



Zbiór Orzeczeń

OPINIA RZECZNIKA GENERALNEGO
GIOVANNIEGO PITRUZZELLI
przedstawiona w dniu 27 stycznia 2022 r.¹

Sprawa C-817/19

**Ligue des droits humains
przeciwko
Conseil des ministres**

[wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Cour constitutionnelle
(Belgia)]

Odesłanie prejudycjalne – Ochrona danych osobowych – Przetwarzanie danych dotyczących
przelotu pasażera (PNR) – Rozporządzenie (UE) 2016/679 – Zakres stosowania – Dyrektywa
(UE) 2016/681 – Ważność Karta praw podstawowych Unii Europejskiej – Artykuły 7, 8
i art. 52 ust. 1

Spis treści

I.	Wprowadzenie	3
II.	Ramy prawne	4
A.	Prawo Unii	4
1.	Karta	4
2.	RODO	5
3.	Dyrektywa PNR	5
4.	Inne istotne akty prawa Unii	8
B.	Prawo belgijskie	8
C.	Postępowanie główne, pytania prejudycjalne oraz postępowanie przed Trybunałem	10

¹ Język oryginału: francuski.

III. Analiza	13
A. W przedmiocie pierwszego pytania prejudycjalnego	13
B. W przedmiocie pytań prejudycjalnych drugiego, trzeciego, czwartego, szóstego i ósmego ..	20
1. W przedmiocie praw podstawowych zapisanych w art. 7 i 8 karty	20
2. W przedmiocie ingerencji w prawa podstawowe ustanowione w art. 7 i 8 karty	21
3. W przedmiocie uzasadnienia ingerencji wynikającej z dyrektywy PNR	26
a) W przedmiocie poszanowania wymogu, aby wszelkie ograniczenia w korzystaniu z prawa podstawowego zapisanego w karcie były przewidziane ustawą	26
b) W przedmiocie poszanowania istoty praw zapisanych w art. 7 i 8 karty	27
c) W przedmiocie poszanowania wymogu, zgodnie z którym ingerencja musi odpowiadać celowi interesu ogólnego	30
d) W przedmiocie przestrzegania zasady proporcjonalności	31
1) W przedmiocie przydatności operacji przetwarzania danych PNR, o których mowa w dyrektywie PNR, do realizacji zamierzonego celu	32
2) W przedmiocie absolutnie koniecznego charakteru ingerencji	33
i) W przedmiocie określenia celów przetwarzania danych PNR	33
ii) W przedmiocie kategorii danych PNR objętych dyrektywą PNR (pytania prejudycjalne drugie i trzecie)	37
– W przedmiocie wystarczająco jasnego i precyzyjnego charakteru pkt 12 i 18 załącznika I (trzecie pytanie prejudycjalne)	38
– W przedmiocie zakresu danych wymienionych w załączniku I (drugie pytanie prejudycjalne)	46
– W przedmiocie danych szczególnie chronionych	49
iii) W przedmiocie pojęcia „pasażera” (czwarte pytanie prejudycjalne)	51
iv) W przedmiocie wystarczająco jasnego, precyzyjnego i ograniczonego do tego, co absolutnie konieczne, charakteru wstępnej oceny pasażerów (szóste pytanie prejudycjalne)	57
– W przedmiocie porównania z bazami danych w rozumieniu art. 6 ust. 3 lit. a) dyrektywy PNR	58
– W przedmiocie przetwarzania danych PNR w świetle wcześniej ustalonych kryteriów	60
– W przedmiocie gwarancji związanych ze zautomatyzowanym przetwarzaniem danych PNR	62

– Wnioski w przedmiocie szóstego pytania prejudycjalnego	64
v) W przedmiocie przechowywania danych PNR (ósme pytanie prejudycjalne)	64
4. Wnioski w przedmiocie pytań prejudycjalnych drugiego, trzeciego, czwartego, szóstego i ósmego	69
C. W przedmiocie piątego pytania prejudycjalnego	70
D. W przedmiocie siódmego pytania prejudycjalnego	71
E. W przedmiocie dziewiątego pytania prejudycjalnego	74
F. W przedmiocie dziesiątego pytania prejudycjalnego	77
IV. Wnioski	78

I. Wprowadzenie

1. We wniosku o wydanie orzeczenia w trybie prejudycjalnym w niniejszej sprawie Cour constitutionnelle (trybunał konstytucyjny, Belgia) zwraca się do Trybunału z serią dziesięciu pytań prejudycjalnych dotyczących wykładni 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 (ogólne rozporządzenie w sprawie ochrony danych, zwane dalej „RODO”)², a także ważności i wykładni 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 „dyrektywą PNR”)³ oraz dyrektywy Rady 2004/82/WE z dnia 29 kwietnia 2004 r. w sprawie obowiązku przekazywania przez przewoźników danych dotyczących pasażerów (zwanej dalej „dyrektywą API”)⁴. Pytania te podniesiono w ramach skargi złożonej przez stowarzyszenie o celu niezarobkowym Ligue des droits humains (zwane dalej „LDH”), mającej na celu stwierdzenie nieważności w całości lub w części ustawy z dnia 25 grudnia 2016 r. o przetwarzaniu danych pasażerów (zwanej dalej „ustawą PNR”)⁵, transponującej do prawa belgijskiego dyrektywę PNR i dyrektywę API.

2. Pytania, które Trybunał będzie musiał rozstrzygnąć w niniejszej sprawie, stanowią odbicie jednego z głównych dylematów współczesnego konstytucjonalizmu liberalno-demokratycznego: jak ustalić równowagę między jednostką a zbiorowością w erze danych, w której technologia cyfrowa umożliwiła gromadzenie, przechowywanie, przetwarzanie i analizę danych osobowych w ogromnej skali do celów prognostycznych? Stosowane przez organy władzy publicznej algorytmy, analiza big data i sztuczna inteligencja mogą służyć upowszechnianiu i ochronie podstawowych interesów społeczeństwa z niewyobrażalną dotychczas efektywnością: począwszy od ochrony zdrowia publicznego, przez zrównoważoną ochronę środowiska, aż po zwalczanie

² Dz.U. 2016, L 119, s. 1, sprostowania Dz.U. 2018, L 127, s. 2; Dz.U. 2021, L 74, s. 35.

³ Dz.U. 2016, L 119, s. 132.

⁴ Dz.U. 2004, L 261, s. 24.

⁵ *Moniteur belge* z dnia 25 stycznia 2017 r., s. 12905.

terroryzmu i zapobieganie przestępczości, a zwłaszcza poważnej przestępczości. Jednocześnie niezróżnicowane gromadzenie danych osobowych i wykorzystywanie technologii cyfrowych przez władze publiczne może prowadzić do powstania cyfrowego panoptikonu, to znaczy władzy publicznej, która widzi każdego, sama pozostając niewidoczna. Wszechwiedza władzy, zdolnej kontrolować i przewidywać zachowania każdej osoby i na tej podstawie podejmować działania, może prowadzić do paradoksalnego rezultatu, przedstawionego przez Stevena Spielberga w filmie *Minority Report* (*Raport mniejszości*), polegającego na prewencyjnym pozbawieniu wolności sprawcy przestępstwa, którego ten jeszcze nie popełnił. Jak wiadomo, w niektórych państwach społeczeństwo ma pierwszeństwo przed jednostką, a wykorzystywanie danych osobowych pozwala zgodnie z prawem na sprawowanie skutecznego nadzoru masowego, służącego ochronie interesów publicznych uznanych w tych państwach za podstawowe. Natomiast konstytucjonalizm europejski – krajowy i ponadnarodowy – w którym centralne miejsce zajmuje jednostka i jej swobody, stanowi istotne zabezpieczenie przed realizacją koncepcji społeczeństwa poddanego masowemu nadzorowi, przede wszystkim dzięki uznaniu praw podstawowych do ochrony życia prywatnego i ochrony danych osobowych. Na ile jednak zabezpieczenie to można ustanowić bez poważnego osłabienia niektórych podstawowych interesów społeczeństwa, takich jak wymienione wcześniej tytułem przykładu, które również mogą mieć konstytucyjne korzenie? Zagadnienie to leży u sedna pytania o relację między jednostką a zbiorowością w społeczeństwie cyfrowym. Jest to pytanie, które z jednej strony wymaga znalezienia i urzeczywistnienia delikatnej równowagi między interesami ogółu a prawami jednostek, obierając za punkt wyjścia bezwzględne znaczenie, jakie prawa te mają w europejskim dziedzictwie konstytucyjnym, a z drugiej strony wiąże się z koniecznością ustanowienia gwarancji chroniących przed nadużyciami. Również tutaj mamy do czynienia ze współczesną wersją klasycznego problemu konstytucjonalizmu, ponieważ, jak stwierdza w sposób lapidarny *The Federalist*, ludzie nie są aniołami i dlatego niezbędne są mechanizmy prawne służące ograniczeniu i kontroli władzy publicznej.

