależności do organizacji związkowej oraz informacji odnoszących się do jej stanu zdrowia, jej życia seksualnego lub jej orientacji seksualnej. Jeżeli dane pasażerów przewożonych przez przewoźników i biura podróży zawierają dane inne niż wymienione w art. 9 lub dane wymienione w art. 10, JIP usuwa te dodatkowe dane w sposób ostateczny z chwilą ich otrzymania. Przepisy te gwarantują, że dane szczególnie chronione nie mogą być co do zasady gromadzone ani przechowywane jako „dane pasażerów”.

- 53 W ww. opinii 1/15 z dnia 26 lipca 2017 r. Trybunał Sprawiedliwości uznał również w odniesieniu do danych szczególnie chronionych, że „art. 7, 8 i 21, a także art. 52 ust. 1 karty stoją na przeszkodzie zarówno przekazywaniu danych szczególnie chronionych do Kanady, jak i wynegocjowanemu przez Unię z tym państwem trzecim uregulowaniu warunków wykorzystywania i zatrzymywania takich danych przez organy tego państwa trzeciego” (pkt 167).

Uwaga ta ma zastosowanie w niniejszej sprawie. Mimo istnienia gwarancji dotyczących danych pasażerów, o których mowa w ustawie PNR, należy jednak zastanowić się, czy gwarancje te są wystarczające, biorąc pod uwagę obszerność odnośnych danych. Dane, o których mowa w art. 9 ust. 1 ustawy PNR, który przytacza dane wymienione w załączniku I do dyrektywy PNR, obejmują bowiem bardzo obszerne dane – oprócz danych dotyczących rejestracji i wejścia na pokład – w szczególności: pełną trasę podróży pasażera, biuro podróży, numer miejsca, wszystkie informacje dotyczące bagażu, informacje dotyczące sposobów płatności, w tym adres na fakturze, uwagi ogólne, „w tym wszystkie dostępne informacje o małoletnich bez opieki poniżej 18 lat”.

W ww. opinii 1/15 z dnia 26 lipca 2017 r. Trybunał zauważył ponadto, że *„nawet jeżeli niektóre dane PNR, 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, takich jak informacje, o których mowa w art. 2 lit. e) przewidywanej umowy”* (pkt 128).

W opinii z dnia 19 sierpnia 2016 r. dotyczącej konsekwencji w zakresie ochrony danych wynikających z przetwarzania danych pasażerów (zwanej dalej „opinią z dnia 19 sierpnia 2016 r.”) Komitet Doradczy konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (zwany dalej „komitetem doradczym konwencji nr 108”) zauważył również, że *„PNR zawierają informacje mające na celu ułatwienie podróży pasażerów i mogą obejmować szereg wrażliwych danych (dane mogące służyć do wskazywania pochodzenia rasowego, przekonań politycznych, przekonań religijnych i innych, stanu zdrowia lub orientacji seksualnej danej osoby) nie tylko w formie pewnych danych „kodowanych”, lecz również w sposób otwarty, w miejscu na ogólne uwagi (takie jak wymagania dietetyczne i medyczne, lub fakt, że organizacja polityczna lub religijna skorzystała z biletów po obniżonej cenie na podróż swoich członków), co mogłoby prowadzić do bezpośredniej dyskryminacji”* (Rada Europy, opinia z dnia 19 sierpnia 2016 r., T-PD (2016) 18rev, s. 7).

Agencja Praw Podstawowych Unii Europejskiej zauważyła również, że dane PNR *„mogą obejmować dane wrażliwe lub szczególne w rubryce »uwagi ogólne«”* (opinia 1/2011 Agencji Praw Podstawowych Unii Europejskiej w sprawie wniosku dyrektywy w sprawie wykorzystania danych dotyczących przelotu pasażera (PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (KOM (2011) 32 wersja ostateczna), 14 czerwca 2011 r., s. 8; zob. również ibid, s. 13).

- 54 Biorąc pod uwagę bardzo szeroki zakres stosowania danych, o których mowa w art. 9 ustawy PNR, mimo że nie mogą one zawierać bezpośrednio szczególnie

chronionych danych, mogą jednak pośrednio ujawniać szczególnie chronione elementy objęte ochroną danych osobowych oraz zasadą poszanowania życia prywatnego. Biorąc pod uwagę opinię 1/15 Trybunału Sprawiedliwości, Cour constitutionnelle zastanawia się, czy takie dane, które obejmują dane wymienione w załączniku I do dyrektywy PNR, nie wykraczają poza to, co „ściśle niezbędne” do osiągnięcia celów realizowanych przez tę dyrektywę. W związku z tym postanawia on zwrócić się do Trybunału z drugim pytaniem prejudycjalnym.

- 55 W ww. opinii 1/15 z dnia 26 lipca 2017 r. Trybunał przedstawił ponadto następujące uwagi w odniesieniu do wymogu jasnej i dokładnej definicji danych objętych projektem umowy między Kanadą a Unią Europejską o przekazywaniu i przetwarzaniu danych dotyczących przelotu pasażera:

„156. W tej kwestii należy zauważyć, że o ile 19 rubryk danych PNR figurujących w załączniku do przewidywanej umowy odpowiada, zgodnie z uwagami Komisji, załącznikowi I do wytycznych Organizacji Międzynarodowego Lotnictwa Cywilnego (ICAO) dotyczących danych PNR, o tyle należy jednak podkreślić – jak wskazał rzecznik generalny w pkt 217 opinii – że rubryka 5, która obejmuje »dostępne informacje dotyczące programów dla stałych klientów (frequent flier) i dotyczące korzyści (darmowe bilety, zamiana klasy biletu na wyższą itd.)« oraz rubryka 7, obejmująca »wszelkie dostępne informacje kontaktowe (w tym informacje na temat jednostki, która utworzyła dane)«, nie określają w sposób wystarczająco jasny i precyzyjny danych PNR podlegających przekazaniu.

157. Użyty bowiem w rubryce 5 skrót »itd.« nie wyznacza w sposób wystarczający zakresu danych podlegających przekazaniu. Ponadto sformułowanie tej rubryki nie pozwala na ustalenie, czy rzeczona rubryka obejmuje informacje dotyczące wyłącznie statusu pasażerów w programach związanych z korzyściami, czy też przeciwnie, obejmuje ona ogół informacji dotyczących pasażerów lotniczych i transakcji dokonywanych w ramach takich programów.

158. Podobnie rubryka 7, w której użyto sformułowania »wszelkie dostępne informacje kontaktowe«, nie wyznacza w sposób wystarczający zakresu danych podlegających przekazaniu. W szczególności nie precyzuje ona rodzaju objętych nią informacji kontaktowych ani też czy te informacje kontaktowe obejmują również – co można wywnioskować z pisemnej odpowiedzi Komisji na pytania Trybunału – informacje o osobach trzecich, które dokonały rezerwacji lotu dla pasażera, o osobach trzecich, za których pośrednictwem można się z nim skontaktować, lub wreszcie o osobach trzecich, które powinny zostać powiadomione w nagłym wypadku.

159. Jeżeli chodzi o rubrykę 8, to obejmuje ona »wszelkie dostępne informacje o płatnościach/fakturowaniu (z wyjątkiem innych szczegółów transakcji dotyczących karty kredytowej lub konta i niepowiązanych z transakcją dotyczącą podróży)«. Z pewnością rubryka ta może wydawać się szczególnie szeroka, jako że zawiera

wyrażenie »wszelkie dostępne informacje«. Jednak, jak wynika z odpowiedzi Komisji na pytania Trybunału, należy przyjąć, że rzeczona rubryka obejmuje wyłącznie informacje dotyczące sposobu płatności za bilet lotniczy i wystawiania faktury za niego, z wyłączeniem wszelkich innych informacji niepozostających w bezpośrednim związku z lotem. Można zatem uznać, że interpretowana w ten sposób rubryka 8 spełnia wymogi jasności i precyzji.