3. Te właśnie pytania o charakterze ogólnym stanowią kontekst niniejszej opinii, która siłą rzeczy ogranicza się do wykładni prawa Unii w świetle wcześniejszego orzecznictwa Trybunału, za pomocą sprawdzonych technik, wśród których znajduje się wykładnia zgodna. Do techniki tej będę często sięgał w niniejszej opinii, gdy będzie to możliwe z prawnego punktu widzenia, w celu znalezienia niezbędnej z konstytucyjnego punktu widzenia równowagi pomiędzy celami publicznymi, na których opiera się system przekazywania, gromadzenia i przetwarzania danych dotyczących przelotu pasażera (zwanymi dalej „danymi PNR”), a prawami zapisanymi w art. 7 i 8 Karty praw podstawowych Unii Europejskiej (zwanej dalej „kartą”).

II. Ramy prawne

A. Prawo Unii

1. Karta

4. Zgodnie z art. 7 karty: „[k]ażdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się”.

5. Zgodnie z brzmieniem art. 8 karty:

„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”.

6. Zgodnie z art. 52 ust. 1 karty: „[w]szelkie ograniczenia w korzystaniu z praw i wolności uznanych w niniejszej [k]arcie 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”.

2. RODO

7. Artykuł 2 ust. 2 lit. d) RODO wyłącza z zakresu stosowania tego rozporządzenia przetwarzanie danych osobowych prowadzone „przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom”.

8. Zgodnie z art. 23 ust. 1 lit. d) RODO:

„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 obowiązkowi 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:

[...]

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”.

3. Dyrektywa PNR

9. Poniżej przedstawię jedynie krótki przegląd funkcjonowania systemu ustanowionego dyrektywą PNR. Bardziej szczegółowe informacje na temat treści przepisów tej dyrektywy, mających znaczenie dla odpowiedzi na pytania prejudycjalne, przedstawię w toku analizy prawnej.

10. Zgodnie z art. 1 dyrektywy PNR, przyjętej na podstawie art. 82 ust. 1 lit. d) TFUE i art. 87 ust. 2 lit. a) TFUE, ustanawia ona na szczeblu Unii system przekazywania przez przewoźników lotniczych danych PNR lotów pozaunijnych⁶, jak również gromadzenia, przetwarzania i przechowywania tych danych przez właściwe organy państw członkowskich w celu zwalczania terroryzmu i poważnej przestępczości.

11. Zgodnie z art. 3 pkt 5 tej dyrektywy „dane dotyczące przelotu pasażera” lub „dane PNR” oznaczają „zbiór danych o podróży każdego pasażera, który zawiera informacje niezbędne, aby umożliwić przetwarzanie i weryfikowanie rezerwacji przez przewoźników lotniczych obsługujących rezerwację i lot w odniesieniu do każdego przelotu zarezerwowanego przez jakąkolwiek osobę lub w jej imieniu, bez względu na to, czy zbiór ten znajduje się w systemach rezerwacji, systemach odpraw pasażerskich lub równorzędnych systemach pełniących te same funkcje”.

12. Załącznik I do dyrektywy PNR (zwany dalej „załącznikiem I”) wymienia dane dotyczące przelotu pasażera gromadzone przez przewoźników lotniczych, które są przekazywane w rozumieniu art. 8 tej dyrektywy i na zasadach określonych w tym artykule.

13. Załącznik II do dyrektywy PNR (zwany dalej „załącznikiem II”) zawiera wykaz przestępstw, które stanowią „poważną przestępczość” w rozumieniu art. 3 pkt 9 tej dyrektywy.

14. Artykuł 2 dyrektywy PNR przewiduje możliwość podjęcia decyzji przez państwa członkowskie o stosowaniu tej dyrektywy również do „lotów wewnątrzunijnych”⁷ lub tylko do wybranych lotów wewnątrzunijnych, uznanych za „niezbędne” do realizacji celów tej dyrektywy.

15. Zgodnie z brzmieniem art. 4 ust. 1 dyrektywy PNR „[k]ażde 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«)”. Zgodnie z ust. 2 lit. a) rzeczonego art. 4 do zadań JIP należy między innymi zbieranie od przewoźników lotniczych danych PNR, ich przechowywanie i przetwarzanie, a także przekazywanie tych danych lub wyników ich przetwarzania właściwym organom, o których mowa w art. 7 dyrektywy PNR. Zgodnie z ust. 2 rzeczonego art. 7 organy te „są organami właściwymi do zapobiegania przestępstwom terrorystycznym lub poważnym przestępstwom, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania”⁸.

⁶ Zgodnie z art. 3 pkt 2 dyrektywy PNR „lot pozaunijny” oznacza „regularny lub nieregularny lot, obsługiwany przez przewoźnika lotniczego, odbywający się z państwa trzeciego, z zaplanowanym lądowaniem na terytorium państwa członkowskiego albo odbywający się z terytorium państwa członkowskiego, z zaplanowanym lądowaniem w państwie trzecim, w tym – w obu przypadkach – loty z postojami na terytorium państw członkowskich lub państw trzecich”.

⁷ Zgodnie z art. 3 pkt 3 dyrektywy PNR „lot wewnątrzunijny” oznacza „regularny lub nieregularny lot, obsługiwany przez przewoźnika lotniczego, odbywający się z terytorium państwa członkowskiego, z zaplanowanym lądowaniem na terytorium co najmniej jednego innego państwa członkowskiego, bez postojów na terytorium państwa trzeciego”.

⁸ Artykuł 7 ust. 1 dyrektywy PNR przewiduje, że każde państwo członkowskie sporządza wykaz właściwych organów uprawnionych do występowania do JIP o dane PNR lub o wyniki przetwarzania tych danych lub do otrzymywania takich danych i wyników ich przetwarzania od JIP na potrzeby dalszego sprawdzenia tych informacji lub podjęcia odpowiednich czynności w celu zapobiegania przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania. Wykaz ten został opublikowany przez Komisję w 2018 r. (Dz.U. 2018, C 194, s. 1; sprostowanie Dz.U. 2020, C 366, s. 55).

16. Zgodnie z brzmieniem art. 6 ust. 1 zdanie drugie dyrektywy PNR, „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”. Ustęp 2 tego artykułu stanowi, co następuje:

„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”.

17. Artykuł 12 dyrektywy PNR zawiera przepisy dotyczące przechowywania danych PNR.

18. Artykuł 5 dyrektywy PNR przewiduje, że każda JIP powołuje inspektora ochrony danych, który odpowiada za monitorowanie przetwarzania danych PNR i stosowanie odpowiednich gwarancji. Ponadto każde państwo członkowskie jest zobowiązane, zgodnie z art. 15 tej dyrektywy, do powierzenia krajowemu organowi nadzorczemu, o którym mowa w art. 25 decyzji ramowej 2008/977/WSiSW⁹, zastąpionej dyrektywą 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 (zwaną dalej „dyrektywą policyjną”)¹⁰, nadzoru nad stosowaniem na jego terytorium przepisów przyjętych na podstawie tej dyrektywy. Organ ów, który wykonuje swoje zadania w celu ochrony praw podstawowych w związku z przetwarzaniem danych osobowych¹¹, jest odpowiedzialny w szczególności, po pierwsze, za rozpatrywanie skarg złożonych przez osoby, których dane dotyczą, badanie danej sprawy oraz, w rozsądnym terminie, informowanie osób, których dane dotyczą, o postępach i wyniku

⁹ Decyzja Rady z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz.U. 2008, L 350, s. 60).

¹⁰ Dz.U. z 2016 r., L 119, s. 89; sprostowanie Dz.U. 2018, L 127, s. 10. Artykuł 25 decyzji ramowej 2008/977 został zastąpiony przez art. 41 dyrektywy policyjnej.

¹¹ Zobacz art. 15 ust. 2 dyrektywy PNR.

rozpatrzenia ich skarg, a po drugie, za sprawdzanie zgodności z prawem przetwarzania danych, prowadzenie postępowań, inspekcji i audytów zgodnie z prawem krajowym, z własnej inicjatywy lub na podstawie skargi¹².

4. *Inne istotne akty prawa Unii*

19. Ramy prawne niniejszej sprawy uzupełniają dyrektywa API i dyrektywa policyjna. W trosce o czytelność niniejszej opinii treść odpowiednich przepisów tych aktów zostanie przedstawiona w zakresie, w jakim będzie to konieczne przy badaniu pytań, które ich dotyczą, lub w sposób bardziej ogólny dla potrzeb analizy prawnej.

B. Prawo belgijskie

20. Zgodnie z art. 22 konstytucji belgijskiej „[k]ażdy człowiek ma prawo do poszanowania jego życia prywatnego i rodzinnego, z wyjątkiem przypadków i warunków określonych w ustawie”.