160. Rubryka 17 obejmuje »uwagi ogólne, w tym inne informacje dodatkowe (OSI), informacje o usługach specjalnych (SSI) i o prośbach o usługi specjalne (SSR)«. Zgodnie z wyjaśnieniami przedstawionymi w szczególności przez Komisję jest to rubryka zwana »tekstem dowolnym« (free text) i służy przedstawieniu »wszystkich informacji dodatkowych« w stosunku do informacji wymienionych w innych miejscach załącznika do przewidywanej umowy. Tak więc rubryka ta nie zawiera żadnej wskazówki co do charakteru i zakresu informacji, które powinny zostać przekazane, i wydaje się nawet, że może ona obejmować informacje nie pozostające w żadnym związku z celem przekazywania danych PNR. Ponadto, skoro informacje wskazane w tej rubryce określone są jedynie przykładowo, o czym świadczy użycie sformułowania »w tym«, rubryka ta nie określa żadnej granicy co do charakteru i zakresu informacji, jakie mogą się w niej zawierać. W tym stanie rzeczy nie można uznać, że rubryka jest określona w sposób wystarczająco jasny i precyzyjny.

161. Co się tyczy na koniec rubryki 18, to obejmuje ona »wszelkie zaawansowane informacje o pasażerach (Advance Passenger Information (API)) zgromadzone do celów rezerwacji«. Zgodnie z wyjaśnieniami udzielonymi przez Radę i Komisję informacje te odpowiadają informacjom, o których mowa w art. 3 ust. 2 dyrektywy 2004/82, a którymi są: 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, a także punkt początkowy załadunku. Rubrykę tę, w zakresie, w jakim będzie interpretowana w ten sposób, że obejmuje wyłącznie informacje wyraźnie wymienione w tym ostatnim przepisie, można uznać za spełniającą wymogi jasności i precyzji.

162. Postanowienia art. 4 ust. 3 przewidywanej umowy, które przewidują po stronie Kanady obowiązek usuwania każdej przekazanej jej danej, jeżeli nie jest ona wymieniona w załączniku do tej umowy, nie pozwalają na zarządzenie brakowi precyzji, którym dotknięte są rubryki 5, 7 i 17 tego załącznika. W zakresie bowiem, w jakim ten wykaz sam w sobie nie określa w sposób wystarczająco jasny i precyzyjny danych PNR podlegających przekazaniu, postanowienia te nie są w stanie zaradzić niepewności co do danych PNR, które powinny zostać przekazane.

163. W takich okolicznościach należy w odniesieniu do danych PNR podlegających przekazaniu do Kanady stwierdzić, że rubryki 5, 7 i 17 załącznika do przewidywanej umowy nie określają w sposób wystarczająco jasny i precyzyjny zakresu ingerencji w prawa podstawowe ustanowione w art. 7 i 8 karty”.

- 56 Ponieważ niektóre z tych uwag można przenieść na grunt niniejszej sprawy, biorąc pod uwagę przykładowy i niewyczerpujący charakter niektórych danych zawartych w załączniku I do dyrektywy PNR, którego transpozycji dokonano w art. 9 ustawy PNR, sąd odsyłający postanawia zadać trzecie pytanie prejudycjalne.

W przedmiocie pojęcia „pasażera” (art. 4 pkt 10 ustawy PNR)

- 57 Strona skarżąca kwestionuje szeroki zakres pojęcia „pasażera”, który prowadzi do systematycznego, automatycznego, nieukierunkowanego przetwarzania danych wszystkich pasażerów.
- 58 Definicja pojęcia „pasażera” (art. 4 pkt 10 ustawy PNR) oznacza w konsekwencji że gromadzenie, przekazywanie i przetwarzanie danych PNR „pasażerów” stanowią ogólny i niezróżnicowany obowiązek mający zastosowanie do wszystkich osób, które są lub mają być przewożone, wpisanych na listę pasażerów. Obowiązki, które nakłada ustawa PNR, mają zatem zastosowanie niezależnie od istnienia poważnych podstaw, by sądzić, że dane osoby popełniły przestępstwo lub zamierzają popełnić przestępstwo, lub zostały skazane za przestępstwo.
- 59 W opinii z dnia 19 sierpnia 2016 r. Komitet Doradczy konwencji nr 108 zauważył w tym względzie, że *„[p]rzetwarzanie danych PNR – których jedyną zaletą jest umożliwienie identyfikacji osób będących przedmiotem zainteresowania – jest ogólnym i nieselektywnym filtrowaniem wszystkich pasażerów, w tym pasażerów, którzy nie są podejrzewani o popełnienie jakiegokolwiek przestępstwa, przez różne właściwe organy, i dotyczy danych pierwotnie gromadzonych do celów handlowych przez podmioty prywatne. Mając na względzie zakres naruszenia prawa do prywatności i ochrony danych wynikającego z przetwarzania danych PNR, należy jasno stwierdzić, że wspomniane przetwarzanie jest niezbędnym środkiem w społeczeństwie demokratycznym w zgodnym z prawem celu; należy ponadto ustanowić odpowiednie gwarancje. Konieczne jest wyraźne wykazanie niezbędności gromadzenia i dalszego wykorzystywania danych PNR”* (opinia z dnia 19 sierpnia 2016 r., T-PD (2016) 18rev, s. 5).
- 60 W dziedzinie łączności elektronicznej Trybunał wypowiedział się w sprawie uregulowania krajowego, które przewidywało uogólnione i niezróżnicowane przechowywanie wszystkich danych o ruchu i danych dotyczących lokalizacji wszystkich abonentów i zarejestrowanych użytkowników, dotyczących wszystkich środków łączności elektronicznej, a także spoczywający na dostawcach usług łączności elektronicznej obowiązek przechowywania tych danych w sposób systematyczny i ciągły, i to bez żadnych wyjątków (wyrok z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in., C-203/15 i C-698/15, EU:C:2016:970).

Uznał on, że *„o ile skuteczność walki z poważną przestępczością, a zwłaszcza z przestępczością zorganizowaną i terroryzmem, może w znacznym stopniu zależeć od wykorzystania nowoczesnych technik dochodzeniowo-śledczych, tego rodzaju*

cel interesu ogólnego, niezależnie od jego fundamentalnego znaczenia, nie może sam w sobie uzasadniać stwierdzenia, że przepisy krajowe przewidujące uogólnione i niezróżnicowane zatrzymywanie wszystkich danych o ruchu oraz danych dotyczących lokalizacji należy uznać za konieczne do celów prowadzenia tej walki” (pkt 103).

Trybunał orzekł, po pierwsze, że takie uregulowanie prowadzi do tego, iż przechowywanie danych o ruchu i danych dotyczących lokalizacji staje się regułą, podczas gdy system ustanowiony przez dyrektywę 2002/58 ustanawia wymóg, by takie przechowywanie danych było wyjątkiem, a po drugie, że „uregulowanie krajowe [...], które obejmuje w sposób uogólniony wszystkich abonentów i zarejestrowanych użytkowników i dotyczy wszystkich środków łączności elektronicznej i wszystkich danych o ruchu, nie przewiduje jakiegokolwiek zróżnicowania, ograniczenia ani wyjątku zależnego od zamierzonego celu. Obejmuje ono całościowo wszystkie korzystające z usług łączności elektronicznej osoby, nawet wtedy, gdy nie ma wobec nich żadnych podstaw, nawet pośrednich, do wszczęcia postępowania karnego. Ma ono zastosowanie nawet wobec tych osób, co do których brak jest dowodów mogących sugerować, że ich zachowanie może mieć związek, chociażby pośredni i daleki, z poważnymi przestępstwami. Ponadto dyrektywa nie przewiduje żadnych wyjątków, a więc w rezultacie ma zastosowanie nawet wobec tych osób, których łączność na gruncie przepisów prawa krajowego objęta jest tajemnicą zawodową (zob. analogicznie, w odniesieniu do dyrektywy 2006/24, wyrok Digital Rights, pkt 57, 58).

106. Takie uregulowanie nie wymaga istnienia żadnego związku między danymi, których zatrzymywanie nakazuje, a zagrożeniem dla bezpieczeństwa publicznego. Nie zawiera ono zwłaszcza żadnych ograniczeń czasowych czy geograficznych ani ograniczeń do grupy osób, które można podejrzewać o taki czy inny rodzaj uczestnictwa w poważnym przestępstwie, tak by obowiązek zatrzymywania danych obejmował tylko te dane, co do których z jakiegoś powodu można zakładać, że mają znaczenie dla walki z przestępczością (zob. analogicznie, w odniesieniu do dyrektywy 2006/24, wyrok Digital Rights, pkt 59).

107. Uregulowanie krajowe takie jak uregulowanie będące przedmiotem sporu zawisłego przed sądem krajowym wykracza więc poza granice tego, co jest absolutnie konieczne, i nie można go uznać za uzasadnione w demokratycznym społeczeństwie, jak tego wymaga art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty.

108. Natomiast nie jest sprzeczne z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty przyjęcie przez państwa członkowskie przepisów krajowych dopuszczających w ramach prewencji indywidualne zatrzymywanie danych dotyczących ruchu i danych o lokalizacji w celu zwalczania poważnej przestępczości, pod warunkiem że takie zatrzymywanie danych – w zakresie dotyczącym kategorii danych podlegających zatrzymywaniu, stosowanych środków łączności, zaangażowanych w ten proces podmiotów oraz

przyjętego okresu przechowywania danych – nie będzie wykraczać poza to, co jest absolutnie konieczne.

109. *Aby spełniać wymogi określone w poprzednim punkcie niniejszego wyroku, rozpatrywane uregulowanie krajowe musi, w pierwszej kolejności, zawierać jasne i dokładne reguły dotyczące zakresu i sposobu stosowania rozpatrywanego środka związanego z zatrzymywaniem danych, a także ustanawiać minimalne zabezpieczenia służące temu, aby osoby, których dane zostały zatrzymane, miały wystarczające gwarancje rzeczywistej ochrony ich danych osobowych przed ryzykiem nadużyć. Uregulowanie to winno w szczególności wskazywać okoliczności i warunki, w których środek związany z zatrzymywaniem danych może zostać zastosowany tytułem prewencji, co pozwoli zagwarantować, by środek ów ograniczał się do tego, co jest absolutnie konieczne (zob. analogicznie, w odniesieniu do dyrektywy 2006/24, wyrok Digital Rights, pkt 54 i przytoczone tam orzecznictwo).*

110. *W drugiej kolejności, jeżeli chodzi o materialne przesłanki, jakie musi spełnić uregulowanie krajowe umożliwiające w ramach zwalczania przestępczości prewencyjne zatrzymywanie danych o ruchu i danych o lokalizacji, aby zagwarantować, że będzie ono ograniczone do tego, co jest absolutnie konieczne, należy zauważyć, że chociaż przesłanki te mogą się różnić w zależności od środków podjętych w celu zapobiegania, dochodzenia, wykrywania i ścigania poważnych przestępstw, to jednak zatrzymywanie danych musi zawsze spełniać obiektywne kryteria określające związek między danymi, które mają być zatrzymywane, a realizowanym celem. W szczególności przesłanki te muszą w praktyce umożliwiać określenie rzeczywistego zakresu środka, a w konsekwencji – grona objętych nim osób.*

111. *Jeśli chodzi o ograniczenie środka do kategorii ewentualnie objętych nim osób i sytuacji, przepisy krajowe winny opierać się na obiektywnych elementach umożliwiających namierzenie osób, których dane mogą mieć związek, nawet pośredni, z poważną przestępczością, przyczyniać się w taki lub inny sposób do walki z ową przestępczością lub też zapobiegać powstawaniu poważnych zagrożeń dla bezpieczeństwa publicznego. Tego rodzaju określenie może być dokonane w oparciu o kryterium geograficzne, gdy właściwe władze krajowe na podstawie obiektywnych elementów uważają, że w jednym lub kilku obszarach geograficznych istnieje wysokie ryzyko przygotowania lub popełnienia takich czynów.*

112. *Mając na względzie całość powyższych rozważań, należy na pierwsze pytanie w sprawie C-203/15 odpowiedzieć, że art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8, 11 i art. 52 ust. 1 karty należy interpretować w ten sposób, iż stoi on na przeszkodzie uregulowaniu krajowemu przewidującemu do celów zwalczania przestępczości uogólnione i nieodróżnicowane zatrzymywanie wszystkich danych o ruchu oraz danych dotyczących lokalizacji wszystkich abonentów i zarejestrowanych użytkowników wszystkich środków łączności elektronicznej”.*

Na drugie pytanie prejudycjalne w sprawie C-203/15 i pierwsze pytanie prejudycjalne w sprawie C-698/15 Trybunał odpowiada, że art. 15 ust. 1 dyrektywy 2002/58/WE w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty należy interpretować *„w ten sposób, iż stoi on na przeszkodzie obowiązywaniu uregulowań krajowych dotyczących ochrony i bezpieczeństwa danych o ruchu i danych o lokalizacji, a w szczególności dostępu właściwych organów władz krajowych do przechowywanych danych, które to przepisy, w ramach zwalczania przestępczości nie ograniczają tego dostępu jedynie do celów walki z poważną przestępczością, nie uzależniają przyznania tego dostępu od uprzedniej kontroli sądowej lub niezależnego organu administracyjnego i nie ustanawiają wymogu, aby dane te były przechowywane na obszarze Unii”* (pkt 125).

- 61 W ocenie ETPC, który orzekał w tym przedmiocie w międzyczasie, dokonywane przez Szwecję masowe przechwytywanie wiadomości elektronicznych jest zgodne z art. 8 Europejskiej konwencji praw człowieka (wyrok z dnia 19 czerwca 2018 r., Centrum för Rättvisa/Szwecja). Wskazał on w szczególności, co następuje:

„Trybunał wyraźnie uznał, że organy krajowe dysponują szerokim zakresem uznania przy wyborze środków ochrony bezpieczeństwa narodowego [...]. W sprawach Weber i Saravia i Liberty i in. Trybunał uznał, że systemy masowego przechwytywania nie podlegają pod zakres uznania. Z uwagi na rozumowanie przyjęte przez Trybunał w tych wyrokach oraz z uwagi na obecne zagrożenia dla wielu umawiających się państw (zwłaszcza globalnego terroryzmu i innych poważnych przestępstw, takich jak handel narkotykami, handel ludźmi, wykorzystywanie seksualne dzieci i cyberprzestępczość), zmiany technologiczne, które pozwoliły terrorystom i przestępcom łatwiej uniknąć wykrycia w internecie, i nieprzewidywalność kanałów przekazywania wiadomości elektronicznych, Trybunał uważa, że decyzja o wykorzystaniu systemu masowego przechwytywania w celu identyfikacji zagrożeń dla bezpieczeństwa narodowego dotychczas nieznaną jest decyzją, która pozostaje w zakresie uznania państw” (wyrok ETPC z dnia 19 czerwca 2018 r., Centrum för Rättvisa/Szwecja, par. 112).

Trybunał ten orzekł natomiast, że angielska ustawa o przechwytywaniu komunikatów naruszała art. 8 EKPC, ponieważ nie spełniała ona kryteriów określonych w jego orzecznictwie. Stwierdził on również, że *„funkcjonowanie systemów masowego przechwytywania należy co do zasady do zakresu swobodnego uznania państwa. Masowe przechwytywanie jest z definicji nieukierunkowane, a uzależnienie go od istnienia »racjonalnego podejrzenia« uniemożliwiłoby jego wdrożenie”* (wyrok ETPC z dnia 13 września 2018 r., Big Brother Watch i in./Zjednoczone Królestwo, par. 317).

- 62 Powstaje pytanie, w jakim zakresie ww. orzecznictwo dotyczące uogólnionego i niezróżnicowanego przechowywania danych w dziedzinie łączności elektronicznej ma zastosowanie do uogólnionego i niezróżnicowanego gromadzenia, przekazywania i przetwarzania danych pasażerów tak, jak zostało to uregulowane w ustawie z dnia 25 grudnia 2016 r.

- 63 W ww. opinii 1/15 z dnia 26 lipca 2017 r. Trybunał wypowiedział się w przedmiocie analogicznego systemu PNR, lecz o bardziej ograniczonym zakresie stosowania, ponieważ projekt umowy między Kanadą a Unią Europejską o przekazywaniu i przetwarzaniu danych dotyczących przelotu pasażerów przewidywał „systematyczne i ciągle przekazywanie danych PNR ogółu pasażerów lotniczych korzystających z lotów między Unią a Kanadą” (pkt 127). Uznał on, że „przekazywanie danych PNR do Kanady i ich późniejsze przetwarzanie są przydatne do zapewnienia osiągnięcia celu przewidywanej umowy związanego z zapewnieniem ochrony publicznej i bezpieczeństwa publicznego” (pkt 153).