21. Ustawa PNR, zgodnie z jej art. 2, dokonuje transpozycji dyrektywy API i dyrektywy PNR, a także częściowo dyrektywy 2010/65/UE¹³.

22. Ustawa PNR zgodnie z jej art. 3 § 1 „określa obowiązki przewoźników i operatorów turystycznych związane z przekazywaniem danych pasażerów udających się na terytorium kraju, przybywającym z niego lub przez nie przejeżdżającym”. Zgodnie z art. 4 pkt 1 i 2 tej ustawy „przewoźnik” oznacza „każdą osobę fizyczną lub prawną, która zawodowo zajmuje się transportem osób drogą lotniczą, morską, kolejową lub lądową”, a „operator turystyczny” to „organizator turystyczny lub pośrednik turystyczny w rozumieniu ustawy z dnia 16 lutego 1994 r. regulującej umowę o organizację podróży oraz umowę pośrednictwa w organizacji podróży”.

23. Artykuł 8 ustawy PNR stanowi:

„§ 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 art. 90b § 2 [...] pkt 7, [...] 8, [...] 11, [...] 14, [...] 17, 18, 19 i [art. 90] § 3 Code d’Instruction criminelle (kodeksu postępowania karnego);
- 2) poszukiwania i ścigania, w tym wykonywania kar lub środków ograniczenia wolności, dotyczących przestępstw, o których mowa w art. 196 w odniesieniu do przestępstw fałszowania dokumentów urzędowych i publicznych, art. 198, 199, 199a, 207, 213, 375 i 505 Code pénal (kodeksu karnego);
- 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);

¹² Zobacz art. 15 ust. 3 lit. a) i b) dyrektywy PNR.

¹³ Dyrektywa Parlamentu Europejskiego i Rady z dnia 20 października 2010 r. w sprawie formalności sprawozdawczych dla statków wchodzących do lub wychodzących z portów państw członkowskich i uchylająca dyrektywę 2002/6/WE (Dz.U. 2010, L 283, s. 1).

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)¹⁴;

5) poszukiwania i ścigania przestępstw, o których mowa w art. 220 § 2 loi générale sur les douanes et accises (ogólnej ustawy o cłach i podatku akcyzowym) z dnia 18 lipca 1977 r. i art. 45 akapit trzeci loi du 22 décembre 2009 relative au régime général d'accise (ustawy z dnia 22 grudnia 2009 r. w sprawie ogólnych zasad dotyczących podatku akcyzowego) [...].

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

24. Artykuł 9 ustawy PNR zawiera wykaz danych podlegających przekazywaniu. Dane te odpowiadają danym wymienionym w załączniku I.

25. Artykuł 18 ustawy PNR przewiduje, że „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”.

26. Artykuł 19 tej ustawy przewiduje, że „[z] chwilą upływu okresu sześciu miesięcy od dnia rejestracji danych pasażerów w bazie danych pasażerów wszystkie dane dotyczące przelotów pasażerów są depersonalizowane poprzez maskowanie informacji”.

27. Artykuł 24 ustawy PNR przewiduje:

„§ 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.

§ 2. W ramach celów, o których mowa w art. 8 § 1 pkt 1, 4 i 5, lub dotyczących zagrożeń, o których mowa w art. 8 pkt 1 lit. a), b), c), d), f), g) i art. 11 § 2 ustawy organicznej z dnia 30 listopada 1998 r. o służbie wywiadowczej i bezpieczeństwa, wstępna ocena pasażerów opiera się na skojarzeniu danych w wyniku skorelowania danych pasażerów z:

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

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

§ 3. W ramach celów, o których mowa w art. 8 § 1 pkt 3, wstępna ocena pasażerów opiera się na skojarzeniach danych wynikających ze skorelowania danych pasażerów z bankami danych, o których mowa w § 2 pkt 1. [...]”.

28. Artykuł 25 ustawy PNR stanowi powtórzenie treści art. 6 ust. 4 dyrektywy PNR.

¹⁴ *Moniteur belge* z dnia 18 grudnia 1998 r., s. 40312.

29. Rozdział 11 ustawy PNR zawiera przepisy regulujące przetwarzanie danych pasażerów z zamiarem ulepszenia kontroli na granicach zewnętrznych i zwalczania nielegalnej imigracji. Przepisy te stanowią transpozycję do prawa belgijskiego dyrektywy API.

30. Artykuł 44 ustawy PNR przewiduje, że JIP wyznacza inspektora ochrony danych w ramach Service Public Fédéral Intérieur (ministerstwa spraw wewnętrznych). Nadzór nad stosowaniem przepisów ustawy PNR prowadzi Commission de la protection de la vie privée (komisja do spraw ochrony prywatności).

31. Artykuł 51 ustawy PNR dokonuje zmiany ustawy organicznej z dnia 30 listopada 1998 r. o służbach wywiadowczych i bezpieczeństwa poprzez dodanie art. 16/3, który ma następujące brzmienie:

„§ 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. 7 ustawy [PNR].

§ 2. Decyzję, o której mowa w § 1, podejmuje szef służby, po czym informuje się o niej na piśmie jednostkę do spraw informacji o pasażerach, o której mowa w rozdziale 7 ww. ustawy. Decyzję wraz z uzasadnieniem doręcza się stałemu Komitetowi R.

Stały Komitet R zabrania służbom wywiadowczym i bezpieczeństwa wykorzystywania zebranych danych w warunkach, które nie spełniają wymogów prawnych.

Decyzja może dotyczyć zbioru danych dotyczących konkretnego dochodzenia wywiadowczego. W takim przypadku raz w miesiącu przekazuje się stałemu Komitetowi R wykaz przypadków zapoznania się z danymi pasażerów”.

C. Postępowanie główne, pytania prejudycjalne oraz postępowanie przed Trybunałem

32. Pismem skierowanym do Cour constitutionnelle (trybunału konstytucyjnego) w dniu 24 lipca 2017 r. LDH wniósł skargę o stwierdzenie nieważności ustawy PNR w całości lub w części. Na poparcie skargi organizacja ta podniosła dwa zarzuty.

33. W zarzucie pierwszym, podniesionym tytułem głównym i dotyczącym naruszenia art. 22 konstytucji belgijskiej w związku z art. 23 RODO, z art. 7, 8 i art. 52 ust. 1 karty oraz w związku z art. 8 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, podpisanej w Rzymie dnia 4 listopada 1950 r. (zwanej dalej „EKPC”), LDH wskazuje, że zaskarżona ustawa narusza zasadę proporcjonalności z uwagi na zakres jej stosowania i kategorie objętych nią danych, określone w niej sposoby przetwarzania danych, a także jej cele oraz czas przechowywania danych. W szczególności twierdzi, że definicja danych PNR jest zbyt szeroka i może doprowadzić do ujawnienia danych szczególnie chronionych, a zawarta w tej ustawie definicja pojęcia „pasażera” pozwala na systematyczne nieukierunkowane przetwarzanie danych wszystkich pasażerów, których te dane dotyczą. LDH uważa ponadto, że ustawa PNR nie określa w sposób wystarczająco jasny charakteru i szczegółowych zasad metody *pre-screeningu* banków danych pasażerów ani kryteriów służących jako „wskaźniki zagrożenia”. Wreszcie, organizacja ta jest zdania, że ustawa PNR wykracza poza granice tego, co absolutnie konieczne, ponieważ realizuje cele przetwarzania danych PNR szersze niż przewidziane w dyrektywie PNR, a pięcioletni okres przechowywania danych PNR jest nieproporcjonalny. W zarzucie drugim, podniesionym

posiłkowo i dotyczącym naruszenia art. 22 konstytucji belgijskiej w związku z art. 3 ust. 2 TUE i art. 45 karty, LDH odnosi się do przepisów rozdziału 11 ustawy PNR, które dokonują transpozycji dyrektywy API.

34. Rada ministrów Królestwa Belgii, jako interwenient przed Cour constitutionnelle (trybunałem konstytucyjnym), sprzeciwia się skardze LDH, kwestionując zarówno dopuszczalność, jak i zasadność obu zarzutów podniesionych na jej poparcie.

35. Cour constitutionnelle (trybunał konstytucyjny) przedstawia natomiast następujące uwagi.

36. W odniesieniu do zarzutu pierwszego sąd odsyłający zastanawia się przede wszystkim nad tym, czy definicja danych PNR zapisana w załączniku I jest wystarczająco jasna i precyzyjna. Opis niektórych z tych danych ma jego zdaniem charakter przykładowy, a nie wyczerpujący. Następnie sąd ów zauważa, że definicja pojęcia „pasażera” zawarta w art. 3 pkt 4 dyrektywy PNR skutkuje gromadzeniem, przekazywaniem, przetwarzaniem i przechowywaniem danych PNR każdej osoby przewiezionej lub która ma być przewieziona i została wpisana na listę pasażerów, niezależnie od tego, czy istnieją poważne powody ku temu, by sądzić, że osoba, której dane dotyczą, popełniła przestępstwo, zamierza popełnić przestępstwo czy też została skazana za przestępstwo. W odniesieniu do przetwarzania danych PNR wskazuje on, że dane te są w sposób systematyczny poddawane wstępnej ocenie obejmującej wzajemne porównanie danych PNR wszystkich pasażerów z bankami danych lub z wcześniej ustalonymi kryteriami, w celu znalezienia skojarzeń. Niemniej jednak Cour constitutionnelle (trybunał konstytucyjny) wyjaśnia, że chociaż kryteria te powinny być szczegółowe, wiarygodne i niedyskryminacyjne, to bardziej szczegółowe zdefiniowanie wcześniej ustalonych kryteriów, służących określeniu profili ryzyka, wydaje mu się technicznie niemożliwe. W odniesieniu do przewidzianego w art. 12 ust. 1 dyrektywy PNR okresu przechowywania danych PNR, zgodnie z którym dane te mogą być zatrzymywane przez okres pięciu lat, sąd odsyłający uważa, że dane pasażerów podlegają przechowaniu bez względu na to, czy w ramach oceny wstępnej stwierdzono, że odnośni pasażerowie mogą stanowić zagrożenie dla bezpieczeństwa publicznego, czy też nie. W tych okolicznościach sąd odsyłający zastanawia się nad kwestią tego, czy w świetle orzecznictwa wynikającego w szczególności z wyroku z dnia 21 grudnia 2016 r., *Tele2 Sverige i Watson i in.*¹⁵, oraz opinii 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r.¹⁶, można uznać, że ustanowiony w dyrektywie PNR system gromadzenia, przekazywania, przetwarzania i przechowywania danych PNR nie wykracza poza granice tego, co absolutnie konieczne. W tym kontekście sąd ów zastanawia się również nad kwestią tego, czy dyrektywa PNR stoi na przeszkodzie uregulowaniu krajowemu, takiemu jak wynikające z art. 8 ust. 1 pkt 4 ustawy PNR, które zezwala na przetwarzanie danych PNR w celu innym niż cele przewidziane w dyrektywie PNR. Wreszcie sąd ten pochyła się nad zagadnieniem, czy można uznać JIP za „inny organ krajowy”, który na podstawie art. 12 ust. 3 lit. b) ppkt (ii) dyrektywy PNR mógłby udzielić zgody na ujawnienie pełnych danych PNR po upływie sześciu miesięcy. W odniesieniu do drugiego zarzutu sąd odsyłający wskazuje, że jest on skierowany przeciwko art. 3 ust. 1, art. 8 ust. 2 oraz art. 28–31 ustawy PNR, regulującym gromadzenie i przetwarzanie danych pasażerów w celu zwalczania nielegalnej imigracji i ulepszenia kontroli granicznych. Przypomniawszy, że zgodnie z pierwszym z tych przepisów rzeczona ustawa obejmuje loty kończące się na terytorium kraju, rozpoczynające się na nim oraz obejmujące tranzyt przez to terytorium, sąd ten uściśla, że ustawodawca krajowy włączył do zakresu stosowania tej ustawy loty „wewnętrzne”, aby uzyskać „bardziej kompleksowy obraz

¹⁵ C-203/15 i C-698/15, zwanego dalej „wyrokiem *Tele2 Sverige*”, EU:C:2016:970.

¹⁶ Zwanej dalej „opinią 1/15”, EU:C:2017:592.

przejazdów pasażerów stanowiących potencjalne zagrożenie dla bezpieczeństwa [na poziomie Unii] i krajowego”, opierając się na możliwości przewidzianej w art. 2 dyrektywy PNR w związku z jej motywem 10.

37. W tym kontekście Cour constitutionnelle (trybunał konstytucyjny) zawiesił postępowanie i zwrócił się do Trybunału z następującymi pytaniami prejudycjalnymi:

- „1) Czy art. 23 [RODO] w związku z art. 2 ust. 2 lit. d) tego rozporządzenia należy interpretować w ten sposób, że ma on zastosowanie do przepisów krajowych takich jak ustawa [PNR], która dokonuje transpozycji dyrektywy [PNR], dyrektywy [API] oraz dyrektywy 2010/65?
- 2) Czy w zakresie, w jakim wymienione w załączniku I [...] dane są bardzo obszerne – w szczególności dane, o których mowa w pkt 18 załącznika I do dyrektywy [PNR], które wykraczają poza dane określone w art. 3 ust. 2 dyrektywy [API] – oraz w zakresie, w jakim mogą one, rozpatrywane łącznie, ujawniać dane szczególnie chronione, a tym samym naruszać granice tego, co »absolutnie konieczne«, załącznik ten jest zgodny z art. 7, 8 i art. 52 ust. 1 [karty]?
- 3) Czy w zakresie, w jakim ze względu na wyrażenia »w szczególności« i »w tym«, zawarte w pkt 12 i 18 załącznika I [...], dane, o których w nich mowa, zostały wymienione tytułem przykładu, a nie w sposób wyczerpujący, w związku z czym nie jest spełniony wymóg precyzyjności i jasności przepisów pociągających za sobą ingerencję w prawo do poszanowania życia prywatnego oraz w prawo do ochrony danych osobowych, wspomniane punkty tego załącznika są zgodne z art. 7, 8 i art. 52 ust. 1 [karty]?
- 4) Czy w zakresie, w jakim ustanowiony w art. 3 pkt 4 dyrektywy [PNR] i załączniku I [...] system uogólnionego zbierania, przekazywania i przetwarzania danych pasażerów dotyczy każdej osoby, która wykorzystuje dany środek transportu, niezależnie od jakiegokolwiek obiektywnego czynnika pozwalającego na uznanie, że osoba ta może stanowić zagrożenie dla bezpieczeństwa publicznego, przepisy te są zgodne z art. 7, 8 i art. 52 ust. 1 [karty]?
- 5) Czy art. 6 dyrektywy [PNR] w związku z art. 7, 8 i art. 52 ust. 1 [karty] należy interpretować w ten sposób, że stoi on na przeszkodzie ustawodawstwu krajowemu takiemu jak zaskarżona ustawa, która dopuszcza, jako cel przetwarzania danych PNR, monitorowanie działalności wywiadowczej [monitorowanie działalności będącej przedmiotem zainteresowania] służb wywiadowczych i bezpieczeństwa, a tym samym uwzględnia ten cel w ramach celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania?
- 6) Czy art. 6 dyrektywy [PNR] jest zgodny z art. 7, 8 i art. 52 ust. 1 [karty] w zakresie, w jakim wstępna ocena danych pasażerów, którą on reguluje, poprzez korelację z bazami danych i określonymi wcześniej kryteriami, jest stosowana w sposób systematyczny i uogólniony, niezależnie od jakiegokolwiek obiektywnego czynnika pozwalającego na uznanie, że pasażerowie ci mogą stanowić zagrożenie dla bezpieczeństwa publicznego?
- 7) Czy pojęcie »innego właściwego organu krajowego«, o którym mowa w art. 12 ust. 3 dyrektywy [PNR], można interpretować w ten sposób, że dotyczy ono JIP utworzonej przez ustawę [PNR], która może zatem zezwolić na dostęp do danych »PNR« po upływie sześciomiesięcznego terminu w ramach wyszukiwań ad hoc?

- 8) Czy art. 12 dyrektywy [PNR] w związku z art. 7, 8 i art. 52 ust. 1 [karty] należy interpretować w ten sposób, że stoi on na przeszkodzie ustawodawstwu krajowemu takiemu jak 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 [API] jest zgodna z art. 3 ust. 2 [TUE] i art. 45 [karty] w zakresie, w jakim ustanowione w niej obowiązki mają zastosowanie do lotów wewnątrz [Unii]?
- b) Czy dyrektywę [API] w związku z art. 3 ust. 2 [TUE] i art. 45 [karty] należy interpretować w ten sposób, że stoi ona na przeszkodzie ustawodawstwu krajowemu takiemu jak zaskarżona ustawa, która w celu zwalczania nielegalnej imigracji i ulepszenia kontroli granicznych zezwala na system gromadzenia i przetwarzania danych pasażerów »udających się do, przybywających z i przejeżdżających przez terytorium kraju«, co może powodować w sposób pośredni przywrócenie kontroli na granicach wewnętrznych?
- 10) Jeżeli na podstawie odpowiedzi udzielonych na poprzednie pytania prejudycjalne Cour constitutionnelle [trybunał konstytucyjny] miałby dojść do wniosku, że zaskarżona ustawa, transponująca w szczególności dyrektywę [PNR], narusza jeden lub więcej obowiązków wynikających z przepisów wskazanych w tych pytaniach, to czy mogłyby on tymczasowo utrzymać w mocy skutki ustawy [PNR], aby uniknąć niepewności prawa i zapewnić możliwość dalszego wykorzystywania uprzednio zgromadzonych i przechowywanych danych do celów określonych w ustawie?”.