W odniesieniu do zainteresowanych pasażerów Trybunał stwierdził:

„186. Przewidywana umowa obejmuje dane PNR ogółu pasażerów korzystających z lotów między Unią a Kanadą. Przekazywanie tych danych Kanadzie następuje niezależnie od jakiegokolwiek obiektywnego elementu pozwalającego na uznanie, że pasażerowie mogą stanowić zagrożenie dla bezpieczeństwa publicznego.

187. W tej kwestii należy zauważyć, że – jak wskazano w pkt 152 i 169 niniejszej opinii – dane PNR podlegają w szczególności przetwarzaniu w sposób zautomatyzowany. I tak, jak podkreśliło wielu interwenientów, przetwarzanie to ma na celu zidentyfikowanie ryzyka dla bezpieczeństwa publicznego, jakie ewentualnie mogłyby stwarzać osoby, które na tym etapie nie są znane właściwym służbom, a które ze względu na to ryzyko mogłyby zostać poddane dokładniejszemu sprawdzeniu. W tej kwestii należy wskazać, 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.

188. Zresztą zgodnie z art. 13 konwencji chicagowskiej, na który powołały się w szczególności Rada i Komisja w odpowiedziach na pytania Trybunału, wszyscy pasażerowie z chwilą przybycia na terytorium umawiającego się państwa, podczas pobytu na nim oraz przy opuszczaniu tego terytorium podlegają ustawom i przepisom tego państwa dotyczącym przybycia pasażerów lotniczych na jego terytorium lub opuszczenia go. Wszyscy pasażerowie lotniczy zainteresowani przybyciem do Kanady lub opuszczenia tego państwa na podstawie tego artykułu podlegają zatem kontrolom granicznym oraz mają obowiązek przestrzegania warunków wjazdu i wyjazdu określonych obowiązującym prawem kanadyjskim. Ponadto, jak wynika z pkt 152 i 187 niniejszej opinii, identyfikacja za pomocą danych PNR pasażerów mogących stanowić zagrożenie dla bezpieczeństwa publicznego stanowi część kontroli granicznych. W konsekwencji pasażerowie lotniczy zamierzający przybyć do Kanady i tam przebywać, ponieważ podlegają

wspomnianym kontrolom, ze względu na samą istotę tego środka są objęci sprawdzeniem ich danych PNR.

189. W tych okolicznościach okazuje się, że przewidywana umowa nie wykracza poza granice tego, co ściśle konieczne, gdy pozwala na przekazywanie danych PNR wszystkich pasażerów lotniczych do Kanady”.

- 64 Cour constitutionnelle (trybunał konstytucyjny) zastanawia się, czy te rozważania można przenieść na grunt dyrektywy PNR oraz ustawodawstwa krajowego, takiego jak ustawa PNR, która transponując dyrektywę PNR ustanawia uogólnione i niezróżnicowane gromadzenie, przekazywanie oraz wykorzystanie danych „PNR” dla wszystkich pasażerów podróżujących w transporcie lotniczym, kolejowym lub autobusowym, niezależnie od przekroczenia granic zewnętrznych Unii. System ten ma bowiem zastosowanie do osób, co do których brak jest dowodów mogących sugerować, że ich zachowanie może mieć związek, nawet pośredni lub daleki, z poważnymi przestępstwami i jest on szerszy niż system przewidziany w umowie „PNR” z Kanadą. W związku z obszernością danych, o których mowa, powstaje pytanie, czy środek ten przestrzega granice tego, co „absolutnie konieczne”. Przed rozstrzygnięciem sprawy co do istoty postanawia on zatem zwrócić się do Trybunału z czwartym pytaniem prejudycjalnym.

W przedmiocie celów przetwarzania danych „PNR” (art. 8 ustawy PNR)

- 65 Strona skarżąca kwestionuje definicję celów przetwarzania danych „PNR” zawartą w art. 8 ustawy PNR, które są znacznie szersze niż „szczególne cele”, które zostały ograniczone w dyrektywie PNR wyłącznie do przestępstw terrorystycznych i poważnych przestępstw. Uważa ona, że te cele wykraczają poza granice tego, co „absolutnie konieczne”.

Cele przetwarzania danych „PNR”, przewidziane w art. 1 ust. 2 i art. 6 ust. 2 dyrektywy PNR, stanowią jedynie cele zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (zob. także motyw 7 dyrektywy PNR).

Niektóre z celów przetwarzania, o których mowa w art. 8 ustawy PNR, odpowiadają przestępstwom wymienionym w załączniku II do dyrektywy PNR, zgodnie z celami zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, o których mowa we wspomnianej dyrektywie. Niemniej jednak inne cele przetwarzania danych „PNR” stanowią uzupełnienie celów przewidzianych w tej dyrektywie. Chodzi tu między innymi o „monitorowanie działalności, o których mowa w art. 7 pkt 1 i 3 ppkt 1 oraz art. 11 ust. 1 pkt 1–3 i 5 ustawy organicznej z dnia 30 listopada 1998 r. o służbach wywiadowczych i bezpieczeństwa” (art. 8 ust. 1 pkt 4).

Sąd odsyłający bada, czy te inne cele zostały wyrażone w sposób jasny, precyzyjny i ograniczony do tego, co jest absolutnie konieczne oraz ma wątpliwości co do celu, o którym mowa w art. 8 ust. 1 pkt 4 ustawy PNR.

W uzasadnieniu do ustawy PNR wskazano, że ów „cel jest związany z kompetencjami służb wywiadowczych, a mianowicie: Sûreté de l'État et le Service général de Renseignement et de Sécurité (służby bezpieczeństwa państwa i ogólne służby wywiadowcze i bezpieczeństwa, SGRS). W celu wykonywania swoich zadań w zakresie pozyskiwania, analizy i przetwarzania informacji dotyczących działalności, które mogą stanowić zagrożenie dla podstawowych interesów państwa, służby te powinny mieć możliwość zbadania danych pasażerów w celu wykrycia możliwie najwcześniej konkretnych zagrożeń, monitorowania przemieszczania się określonych osób, czy też dokonania analizy szerszych zjawisk i tendencji. Zadania w zakresie pozyskiwania, analizy i przetwarzania informacji dotyczących działalności zagranicznych służb wywiadowczych na terytorium belgijskim wchodzą w zakres tego celu” (Doc. Parl, Chambre, 2018-2019, DOC 54-3652/001, s. 19-20).

O ile zadania służb wywiadowczych i bezpieczeństwa przyczyniają się ogólnie do zapewnienia bezpieczeństwa narodowego i międzynarodowego, o tyle przetwarzanie danych „PNR” w świetle celu, o którym mowa w art. 8 ust. 1 pkt 4 ustawy PNR, wydaje się bardzo niejasne i ogólne.

Cel ten jest ponadto, z punktu widzenia wstępnej oceny pasażerów, traktowany tak samo jak cele określone w art. 8 ust. 1 pkt 1, 2 i 5 ustawy PNR (art. 24 ust. 2 i art. 26 ust. 2).

W tym kontekście Cour constitutionnelle postanowił zwrócić się do Trybunału z piątym pytaniem prejudycjalnym w celu rozstrzygnięcia, czy cel ten jest wystarczająco jasny, precyzyjny i ograniczony do tego, co jest absolutnie konieczne.

W przedmiocie zarządzania bazą danych pasażerów i przetwarzaniem danych w ramach wstępnej oceny pasażerów i wyszukiwań ad hoc (art. 16, 24–27, 50 i 51 ustawy PNR)

- 66 Strona skarżąca uważa, że różne przypadki przetwarzania i przepływu danych osobowych są w oczywisty sposób nieproporcjonalne.
- 67 W art. 16 ustawy PNR przewidziano, że w ramach celów określonych w art. 8 ust. 1 dane pasażerów są przetwarzane, zgodnie z art. 24–27.

– *Wstępna ocena pasażerów (art. 24–26)*

- 68 Dane pasażerów są przetwarzane w celu dokonania wstępnej oceny („pre-screening”) pasażerów przed ich planowanym przyjazdem, odjazdem lub przejazdem przez terytorium kraju w celu ustalenia, które osoby powinny

podlegać bardziej szczegółowej kontroli. „Chodzi o dokonanie oceny potencjalnego zagrożenia i ustalenie, którzy pasażerowie są przedmiotem zainteresowania z punktu widzenia wykonywanych przez nich zadań lub na przykład wymagają podjęcia danego środka (wykonania nakazu aresztowania, przeszukania [...])” (Doc. Parl, Chambre, 2018-2019, DOC 54-3652/001, s. 28).