38. Uwagi na piśmie na podstawie art. 23 statutu Trybunału Sprawiedliwości Unii Europejskiej złożyły LDH, rządy belgijski, czeski, duński, niemiecki, estoński, hiszpański, francuski, irlandzki, cypryjski, łotewski, niderlandzki, austriacki, polski, fiński oraz Parlament Europejski, Rada Unii Europejskiej i Komisja Europejska. Zgodnie z art. 24 statutu Trybunału Sprawiedliwości Unii Europejskiej Komisję Europejskiego Inspektora Ochrony Danych (EIOD) i Agencję Praw Podstawowych Unii Europejskiej (FRA) wezwano do udzielenia odpowiedzi na piśmie na pytania zadane przez Trybunał. Rozprawa odbyła się w dniu 13 lipca 2021 r.

III. Analiza

A. W przedmiocie pierwszego pytania prejudycjalnego

39. W pierwszym pytaniu prejudycjalnym sąd odsyłający zwraca się w istocie do Trybunału o wyjaśnienie, czy art. 2 ust. 2 lit. d) RODO należy interpretować w ten sposób, że rozporządzenie to, a w szczególności jego art. 23 ust. 1, zgodnie z którym prawo Unii lub prawo państwa członkowskiego może aktem prawnym, z powodów wymienionych wyczerpująco, ograniczyć zakres obowiązków i praw przewidzianych w tym rozporządzeniu, ma zastosowanie do przetwarzania danych na podstawie ustawodawstwa krajowego, takiego jak ustawa PNR, transponującego do prawa krajowego dyrektywę PNR, a także dyrektywę API i dyrektywę 2010/65.

40. Artykuł 2 ust. 2 RODO przewiduje wyjątki od zakresu stosowania tego rozporządzenia, określonego w sposób bardzo szeroki¹⁷ w jego art. 2 ust. 1¹⁸. Jako odstępstwa od stosowania przepisów regulujących przetwarzanie danych osobowych mogące naruszyć podstawowe wolności wyjątki te należy interpretować w sposób ścisły¹⁹.

41. Artykuł 2 ust. 2 lit. d) RODO zawiera między innymi klauzulę wykluczającą, zgodnie z którą rozporządzenie to nie ma zastosowania do przetwarzania danych osobowych dokonywanego „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”. Rzeczona klauzula wykluczająca opiera się na podwójnym kryterium subiektywnym i obiektywnym. Z zakresu stosowania tego rozporządzenia wyłączone jest zatem przetwarzanie danych dokonywane, po pierwsze, przez „właściwe organy”, a po drugie, do celów wymienionych w tym przepisie. Zatem różne rodzaje przetwarzania danych objęte ustawą PNR należy ocenić w świetle tego podwójnego kryterium.

42. Co się tyczy w pierwszej kolejności przetwarzania danych przez przewoźników (lotniczych, kolejowych, lądowych i morskich) na rzecz JIP lub przez operatorów turystycznych *w celu świadczenia usług lub działalności gospodarczej*, o ile jest ono objęte tą ustawą, o tyle nadal podlega RODO, ponieważ ani element subiektywny, ani element obiektywny kryterium wykluczenia zapisanego w art. 2 ust. 2 lit. d) tego rozporządzenia nie jest spełniony.

43. Co się tyczy w drugiej kolejności *przekazywania przez przewoźników lub operatorów turystycznych danych PNR do JIP*, które samo w sobie stanowi „przetwarzanie” w rozumieniu art. 4 pkt 2 RODO²⁰, jego przynależność do zakresu stosowania tego rozporządzenia jest mniej oczywista.

44. Po pierwsze bowiem, przekazania tego nie dokonuje „właściwy organ” w rozumieniu art. 3 pkt 7 dyrektywy policyjnej, do której należy się odnieść przez analogię wobec braku definicji tego pojęcia w RODO²¹. Jednostki gospodarczej, takiej jak przewoźnik lub biuro podróży, na której

¹⁷ Zobacz podobnie wyrok z dnia 22 czerwca 2021 r., Latvijas Republikas Saeima (Punkty karne) (C-439/19, EU:C:2021:504, pkt 61).

¹⁸ Zgodnie z art. 2 ust. 1 RODO „[n]iniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych”.

¹⁹ Zobacz wyrok z dnia 16 lipca 2020 r., Facebook Ireland i Schrems (C-311/18, EU:C:2020:559, pkt 84); a także wyrok z dnia 22 czerwca 2021 r., Latvijas Republikas Saeima (Punkty karne) (C-439/19, EU:C:2021:504, pkt 62).

²⁰ Zobacz podobnie wyrok z dnia 6 października 2020 r., Privacy International (C-623/17, zwany dalej „wyrokiem Privacy International”, EU:C:2020:790, pkt 41 i przytoczone tam orzecznictwo). Zgodnie z art. 4 pkt 2 RODO „przetwarzanie” oznacza „operację [...] wykonywan[ą] na danych osobowych lub zestawach danych osobowych [...] taką jak [...] ujawnianie poprzez przesłanie [...]”.

²¹ Zobacz podobnie wyrok z dnia 22 czerwca 2021 r., Latvijas Republikas Saeima (Punkty karne) (C-439/19, EU:C:2021:504, pkt 69). Zgodnie z art. 3 pkt 7 lit. a) i b) dyrektywy policyjnej „właściwy organ” to „a) organ publiczny właściwy do zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom; b) inny organ lub podmiot, któremu prawo państwa członkowskiego powierza sprawowanie władzy publicznej i wykonywanie uprawnień publicznych” do tych samych celów.

cięży wyłącznie prawny obowiązek przekazywania danych osobowych i której nie powierzono żadnych uprawnień publicznych²², nie można uznać za organ lub podmiot w rozumieniu lit. b) rzeczonego art. 3 pkt 7²³.

45. Po drugie, przekazywanie danych PNR przez przewoźników i operatorów turystycznych odbywa się w wykonaniu obowiązku nałożonego ustawą, aby umożliwić realizację celów wymienionych w art. 2 ust. 2 lit. d) RODO.

46. Jednakże moim zdaniem z brzmienia tego przepisu jasno wynika, że poza zakresem stosowania RODO znajdują się jedynie te operacje przetwarzania, które odpowiadają zarówno elementowi subiektywnemu, jak i elementowi obiektywnemu ustanowionego w nim kryterium wykluczenia. Przekazywanie danych PNR do JIP, wymagane zgodnie z ustawą PNR od przewoźników lotniczych i operatorów turystycznych, jest zatem objęte zakresem tego rozporządzenia.

47. Jeżeli chodzi o przepisy ustawy PNR transponującej dyrektywę PNR, wniosek ten znajduje potwierdzenie w art. 21 ust. 2 tej dyrektywy, który przewiduje, że rzeczona dyrektywa „nie ma wpływu na możliwość stosowania dyrektywy 95/46/WE²⁴ do przetwarzania danych osobowych przez przewoźników lotniczych”. Moim zdaniem wykładnię tego przepisu, proponowaną między innymi przez rząd francuski, zgodnie z którą przepis ów przewiduje jedynie, że przewoźnicy nadal podlegają obowiązkom ustanowionym w RODO w zakresie operacji przetwarzania danych, które nie są przewidziane w dyrektywie PNR, należy oddalić. Należy bowiem wskazać, mając na uwadze brzmienie tej „klauzuli braku wpływu”, że jej zakres jest szeroki, przy czym zdefiniowano go wyłącznie poprzez odniesienie do podmiotu przetwarzającego dane, nie ma zaś żadnej wzmianki ani o celu przetwarzania, ani o kontekście, w jakim ma ono miejsce – czy to w ramach działalności gospodarczej przewoźnika lotniczego, czy w wykonaniu obowiązku prawnego. Pragnę ponadto zauważyć, że klauzulę o takiej samej treści zawarto w art. 13 ust. 3 dyrektywy PNR, który odnosi się w szczególności do spoczywających na przewoźnikach lotniczych na podstawie RODO obowiązków „podjęcia odpowiednich środków technicznych i organizacyjnych w celu ochrony bezpieczeństwa i poufności danych osobowych”. Przepis ten należy do unormowań regulujących ochronę danych osobowych przetwarzanych na podstawie dyrektywy PNR, a poprzedza go art. 13 ust. 1 tej dyrektywy, który w sposób ogólny poddaje przetwarzanie danych na podstawie tejże dyrektywy wymienionym w nim przepisom decyzji ramowej 2008/977. Wbrew temu, co twierdzi rząd francuski, taki układ normatywny pozwala, po pierwsze, na odczytanie ust. 3 rzeczonego art. 13 jako klauzuli przywracającej pod rządą RODO jedynie te operacje przetwarzania danych przewidziane w dyrektywie PNR, które nie są dokonywane przez „właściwe organy” w rozumieniu dyrektywy policyjnej, a po drugie, na interpretowanie

²² Postanowienie odsyłające nie daje w tym względzie żadnych wskazówek.

²³ Takiej jednostki nie można również uznać za „podmiot przetwarzający” w rozumieniu art. 4 pkt 8 RODO lub art. 3 pkt 9 dyrektywy policyjnej, lecz należy ją raczej uznać za „administratora” w rozumieniu art. 4 pkt 7 zdanie drugie RODO. Zgodnie z art. 4 pkt 8 RODO i art. 3 pkt 9 dyrektywy policyjnej, które są sformułowane w identyczny sposób, „podmiot przetwarzający” oznacza „osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, który przetwarza dane osobowe w imieniu administratora”. W rozumieniu art. 4 pkt 7 zdanie pierwsze RODO „administrator” oznacza „osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który [...] ustala cele i sposoby przetwarzania [...]”, przy czym zdanie drugie tego przepisu uściśla, że „jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania”.

²⁴ Dyrektywa Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. 1995, L 281, s. 31). Dyrektywa ta została uchylona i zastąpiona przez RODO, zob. art. 94 tego rozporządzenia.

odniesienia do przestrzegania obowiązków nałożonych przez to rozporządzenie w zakresie bezpieczeństwa i poufności danych jako przypomnienia gwarancji, którym musi obowiązkowo podlegać przekazywanie przez przewoźników do JIP danych PNR.

48. Wniosku przedstawionego w pkt 46 niniejszej opinii nie podważają motyw 19 RODO ani motyw 11 dyrektywy policyjnej, do którego odnoszą się między innymi rządy niemiecki, francuski i irlandzki na poparcie tezy, że dyrektywa PNR ma charakter *lex specialis*. W tym względzie prawdą jest, że w odniesieniu do przetwarzania danych osobowych, którego dotyczy, dyrektywa ta ustanawia ramy ochrony tych danych niezależne od RODO. Jednakże te szczególne ramy mają zastosowanie wyłącznie do przetwarzania danych PNR przez „właściwe organy” w rozumieniu art. 3 pkt 7 dyrektywy policyjnej, do których należą w szczególności JIP, podczas gdy przekazywanie danych PNR do JIP podlega ogólnym zasadom ustanowionym przez RODO na podstawie między innymi „klauzuli braku wpływu” przewidzianej w art. 21 ust. 2 dyrektywy PNR.

49. Na poparcie swojej tezy, zgodnie z którą RODO nie ma zastosowania do przekazywania danych PNR do JIP przez przewoźników i operatorów turystycznych, rządy belgijski, francuski, irlandzki i cypryjski odwołują się do wyroku z dnia 30 maja 2006 r., Parlament/Rada i Komisja²⁵, w którym Trybunał orzekł, że przekazywanie danych PNR przez wspólnotowych przewoźników lotniczym organom Stanów Zjednoczonych Ameryki w ramach umowy negocjowanej między tym państwem a Wspólnotą Europejską stanowiło przetwarzanie danych osobowych w rozumieniu art. 3 ust. 2 tiret pierwsze dyrektywy 95/46²⁶ i, co za tym idzie, nie było objęte zakresem stosowania tej dyrektywy. Dochodząc do takiego wniosku, Trybunał uwzględnił *cel przekazania* danych oraz fakt, że przetwarzanie to „następuje w ramach ustanowionych przez władze publiczne”, mimo że dane gromadziły i przekazywały podmioty prywatne²⁷.

50. W tym względzie wystarczy zauważyć, że w wyroku z dnia 6 października 2020 r., La Quadrature du Net i in.²⁸, Trybunał zasadniczo uznał wyrok Parlament/Rada za nienadający się do przeniesienia na grunt RODO²⁹.

51. Ponadto w pkt 102 wyroku La Quadrature du Net³⁰ Trybunał zastosował w drodze analogii rozumowanie przeprowadzone w wyrokach Tele2 Sverige i z dnia 2 października 2018 r., Ministerio Fiscal³¹, i stwierdził, że „jakkolwiek w art. 2 ust. 2 lit. d) [RODO] sprecyzowano, że nie ma ono zastosowania do przetwarzania »przez właściwe organy« do celów w szczególności wykrywania i ścigania czynów zabronionych, w tym ochrony przed zagrożeniami dla

²⁵ C-317/04 i C-318/04, zwany dalej „wyrokiem Parlament/Rada”, EU:C:2006:346. W sprawach, w których wydano ten wyrok, Parlament wniósł, po pierwsze, o stwierdzenie nieważności decyzji Rady 2004/496/WE z dnia 17 maja 2004 r. w sprawie zawarcia Porozumienia pomiędzy Wspólnotą Europejską a Stanami Zjednoczonymi Ameryki w sprawie przetwarzania i przekazywania danych dot. nazwy rekordu pasażera (PNR) przez przewoźników lotniczych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych, Biura Cel i Ochrony Granic (Dz.U. 2004, L 183, s. 83; sprostowanie Dz.U. 2005, L 255, s. 168), a po drugie, stwierdzenie nieważności decyzji Komisji 2004/535/WE z dnia 14 maja 2004 r. w sprawie odpowiedniej ochrony danych osobowych zawartych w Passenger Name Record (PNR) pasażerów lotniczych przekazywanych do Biura Celnego i Ochrony Granic Stanów Zjednoczonych (Dz.U. 2004, L 235, s. 11).

²⁶ Artykuł 3 ust. 2 tiret pierwsze dyrektywy 95/46 stanowi, że dyrektywa ta nie ma zastosowania do przetwarzania danych osobowych „w ramach działalności wykraczającej poza zakres prawa Wspólnoty, jak np. dane, o których stanowi tytuł V i VI Traktatu o Unii Europejskiej, a w *żadnym razie* do działalności na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (łącznie z dobrą kondycją gospodarczą państwa, gdy działalność ta dotyczy spraw związanych z bezpieczeństwem państwa) oraz działalności państwa w obszarach prawa karnego” (wyróżnienie własne).

²⁷ W przedmiocie „podejścia celowościowego” i „kontekstowego” Trybunału w wyroku Parlament/Rada zob. opinia rzecznika generalnego M. Camposa Sánchez-Bordony w sprawach połączonych La Quadrature du Net i in. (C-511/18 i C-512/18, EU:C:2020:6, pkt 47, 62).

²⁸ C-511/18, C-512/18 i C-520/18, zwany dalej „wyrokiem La Quadrature du Net”, EU:C:2020:791.

²⁹ Zobacz wyrok La Quadrature du Net, pkt 100–102.

³⁰ Zobacz podobnie wyrok Privacy International pkt 47.

³¹ C-207/16, zwany dalej „wyrokiem Ministerio Fiscal”, EU:C:2018:788, pkt 34.

bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, to jednak z art. 23 ust. 1 lit. d) i h) tego rozporządzenia wynika, że przetwarzanie danych osobowych w tych samych celach przez osoby prywatne jest objęte zakresem stosowania tego rozporządzenia”³².

52. Z przedstawionych wyżej powodów jestem przekonany, że wniosek, zgodnie z którym przekazywanie danych PNR przez przewoźników i operatorów turystycznych do JIP jest objęte RODO, wynika jasno już z brzmienia art. 2 ust. 2 lit. d) RODO, który odnosi się jedynie do przetwarzania przez „właściwe organy”, i nie ma potrzeby odwoływania się do klauzuli ograniczającej zawartej w art. 23 ust. 1 wspomnianego rozporządzenia³³. Niezależnie od tego jasne stanowisko Trybunału na rzecz takiego wniosku znaleźć można w stwierdzeniu zawartym w pkt 102 wyroku *La Quadrature du Net*.

53. Ponieważ przekazywanie danych PNR przez przewoźników i operatorów turystycznych wchodzi w zakres stosowania RODO, ustawodawstwo krajowe, takie jak ustawa PNR, które zobowiązuje rzeczne podmioty do przekazywania tych danych, stanowi „akt prawny” w rozumieniu art. 23 pkt 1 lit. d) RODO i w związku z tym musi spełniać warunki przewidziane w tym przepisie³⁴.

54. Co się tyczy w trzeciej kolejności przetwarzania danych PNR *przez JIP i właściwe organy krajowe*, stosowanie RODO, jak wynika z powyższych rozważań, zależy od tego, jakie cele są w ten sposób realizowane.