Wstępna ocena opiera się na dwóch aspektach: po pierwsze, korelacja danych pasażerów z bazami danych, a po drugie, korelacja danych z określonymi wcześniej kryteriami.

- 69 Co się tyczy korelacji z bazami danych, prace przygotowawcze nad ustawą PNR wskazują, że „[p]ierwszy aspekt polega na skojarzeniu danych poprzez zestawienie danych pasażerów z danymi przetwarzanymi w bazach danych zarządzanych przez właściwe służby. Pozwala to na przykład ocenić, czy dana osoba wykazuje wysoki stopień zagrożenia, ponieważ figuruje ona w policyjnej bazie danych w ramach dokumentacji dotyczącej terroryzmu, a z analizy danych pasażera wynika, że osoba ta udaje się regularnie do krajów, w których znajdują się obozy szkoleniowe terrorystów lub do krajów, przez które się przejeżdża do takich miejsc. Może na przykład chodzić również o osobę, w odniesieniu do której informacje dostępne w służbach wywiadowczych wskazują, że przygotowuje ona porwanie zakładników i że na podstawie danych na temat transportu udaje się ona do państwa, o którym służby wywiadowcze wiedzą na podstawie otrzymanych informacji, że osoba ta mogłaby tam werbować ludzi w celu wykonania jej planów. Ponadto im więcej zgodności zostanie wykrytych przez różne służby w odniesieniu do tej samej osoby, tym większe jest prawdopodobieństwo, że istnieje realne zagrożenie.

Skojarzenie danych może również spowodować konieczność podjęcia środka na podstawie nakazu organu sądowego, takiego jak wykonanie nakazu aresztowania osoby, która zamierza opuścić Belgię.

Skojarzenie danych może wynikać również z korelacji z międzynarodowymi bazami danych, takimi jak SIS II, Interpol (SLTD).

Celem nie jest oczywiście powiązanie wszystkich baz danych służb z bazą danych pasażerów, lecz ograniczenie pod względem technicznym korelacji z bazami danych w bezpośrednim związku z celami takimi, jak cele określone w ustawie.

[...]

Korelacja ta będzie mogła również odbywać się za pośrednictwem wykazów osób opracowanych specjalnie w tym celu przez właściwe służby. Zgodnie z ustawą o ochronie życia prywatnego, a w szczególności z jej art. 4 ust. 1 pkt 4, wykazy te muszą być regularnie uaktualniane” (Doc. Parl, Chambre, 2015-2016, DOC 54-2069/001, s. 28-29).

- 70 W odniesieniu do korelacji z określonymi wcześniej kryteriami prace przygotowawcze do ustawy PNR wyjaśniają:

„Drugi aspekt polega na skojarzeniu danych za pomocą określonych wcześniej przez JIP kryteriów (jednego lub więcej), stosowanych w odniesieniu do danych pasażerów. Kryteria te składają się z jednego lub kilku obiektywnych wskaźników, na podstawie których można wywieść, że osoby, do których się one odnoszą, zachowują się w sposób wywołujący szczególne ryzyko, mogące stanowić zagrożenie w świetle celów, o których mowa w art. 8 ust. 1 pkt 1, 4 i 5 ustawy.

Kryteria te mogą na przykład obejmować pewne szczególne zachowania w kontekście rezerwacji lub podróży.

Ich wykorzystanie ma tę zaletę, że może spowodować wykrycie profili pasażerów stanowiących zagrożenie, którzy niekoniecznie są znani lub wymieniani w bazach danych służb.

Kryteria te mogą dotyczyć na przykład kraju przeznaczenia lub wyjazdu w związku z pewnymi informacjami na temat podróży, takimi jak sposób płatności i data rezerwacji” (Doc. Parl, Chambre, 2018-2019, DOC 54-3652/001, s. 29-30).

„Wstępna ocena przeprowadzona w ramach realizacji celu polegającego na monitorowaniu przez policję administracyjną zjawisk i ugrupowań związanych z radykalizacją postaw prowadzącej do aktów przemocy podlega znacznie bardziej restrykcyjnym warunkom niż inne cele [...]

Wstępna ocena dokonana w ramach innych celów opiera się na dostępie do wszystkich danych pasażerów wymienionych w art. 9” (ibid, s. 31).

„Skojarzenie danych powinno we wszystkich przypadkach zostać zatwierdzone przez JIP. W celu zapewnienia pełnego poszanowania prawa do ochrony danych osobowych [...] nie można bowiem podejmować żadnej decyzji wywierającej dla danej osoby skutki prawne lub mogącej wyrządzić jej poważną szkodę wyłącznie na podstawie zautomatyzowanego przetwarzania danych w zbiorze zawierającym informacje dotyczące jej podróży. To właśnie z tego powodu ocena ze strony człowieka poprzedza zawsze jakąkolwiek wiążącą dla osoby, której dane dotyczą decyzję.

Takie zatwierdzenie powinno nastąpić w przeciągu 24 godzin w celu uzyskania prawa dostępu do bazy danych pasażerów.

Po zatwierdzeniu skojarzenia danych służby, które tego dokonały, zapewniają skuteczne monitorowanie we właściwym terminie. Skuteczne monitorowanie może oznaczać aktywne działanie (przeszukanie, zatrzymanie [...]), ale może również chodzić o tymczasowe niepodjęcie żadnego aktywnego działania. Dokonanie tej oceny operacyjnej należy w pełni do właściwych służb” (ibid, s. 30–31).

- 71 Co się tyczy określonych wcześniej przez JIP kryteriów oceny, nie mogą one opierać się na danych ujawniających pochodzenie rasowe lub etniczne danej

osoby, jej przekonania religijne lub filozoficzne, poglądy polityczne, przynależność do związków zawodowych, stan zdrowia, życie seksualne lub orientację seksualną. Ocena pasażerów przed ich przyjazdem, przejazdem lub wyjazdem z punktu widzenia określonych wcześniej kryteriów odbywa się w sposób niedyskryminujący. Kryteria te nie mogą odnosić się do identyfikacji osoby i muszą być ukierunkowane, proporcjonalne i szczególne.

- 72 W opinii z dnia 19 sierpnia 2016 r. Komitet Doradczy konwencji nr 108 stwierdził, co następuje:

„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.

[...]

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.

Rozwój algorytmów eksploracji danych powinien opierać się na wynikach regularnych ocen potencjalnego wpływu przetwarzania danych na podstawowe prawa i wolności osób, których dane dotyczą.

Podstawową strukturę analiz należy oprzeć na określonych wcześniej wskaźnikach ryzyka, które zostały wcześniej jasno ustalone.

Znaczenie indywidualnych wyników tych automatycznych ocen powinno zostać starannie zbadane w każdym konkretnym przypadku przez określoną osobę i w sposób niezautomatyzowany” (opinia z dnia 19 sierpnia 2016 r., T-PD (2016) 18rev, s. 8).

- 73 W niniejszym przypadku bazy danych, o których mowa w art. 24, zostały precyzyjnie określone i pozostają w bezpośrednim związku z celami określonymi w art. 8 ustawy PNR. Chodzi tu bowiem o bazy danych „właściwych służb”, czyli służb policji, Sûreté de l'État (służb bezpieczeństwa państwa) lub Service général de Renseignement et de Sécurité et des Douanes (służb wywiadowczych i bezpieczeństwa oraz służb celnych).

Ponadto art. 24 ust. 4 i 5 ustawy PNR gwarantuje, że w przypadku skojarzenia danych systematyczne zautomatyzowane przetwarzanie podlega indywidualnej weryfikacji w sposób niezautomatyzowany w celu dokonania oceny, czy właściwe organy zobowiązane są podjąć działania zgodnie z prawem krajowym, jak wymaga tego art. 6 ust. 5 dyrektywy PNR.¹³

- 74 W opinii 1/15 (umowa PNR UE-Kanada) z dnia 26 lipca 2017 r. (EU:C:2017:592) Trybunał Sprawiedliwości podkreślił również konieczność indywidualnej ponownej oceny przeprowadzonej w sposób niezautomatyzowany przed podjęciem indywidualnego środka (pkt 173).