55. I tak, po pierwsze, przetwarzanie danych PNR przez JIP i przez właściwe organy krajowe do celów wymienionych w art. 8 § 1 pkt 1–3 i 5 ustawy PNR³⁵ jest wyłączone z zakresu stosowania RODO, ponieważ wspomniane cele, jak się wydaje, należą do celów objętych klauzulą wykluczającą zawartą w art. 2 ust. 2 lit. d) RODO. Ochrona danych osób, których przetwarzanie dotyczy, jest objęta zakresem prawa krajowego, z zastrzeżeniem stosowania dyrektywy policyjnej³⁶, a w ramach jej zakresu stosowania – dyrektywy PNR.

56. Po drugie, podobnie jest w przypadku przetwarzania danych PNR przez JIP oraz przez służby bezpieczeństwa i wywiadowcze w ramach monitorowania działań, o których mowa w przepisach ustawy organicznej o służbach wywiadowczych i bezpieczeństwa, wymienionych w art. 8 § 1 pkt 4 ustawy PNR, na tyle, na ile odpowiadają one celom określonym w art. 2 ust. 2 lit. d) RODO, czego ocena należy do sądu odsyłającego.

57. Rząd belgijski utrzymuje, że przetwarzanie przeprowadzane na podstawie art. 8 § 1 pkt 4 ustawy PNR jest w każdym wypadku objęte klauzulą wykluczającą zapisaną w art. 2 ust. 2 lit. a) RODO, a także klauzulą przewidzianą w art. 2 ust. 3 lit. a) dyrektywy policyjnej, ponieważ działalność służb bezpieczeństwa i wywiadowczych nie wchodzi w zakres stosowania prawa Unii.

³² Zobacz analogicznie wyroki *Tele2 Sverige*, pkt 72–74, i *Ministerio fiscal*, pkt 34. Wyroki te dotyczyły wykładni art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. 2002, L 201, s. 37), który przewiduje klauzulę ograniczającą analogiczną do klauzuli zawartej w art. 23 ust. 1 lit. a)–d) RODO.

³³ Odniesienie do art. 15 ust. 1 dyrektywy 2002/58 było uzasadnione w kontekście tej dyrektywy brzmieniem klauzuli wykluczającej przewidzianej w jej art. 1 ust. 3, która odnosi się w sposób ogólny do „działalności państwa w dziedzinie prawa karnego”.

³⁴ Zobacz analogicznie wyrok *Privacy International*, pkt 38, 39.

³⁵ Chodzi o przetwarzanie regulowane rozdziałami 7–10 i 12 ustawy PNR.

³⁶ Zobacz podobnie wyroki: *La Quadrature du Net*, pkt 103; *Privacy International*, pkt 48.

58. W tym względzie – podkreślając jednocześnie, że do Trybunału nie zwrócono się z pytaniem dotyczącym wykładni tych przepisów – pragnę zauważyć przede wszystkim, iż Trybunał stwierdził już, że przepisy krajowe nakładające obowiązki przetwarzania na podmioty prywatne podlegają przepisom prawa Unii w dziedzinie ochrony danych osobowych, nawet jeśli dotyczą one ochrony bezpieczeństwa narodowego³⁷. Stąd wniosek, że przekazywanie danych PNR wymagane przez ustawę PNR od przewoźników i operatorów turystycznych podlega co do zasady RODO, nawet jeśli odbywa się do celów art. 8 § 1 pkt 4 tej ustawy.

59. Następnie pragnę zauważyć, że o ile motyw 16 RODO stanowi, iż akt ten nie ma zastosowania do „działalności dotyczącej bezpieczeństwa narodowego”, a motyw 14 dyrektywy policyjnej uściśla, że „czynności w zakresie bezpieczeństwa narodowego, czynności agencji lub jednostek zajmujących się bezpieczeństwem narodowym [...] nie należy uznawać za czynności wchodzące w zakres [tej] dyrektywy”, o tyle kryteria decydujące o tym, że przetwarzanie danych osobowych przez organ, jednostkę lub agencję publiczną państwa członkowskiego albo należy do zakresu stosowania jednego lub drugiego aktu prawa Unii organizującego ochronę osób w odniesieniu do przetwarzania ich danych, albo sytuuje się poza zakresem stosowania tego prawa, oparte są na koncepcji odnoszącej się zarówno do zadań wyznaczonych danemu organowi, jednostce lub agencji, jak i do celów rzeczowego przetwarzania. I tak, Trybunał orzekł, że art. 2 ust. 2 lit. a) RODO w związku z motywem 16 tego rozporządzenia „należy uznać za mający na celu jedynie wyłączenie z zakresu stosowania tego rozporządzenia przetwarzania danych osobowych dokonywanego przez organy państwowe w ramach działalności mającej na celu ochronę bezpieczeństwa narodowego lub działalności, która może zostać zaliczona do tej samej kategorii, wobec czego sam fakt, iż dana działalność jest właściwa państwu lub organowi publicznemu, nie wystarcza, aby wyjątek ten mógł być automatycznie stosowany do takiej działalności”³⁸. Trybunał wyjaśnił również, że „działalność, której celem jest ochrona bezpieczeństwa narodowego, a o której mowa w art. 2 ust. 2 lit. a) RODO, obejmuje w szczególności [...] działalność mającą na celu ochronę podstawowych funkcji państwa i podstawowych interesów społeczeństwa”³⁹. Wynika z tego, że w przypadku gdy państwo członkowskie powierza swoim służbom bezpieczeństwa i wywiadowczym zadania w dziedzinach wymienionych w art. 3 pkt 7 lit. a) dyrektywy policyjnej, przetwarzanie danych przez te służby w celu wykonywania tych zadań wchodzi w zakres stosowania tej dyrektywy, a także, w odpowiednim przypadku, dyrektywy PNR. Mówiąc bardziej ogólnie, pragnę zauważyć, że Trybunał wielokrotnie orzekał w ramach wykładni art. 4 ust. 2 TUE, który za podstawę swojej argumentacji przyjmuje między innymi rząd belgijski, że sam fakt, iż środek krajowy został przyjęty w celu ochrony bezpieczeństwa narodowego, nie może prowadzić do niemożności stosowania prawa Unii i zwalniać państw członkowskich z konieczności przestrzegania tego prawa⁴⁰, wykazując w ten sposób niechęć do automatycznego wyłączenia en bloc z zakresu stosowania prawa Unii działalności państw członkowskich związanej z ochroną bezpieczeństwa narodowego.

60. Po trzecie, zgodnie z opinią wszystkich zainteresowanych stron, które przedstawiły uwagi, z wyjątkiem rządu francuskiego, należy uznać, że przetwarzanie danych PNR przez właściwe organy belgijskie do celów określonych w art. 8 § 2 ustawy PNR, a mianowicie „ulepszenia kontroli osób na granicach zewnętrznych oraz [zwalczania] nielegalnej imigracji”⁴¹, nie jest objęte klauzulą wykluczającą zawartą w art. 2 ust. 2 lit. d) RODO ani inną klauzulą wykluczającą przewidzianą w tym artykule, a zatem należy do zakresu stosowania tego rozporządzenia.

³⁷ Zobacz w szczególności wyrok La Quadrature du Net.

³⁸ Zobacz wyrok z dnia 22 czerwca 2021 r., Latvijas Republikas Saeima (Punkty karne) (C-439/19, EU:C:2021:504, pkt 66).

³⁹ Zobacz wyrok z dnia 22 czerwca 2021 r., Latvijas Republikas Saeima (Punkty karne) (C-439/19, EU:C:2021:504).

⁴⁰ Zobacz wyrok La Quadrature du Net, pkt 99 i przytoczone tam orzecznictwo.

⁴¹ Warunki związane z takim przetwarzaniem danych określono w rozdziale 11 ustawy PNR.

W przeciwieństwie do tego, co twierdzi rząd francuski, rzeczonych operacji przetwarzania nie może regulować dyrektywa PNR, której art. 1 ust. 2 stanowi, że „[d]ane PNR zebrane zgodnie z niniejszą dyrektywą mogą być przetwarzane wyłącznie w celach zapobiegania przestępstwom terrorystycznym i poważnej przestępczości oraz ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania”, ani też zasadniczo dyrektywa policyjna, która zgodnie z jej art. 1 ust. 1 ma zastosowanie jedynie do operacji przetwarzania danych osobowych 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”. Jak wynika z postanowienia odsyłającego, art. 8 § 2 ustawy PNR i rozdział 11 tej ustawy – który zawiera przepisy regulujące przetwarzanie danych PNR w celu ulepszenia kontroli granicznych oraz zwalczania nielegalnej imigracji i przewiduje w tym celu przekazywanie tych danych przez JIP między innymi służbom policyjnym odpowiedzialnym za kontrolę granic – mają na celu transpozycję do prawa belgijskiego dyrektywy API i dyrektywy 2010/65. Te dwie dyrektywy zaś w zakresie przewidzianego w nich przetwarzania nakładają na właściwe organy obowiązek przestrzegania przepisów dyrektywy 95/46⁴². Wbrew temu, co twierdzi rząd francuski, odesłanie do przepisów ochronnych tej dyrektywy należy rozumieć w ten sposób, że obejmuje ono każdą operację przetwarzania danych osobowych na podstawie dyrektywy API i dyrektywy 2010/65. Okoliczność, że dyrektywa API weszła w życie przed decyzją ramową 2008/977, nie ma w tym względzie znaczenia, ponieważ ta decyzja ramowa, jak również zastępująca ją dyrektywa policyjna dotyczą jedynie operacji przetwarzania danych osobowych, o których mowa w art. 3 ust. 1 dyrektywy API, przez właściwe organy w celu zwalczania przestępczości⁴³.