Wymóg interwencji ze strony człowieka po skojarzeniu danych stanowi gwarancję, że wstępna ocena nie opiera się wyłącznie na zautomatyzowanych środkach, a tym samym przyczynia się on do skuteczności tego systemu.

Systematyczna wstępna ocena pasażerów stanowi zatem co do zasady odpowiedni środek z punktu widzenia celu, który polega na identyfikacji zagrożeń dla bezpieczeństwa publicznego i zapobieganiu im.

Jak jednak stwierdził Trybunał Sprawiedliwości w ww. opinii 1/15 z dnia 26 lipca 2017 r., wypadki przetwarzania wynikające ze wstępnej oceny „mogą [...] dostarczać dodatkowych informacji na temat życia prywatnego pasażerów lotniczych” (pkt 131); ponadto „analizy te są dokonywane, mimo iż nie istnieją uzasadnione indywidualnymi okolicznościami powody pozwalające na uznanie, że dane osoby mogą stanowić zagrożenie dla bezpieczeństwa publicznego” (ibid, pkt 132).

Stwierdzając, że zautomatyzowane przetwarzanie danych „PNR”, oparte na określonych wcześniej modelach i kryteriach, obarczone jest znaczącym marginesem błędu (ibid, pkt 169–170), Trybunał uznał jednak, że „określone wcześniej modele i kryteria powinny być konkretne i wiarygodne, pozwalające [...] na uzyskanie wyników ukierunkowanych na osoby, na których mogłoby ciążyć racjonalne podejrzenie udziału w przestępstwach terrorystycznych lub poważnych przestępstwach międzynarodowych, a zarazem powinny być niedyskryminacyjne” oraz że „bazy danych, z którymi danych PNR są porównywane, powinny być wiarygodne, aktualne i ograniczone do danych wykorzystywanych przez Kanadę w związku ze zwalczania terroryzmu oraz poważnej przestępczości międzynarodowej” (ibid, pkt 172). Wreszcie, aby zagwarantować, że ocena ta nie ma charakteru dyskryminacyjnego i jest ograniczona do tego, co absolutnie konieczne, Trybunał uznał, że „wiarygodność i aktualność tych wcześniej określonych modeli i kryteriów powinna być przedmiotem wspólnego przeglądu – uwzględniającego dane statystyczne i badania międzynarodowe – wdrażania przewidywanej umowy”, rok po jej wejściu w życie, a następnie w regularnych odstępach (ibid, pkt 174).

- 75 Ponadto bardziej szczegółowe zdefiniowanie kryteriów, które miałyby służyć określeniu profili ryzyka wydaje się technicznie niemożliwe. Jak wskazano powyżej, kryteria te powinny być szczegółowe, wiarygodne i niedyskryminacyjne.
- 76 Chociaż dyrektywa PNR oraz ustawa PNR nie dają wskazówek co do sposobu, w jaki JIP określa kryteria stanowiące podstawę wstępnej oceny, gwarancje, które wiążą się z opracowaniem tych kryteriów, wydają się być wystarczające, aby

zaskarżony środek nie został uznany za nieproporcjonalny. W celu ustalenia, czy ta systematyczna wstępna ocena jest wystarczająco jasna, precyzyjna i ograniczona do tego, co absolutnie konieczne, należy jednak zadać Trybunałowi szóste pytanie prejudycjalne.

– *Wyszukiwania ad hoc (art. 27, 50 i 51)*

- 77 Artykuł 27 ustawy PNR zezwala na przetwarzanie danych pasażerów w celu przeprowadzenia wyszukiwań ad hoc, o których mowa w art. 8 ust. 1 pkt 1, 2, 4 i 5, na warunkach przewidzianych w art. 46f kodeksu postępowania karnego lub art. 16/3 ustawy z dnia 30 listopada 1998 r., ustanowionych odpowiednio w art. 50 i 51 ustawy PNR. Zgodnie z art. 20 ustawy PNR przesłanki stosowania art. 27 stosuje się również do wniosków o dostęp do danych po upływie sześciomiesięcznego terminu, o którym mowa w art. 19.
- 78 Artykuł 46f kodeksu postępowania karnego dotyczy wyszukiwań ad hoc w kontekście celu, o którym mowa w art. 8 ust. 1 pkt 1, 2 i 5 ustawy PNR. Środek ten obwarowany jest kilkoma gwarancjami, w tym wymogiem uprzedniej zgody prokuratora królewskiego.
- 79 Artykuł 16/3 ustawy z dnia 30 listopada 1998 r. dotyczy natomiast wyszukiwań ad hoc w kontekście celu, o którym mowa w art. 8 ust. 1 pkt 4 ustawy PNR. Środek ten jest obwarowany kilkoma gwarancjami, w tym wymogiem informowania i kontroli stałego Komitetu R.
- 80 Strona skarżąca uważa, że delegowani członkowie służb policyjnych należący do JIP nie są wystarczająco niezależni, aby móc ustosunkować się do wniosków o udzielenie dostępu do danych w ramach owych wyszukiwań ad hoc.
- 81 Artykuł 14 ust. 1 ustawy PNR określa skład JIP. W pracach przygotowawczych wskazano w tym względzie: *„Model belgijski opiera się na koncepcji multidyscyplinarnej jednostki organizacyjnej złożonej z urzędnika kierującego, pełniącego funkcję zarządzającą, członków administracyjnych i członków oddelegowanych z właściwych służb.*

JIP będzie składać się z:

- *urzędnika kierującego, wspieranego przez służbę wspierającą, który w ramach SPF Intérieur będzie odpowiedzialny w szczególności za zarządzanie bazą danych, wypełnianie obowiązków przewoźników i operatorów turystycznych, sprawozdawczość, zawieranie protokołów z właściwymi służbami i przestrzeganie warunków przetwarzania. Służba wspierająca będzie w szczególności składać się z analityków, prawników, ekspertów ICT i inspektora ds. ochrony danych, którzy będą posiadali niezbędne uprawnienia w zakresie bezpieczeństwa.*
- *członków oddelegowanych z właściwych służb wymienionych enumeratywnie w ust. 1 pkt 2, a mianowicie: służb policji, służb wywiadowczych i celnych. Precyzyjne cele jako takie stanowią pierwsze ograniczenie. Na przykład na*

poziomie zintegrowanych służb policji jest oczywiste, że dzielnicowy w policji miejscowej nie będzie mógł nigdy zapoznać się z danymi pasażerów, ponieważ cele te nie wchodzą w zakres jego zadań.

Delegowanie z właściwych służb ma na celu zagwarantowanie pewnego stopnia ekspertyzy, lecz nie wyklucza w żaden sposób porozumień między nimi w celu wspólnego oddelegowania” (Doc. Parl, Chambre, 2015-2016, DOC 54-2069/001, s. 22).

Ministre de la Sécurité et de l’Intérieur (minister bezpieczeństwa i spraw wewnętrznych) dodał, że „[w]yznaczony zostanie również data protection officer zajmujący się sporządzaniem sprawozdań dla Komisji w sprawie ochrony życia prywatnego” (Doc. parl, Chambre, 2015-2016, DOC 54-2069/003, s. 24).

Rozporządzenie królewskie z dnia 21 grudnia 2017 r. dotyczące wykonania ustawy PNR określa zasady dotyczące składu i organizacji JIP. W sprawozdaniu dla króla poprzedzającym to rozporządzenie królewskie wyjaśniono, że „[b]aza danych może być konsultowana jedynie w obrębie JIP wyłącznie przez członków JIP w ramach ich zadań, jak również przez inspektora ochrony danych”³.

Procedura oddelegowania została uregulowana w art. 12–21 tego rozporządzenia królewskiego. Okoliczność, że oddelegowani członkowie właściwych służb uczestniczą w działaniach JIP, ma zapewnić, aby JIP składała się z osób posiadających pewną wiedzę, w celu wzmocnienia w ten sposób skuteczności JIP. Ta możliwość oddelegowania została zresztą wyraźnie przewidziana w art. 4 ust. 3 dyrektywy PNR.

Nie ma żadnych podstaw, by uznać, że osoby te, nawet jeśli zachowują swój status w służbach, z których pochodzą, nie wykonują swoich funkcji w sposób niezależny w ramach JIP. Członkowie JIP podlegają ponadto sankcjom karnym w przypadku nieprzestrzegania tajemnicy zawodowej lub jeżeli świadomie i umyślnie zatrzymują informacje i dane w sprzeczności z celami określonymi w art. 8 (art. 48 i 49).

- 82 Jeśli chodzi o dostęp do danych „PNR” w ramach wyszukiwań ad hoc po upływie sześciomiesięcznego terminu, Trybunał uznał w opinii 1/15 (umowa PNR UE-Kanada) z dnia 26 lipca 2017 r. (EU:C:2017:592), że wykorzystywanie w ten sposób przechowywanych danych PNR powinno „opierać się na obiektywnych kryteriach, by określić okoliczności i warunki, w których kanadyjskie organy wskazane w przewidywanej umowie mogą mieć do nich dostęp w celu ich wykorzystania” oraz że „[w]ykorzystanie to powinno [...], z wyjątkiem nagłych, należycie uzasadnionych wypadków, być uzależnione od uprzedniej kontroli dokonywanej bądź przez sąd, bądź przez niezależny organ administracyjny, których rozstrzygnięcie zezwalające na wykorzystanie jest wydawane w następstwie uzasadnionego wniosku rzeczonych organów, złożonego w

³ Moniteur belge z dnia 29 grudnia 2017 r., wydanie drugie, s. 116833.

szczegółności w ramach postępowań mających na celu zapobieganie przestępstwom, ich wykrywanie lub ściganie” (pkt 208).

- 83 W celu zbadania, czy JIP można uznać za ten „inny [właściwy] organ krajowy” w rozumieniu art. 12 ust. 3 dyrektywy PNR, należy przed orzeczeniem co do istoty zwrócić się do Trybunału Sprawiedliwości z siódmym pytaniem prejudycjalnym.

W przedmiocie okresu przechowywania danych „PNR” (art. 18 ustawy PNR)

- 84 Strona skarżąca uważa, że termin pięciu lat, w którym przechowywane są dane „PNR”, jest nieproporcjonalny.

- 85 Motyw 25 dyrektywy PNR stanowi:

„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 wystarczająco długi okres, 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”.

- 86 Zgodnie z orzecznictwem Trybunału okres przechowywania danych powinien „zawsze spełniać obiektywne kryteria ustanawiające związek między danymi osobowymi podlegającymi zatrzymaniu a zamierzonym celem” (wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650, pkt 93; postanowienie z dnia 16 marca 2017 r., Tele2 Sverige i Watson i in., C-203/15 REC i C-698/15 REC, EU:C:2017:222, pkt 110; opinia 1/15 (porozumienie PNR UE-Kanada) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 191).

- 87 Co się tyczy konkretnie danych „PNR”, Trybunał Sprawiedliwości uznał w ww. opinii 1/15 z dnia 26 lipca 2017 r., że okres pięciu lat *„nie wykracza poza granice tego, co jest ściśle konieczne do celów zwalczania terroryzmu i poważnych przestępstw międzynarodowych”* (pkt 209), pod warunkiem, że *„jeżeli chodzi o pasażerów lotniczych, w odniesieniu do których takiego ryzyka nie zidentyfikowano w chwili ich przybycia do Kanady i aż do opuszczenia przez nich tego państwa trzeciego, okazuje się, że od chwili ich wyjazdu nie istnieje chociażby pośredni związek między ich danymi PNR a celem przewidywanej umowy, który to związek uzasadniałby [...] [trwale przechowywanie] danych PNR wszystkich pasażerów lotniczych po opuszczeniu przez nich Kanady do celów ewentualnego dostępu do rzeczonych danych niezależnie od jakiegokolwiek*

związku ze zwalczania terroryzmu i poważnych przestępstw międzynarodowych (zob. analogicznie wyrok z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in., C-203/15 i C-698/15, EU:C:2016:970, pkt 119)” (pkt 205).

- 88 W art. 18 ustawy PNR przewidziano, że dane pasażerów są przechowywane w bazie danych pasażerów przez okres nieprzekraczający pięciu lat od chwili ich rejestracji, oraz że po upływie tego terminu są one usuwane. Zgodnie z art. 21 ust. 1 tej ustawy JIP zapewnia usunięcie danych pasażerów z jej bazy danych w sposób ostateczny, po upływie okresu, o którym mowa w art. 18.

Pięcioletni termin należy jednak odczytywać w związku z art. 19 i nast. tej ustawy, które również regulują sposoby przechowywania danych. Artykuł 19 tej ustawy należy natomiast interpretować w związku z art. 4 pkt 14, w którym zdefiniowano „depersonalizację poprzez maskowanie elementów danych” jako „fakt ukrycia przed użytkownikiem elementów danych, mogących służyć do bezpośredniej identyfikacji osoby, której dane dotyczą, o którym mowa w art. 19”.

W art. 20 ustawy PNR przewidziano, że po upływie sześciomiesięcznego okresu, o którym mowa w art. 19, udostępnienie wszystkich danych pasażerów jest dozwolone jedynie w celu przetwarzania danych, o którym mowa w art. 27 i wyłącznie zgodnie z warunkami określonymi w tym przepisie.

Ponadto JIP zachowuje wynik przetwarzania, o którym mowa w art. 24, jedynie przez okres niezbędny do poinformowania właściwych organów i JIP pozostałych państw członkowskich o skojarzeniu danych (art. 21 ust. 3 akapit pierwszy).

Artykuł 22 ustawy PNR gwarantuje, że urzędnik kierujący i inspektor ochrony danych mają dostęp do wszystkich istotnych danych jedynie w ramach wykonywania swoich zadań.

Wreszcie przetwarzanie danych jest codziennie uaktualniane i pozostaje w bezpośrednim związku z celami przewidzianymi w art. 8 (art. 23 ust. 1). JIP czuwa nad aktualizacją, zachowując przez okres pięciu lat dokumentację wszystkich systemów i procedur przetwarzania, za które jest odpowiedzialna (art. 23 ust. 2 akapit pierwszy).

- 89 Okres przechowywania danych pasażerów powinien zostać wyznaczony z uwzględnieniem celów przetwarzania tych danych, w bezpośrednim związku z celami zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania.
- 90 Commission de la protection de la vie privée (komisja ochrony życia prywatnego) stwierdziła jednak, że w przypadku gdy okres przechowywania danych jest długi, a dane są przechowywane masowo, „ryzyko profilowania osób, których dane dotyczą, wzrasta, podobnie jak ryzyko wypaczenia celów (*funkcja creep*), to znaczy potencjalnego nadużycia wykorzystania danych w odniesieniu do innych

przestępstw, co do których początkowo nie było (politycznego) porozumienia o wymianie danych” (Commission de la Protection de la Vie privée, opinia z inicjatywy własnej nr 01/2010 z dnia 13 stycznia 2010 r. dotycząca projektu ustawy w sprawie przystąpienia do porozumienia między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu danych dotyczących przelotu pasażerów (DHS) (porozumienie PNR 2007), sporządzonej w Brukseli w dniu 23 lipca 2007 r. i w Waszyngtonie w dniu 26 lipca 2007 r., pkt 3.3, s. 17–18).

W opinii nr 55/2015 z dnia 16 grudnia 2015 r. dotyczącej wstępnego projektu ustawy PNR Commission de la protection de la vie privée (komisja ochrony życia prywatnego) stwierdziła również, że konieczność przechowywania danych przez okres pięciu lat powinna być uzasadniona w sposób bardziej precyzyjny.

W opinii z dnia 19 sierpnia 2016 r. Komitet Doradczy konwencji nr 108 zwrócił również uwagę, 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” (opinia z dnia 19 sierpnia 2016 r. w sprawie T-PD (2016) 18rev, s. 9).

- 91 Cour constitutionnelle uważa, że w celu sprawdzenia, czy ów pięcioletni okres przechowywania, jaki dopuszcza dyrektywa PNR, w świetle powyższych rozważań i poszczególnych gwarancji wymienionych w pkt 88 powyżej, jest zgodny z uwagami Trybunału Sprawiedliwości wskazanymi w pkt 87 powyżej, ponieważ nie dokonuje on żadnego rozróżnienia w zależności od tego, czy w ramach wstępnej oceny okaże się, że dani pasażerowie mogą lub nie mogą stanowić zagrożenia dla bezpieczeństwa publicznego, konieczne jest przedstawienie Trybunałowi ósmego pytania prejudycjalnego.

3. W przedmiocie zarzutu drugiego

- 92 Strona skarżąca uważa, że rozszerzając system „PNR” na loty wewnątrzunijne, zaskarżone przepisy przywracają w sposób pośredni kontrole graniczne, które są sprzeczne ze swobodą przepływu osób.
- 93 W odniesieniu do zakresu stosowania ustawy PNR w pracach przygotowawczych wyjaśniono:

„Gromadzenie danych w zakresie przewozów wewnątrzunijnych pozwoli na uzyskanie bardziej kompleksowy obraz przejazdów pasażerów stanowiących potencjalne zagrożenie dla bezpieczeństwa wewnątrzspółnotowego i krajowego. Praktyka wykazała już, że niektórzy „returnees” (zwani także „foreign fighters”, którzy powracają do Europy) wsiadają na pokład różnych lotów przed osiągnięciem ich miejsca docelowego.

Dyrektywa UE PNR przewiduje wyraźnie możliwość przetwarzania przez państwa członkowskie danych pasażerów UE w ruchu międzynarodowym w Unii

Europejskiej. Ponadto w dniu 21 kwietnia 2016 r. wszystkie państwa członkowskie zatwierdziły w Conseil des ministres de l'Intérieur et de la Justice (radzie ministrów spraw wewnętrznych i sprawiedliwości) deklarację mającą na celu transpozycję dyrektywy UE PNR do praw krajowych także w odniesieniu do przejazdów wewnątrz Unii Europejskiej” (Doc. Parl., Chambre, 2015-2016, DOC 54-2069/001, s. 7).

- 94 Cour constitutionnelle podnosi, że pasażerowie, o których mowa w rozdziale 11 ustawy PNR, podobnie jak odnośne dane i okres przechowywania, są ograniczeni.

Prace przygotowawcze wyjaśniają bowiem, że „[...] chodzi jedynie o pasażerów, którzy chcą przekroczyć lub przekroczyli granice zewnętrzne Belgii, aby wjechać na terytorium tego państwa lub z niego wyjechać, i to niezależnie od wybranego środka transportu (morskiego, kolejowego, lądowego, powietrznego). Wyłącznie dane tych pasażerów będą zatem przetwarzane przez służby policji przeprowadzające kontrolę graniczną oraz Office des étrangers (urząd ds. cudzoziemców).

Dotyczy to także pasażerów, którzy zamierzają przejechać przez międzynarodową strefę tranzytową na przykład lotniska znajdującego się w Belgii, ponieważ przepisy dotyczące wjazdu na terytorium, pobytu, osiedlenia się i wydalenia cudzoziemców mają zastosowanie również do nich. Osoby te powinny zatem dysponować wymaganymi dokumentami podróży. Niektóre osoby podlegają obowiązkowi wizowemu w odniesieniu do tranzytu lotniczego; kontrole w tych strefach są dopuszczalne i mogą w niektórych przypadkach doprowadzić do wydalenia.

[...] jedynie dane pasażerów zwane „API” zostaną przekazane służbom policyjnym i urzędowi ds. cudzoziemców na mocy niniejszego rozdziału. Dane te zostały wymienione w art. 9 ust. 2 wstępnego projektu ustawy.

Odpowiadają one w istocie tym danym, które przewoźnicy lotniczy są już zobowiązani przekazać na mocy rozporządzenia królewskiego z dnia 11 grudnia 2006 r.

[...]

Wykorzystanie danych jest również ograniczone do 24 godzinnego okresu. Ponadto, jeżeli dostęp do danych pasażerów jest konieczny w ramach wykonywania zadań ustawowych urzędu ds. cudzoziemców, urząd ten przesyła JIP wnioszek z uzasadnieniem” (ibid), s. 34–35.

- 95 Jak to zostało wskazane powyżej, motyw 10 dyrektywy PNR zezwala na rozszerzenie systemu „PNR” na loty wewnątrzunijne. W art. 2 dyrektywy PNR ustanowiono procedurę mającą na celu rozszerzenie zakresu stosowania.

Cel walki z nielegalną imigracją i ulepszenia kontroli granicznych dotyczy wyłącznie kategorii pasażerów wymienionych w art. 29 ust. 2 ustawy PNR oraz

ogranicza się do danych „API”, o których mowa w art. 9 ust. 1 pkt 18 tej ustawy. Przetwarzanie dokonywane w ramach tego celu jest również ograniczone. Zaskarżone przepisy wpisują się w ramy transpozycji dyrektywy „API”, która ma również na celu zwalczanie nielegalnej imigracji i ulepszenie kontroli granicznych.

- 96 W swojej opinii nr 55/2015 z dnia 16 grudnia 2015 r. w sprawie wstępnego projektu ustawy przyjętej w dniu 25 grudnia 2016 r. Komisja ochrony życia prywatnego zastanawia się jednakże co do zgodności z zasadą swobodnego przepływu osób wprowadzonego systemu „PNR”, który odnosi się „zarówno do przewozów do i ze strefy Schengen (spoza strefy Schengen), jak i do wjazdów i wyjazdów ze strefy Schengen (wewnątrz strefy Schengen)”, co może prowadzić „w sposób pośredni do przywrócenia kontroli na granicach wewnętrznych” (pkt 21–25).
- 97 Mając wątpliwości co do wykładni i ważności dyrektywy 2004/82 „API” w świetle karty i TUE, Cour constitutionnelle postanawia przedłożyć Trybunałowi dziewięć pytań prejudycjalnych.
- 98 Cour constitutionnelle przedstawia ostatnie pytanie dotyczące ewentualnego dostosowania skutków swego wyroku w czasie.

IV. Pytania prejudycjalne

Cour constitutionnelle przedstawia zatem następujące pytania prejudycjalne:

1. Czy 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 – 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. „w sprawie przetwarzania danych pasażerów”, która dokonuje transpozycji 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”, dyrektywy Rady 2004/82/WE z dnia 29 kwietnia 2004 r. „w sprawie zobowiązania przewoźników do przekazywania danych pasażerów” 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”?

2. Czy w zakresie, w jakim wymienione w załączniku I do dyrektywy (UE) 2016/681 dane są bardzo obszerne – w szczególności dane, o których mowa w pkt

18 załącznika I do dyrektywy (UE) 2016/681, które wykraczają poza dane określone w art. 3 ust. 2 dyrektywy 2004/82/WE – 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 praw podstawowych Unii Europejskiej?

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 (UE) 2016/681, 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 praw podstawowych Unii Europejskiej?

4. Czy w zakresie, w jakim ustanowiony w art. 3 pkt 4 dyrektywy (UE) 2016/681 i 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 praw podstawowych Unii Europejskiej?

5. Czy art. 6 dyrektywy (UE) 2016/681 w związku z art. 7, 8 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej należy interpretować w ten sposób, że stoi on na przeszkodzie ustawodawstwu krajowemu takiemu jak zaskarżona ustawa, która dopuszcza, jako cel przetwarzania danych „PNR”, monitorowanie działalności wywiadowczej 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 (UE) 2016/681 jest zgodny z art. 7, 8 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej 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 (UE) 2016/681, 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 (UE) 2016/681 w związku z art. 7, 8 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej należy interpretować w ten sposób, że stoi on na przeszkodzie ustawodawstwu krajowemu takiemu jak zaskarżona ustawa, 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 2004/82/WE jest zgodna z art. 3 ust. 2 Traktatu o Unii Europejskiej i art. 45 Karty praw podstawowych Unii Europejskiej w zakresie, jakim ustanowione w niej obowiązki mają zastosowanie do lotów wewnątrz Unii Europejskiej?

b) Czy dyrektywę 2004/82/WE w związku z art. 3 ust. 2 Traktatu o Unii Europejskiej i art. 45 Karty praw podstawowych Unii Europejskiej 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 miałyby dojść do wniosku, że zaskarżona ustawa, transponująca w szczególności dyrektywę (UE) 2016/681, 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. „o przetwarzaniu danych pasażerów”, aby uniknąć niepewności prawa i zapewnić możliwość dalszego wykorzystywania uprzednio zgromadzonych i przechowywanych danych do celów określonych w ustawie?