61. Na podstawie całości powyższych rozważań proponuję, aby na pierwsze pytanie prejudycjalne Trybunał odpowiedział, że art. 23 RODO w związku z art. 2 ust. 2 lit. d) tego rozporządzenia należy interpretować w ten sposób, że:

- ma on zastosowanie do przepisów krajowych dokonujących transpozycji dyrektywy PNR w zakresie, w jakim przepisy te regulują przetwarzanie danych PNR przez przewoźników i przez inne podmioty gospodarcze, w tym przekazywanie danych PNR do JIP, przewidziane w art. 8 tej dyrektywy;
- nie ma on zastosowania do przepisów krajowych dokonujących transpozycji dyrektywy PNR w zakresie, w jakim regulują one przetwarzanie danych do celów określonych w art. 1 ust. 2 tej dyrektywy przez właściwe organy krajowe, włączając w to JIP, oraz w odpowiednich przypadkach służby bezpieczeństwa i wywiadowcze zainteresowanego państwa członkowskiego;
- ma on zastosowanie do przepisów krajowych dokonujących transpozycji dyrektywy API i dyrektywy 2010/65 w celu ulepszenia kontroli osób na granicach zewnętrznych oraz w celu zwalczania nielegalnej imigracji.

⁴² Zobacz motywy 8, 9 i 12 oraz art. 6 dyrektywy API, a także art. 8 ust. 2 dyrektywy 2010/65.

⁴³ Wykorzystanie uprzednich informacji o pasażerach (zwanym dalej „danymi API”) przez organy ścigania przewidziano wyraźnie w art. 6 ust. 1 akapit ostatni dyrektywy API.

B. W przedmiocie pytań prejudycjalnych drugiego, trzeciego, czwartego, szóstego i ósmego

62. W pytaniach prejudycjalnych drugim, trzecim, czwartym i szóstym belgijski trybunał konstytucyjny zwraca się do Trybunału w kwestii ważności dyrektywy PNR w świetle art. 7, 8 i art. 52 ust. 1 karty. Ósme pytanie prejudycjalne, choć sformułowane jako pytanie dotyczące wykładni, również w istocie zmierza do uzyskania od Trybunału orzeczenia w przedmiocie ważności tej dyrektywy.

63. Pytania te dotyczą różnych elementów ustanowionego w dyrektywie PNR systemu przetwarzania danych PNR, a w odniesieniu do każdego z tych elementów wymagają oceny przestrzegania warunków, od których zależy zgodność z prawem ograniczeń w wykonywaniu praw podstawowych określonych w art. 7 i 8 karty. Pytania prejudycjalne drugie i trzecie dotyczą katalogu danych PNR zawartego w załączniku I, tematem pytania czwartego jest definicja pojęcia „pasażera” zapisana w art. 3 pkt 4 dyrektywy PNR, pytanie szóste odnosi się do wykorzystywania danych PNR do celów wstępnej oceny na podstawie art. 6 tej dyrektywy, a przedmiotem pytania ósmego jest okres przechowywania danych PNR przewidziany w jej art. 12 ust. 1.

1. W przedmiocie praw podstawowych zapisanych w art. 7 i 8 karty

64. Artykuł 7 karty gwarantuje każdemu prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się. W art. 8 ust. 1 karty wyraźnie zaś przyznano każdemu prawo do ochrony danych osobowych, które go dotyczą. Zgodnie z utrwalonym orzecznictwem prawa te, które odnoszą się do wszelkich informacji dotyczących zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, są ze sobą ściśle powiązane, przy czym dostęp do danych osobowych osoby fizycznej w celu ich zatrzymywania lub wykorzystywania narusza przysługujące tej osobie prawo podstawowe do poszanowania życia prywatnego⁴⁴.

65. Niemniej jednak praw zagwarantowanych w art. 7 i 8 karty nie sposób uznać za stanowiące prerogatywy o charakterze absolutnym, lecz powinny być one oceniane w świetle ich funkcji społecznej⁴⁵. Artykuł 8 ust. 2 karty zezwala tym sposobem na przetwarzanie danych osobowych, jeżeli spełnione są określone warunki. Postanowienie to stanowi, że dane te muszą być przetwarzane „rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą”.

66. Ponadto każde ograniczenie prawa do ochrony danych osobowych oraz prawa do życia prywatnego musi być zgodne z postanowieniami art. 52 ust. 1 karty. Zatem ograniczenie takie musi być przewidziane ustawą i nie może naruszać istoty rzeczonych praw oraz – w zgodzie z zasadą proporcjonalności – musi być konieczne i rzeczywiście odpowiadać celom interesu ogólnego uznanym przez Unię lub wynikać z potrzeby ochrony praw i wolności innych osób.

⁴⁴ Zobacz podobnie w szczególności wyrok z dnia 16 lipca 2020 r., Facebook Ireland i Schrems (C-311/18, EU:C:2020:559, pkt 170 i przytoczone tam orzecznictwo).

⁴⁵ Zobacz w szczególności wyrok z dnia 16 lipca 2020 r., Facebook Ireland i Schrems (C-311/18, EU:C:2020:559, pkt 172 i przytoczone tam orzecznictwo).

67. Ocena środka ograniczającego wspomniane prawa powinna uwzględniać również znaczenie praw ustanowionych w art. 3, 4, 6 i 7 karty oraz znaczenie, jakie mają cele ochrony bezpieczeństwa narodowego i walki z poważną przestępczością, przyczyniające się do ochrony praw i wolności innych osób⁴⁶. W tym względzie art. 6 karty gwarantuje każdemu prawo nie tylko do wolności, ale też do bezpieczeństwa osobistego⁴⁷.

68. Ponadto art. 52 ust. 3 karty ma na celu zapewnienie niezbędnej spójności między prawami zawartymi w karcie a odpowiadającymi im prawami zagwarantowanymi w EKPC, które należy uwzględnić jako próg ochrony minimalnej⁴⁸. Prawo do poszanowania życia prywatnego i rodzinnego, zapisane w art. 7 karty, odpowiada prawu zagwarantowanemu w art. 8 EKPC, a w związku z tym należy nadawać mu takie samo znaczenie i zakres⁴⁹. Z orzecznictwa Europejskiego Trybunału Praw Człowieka (zwanego dalej „ETPC”) wynika, że ingerencja w prawa gwarantowane przez ten artykuł może być uzasadniona w świetle ust. 2 tego artykułu tylko wtedy, gdy jest przewidziana ustawą, dotyczy jednego lub szeregu zgodnych z prawem celów wymienionych w tym ustępie i jest niezbędna w społeczeństwie demokratycznym do osiągnięcia tego celu lub tych celów⁵⁰. Dany środek powinien być również zgodny z zasadą państwa prawnego, wyraźnie wskazaną w preambule EKPC i nierozzerwalnie związaną z przedmiotem i celem jej art. 8⁵¹.

69. To w świetle tych właśnie zasad należy zbadać pytania dotyczące ważności, przedstawione przez Cour constitutionnelle (trybunał konstytucyjny).

2. W przedmiocie ingerencji w prawa podstawowe ustanowione w art. 7 i 8 karty

70. Trybunał orzekł już, że przepisy nakazujące lub dopuszczające przekazanie podmiotowi trzeciemu, takiemu jak organ publiczny, danych osobowych osób fizycznych należy, w braku zgody tych osób fizycznych i niezależnie od późniejszego wykorzystania tych danych, uznać za ingerencję w ich życie prywatne, a zatem za ograniczenie prawa podstawowego zagwarantowanego w art. 7 karty, bez uszczerbku dla możliwości ich ewentualnego uzasadnienia⁵². Jest tak nawet w braku okoliczności pozwalających na zakwalifikowanie takiej ingerencji jako „poważnej”, i nie ma znaczenia, czy informacje związane z życiem prywatnym osób, których dotyczą, mają charakter wrażliwy czy nie lub czy zainteresowane osoby poniosły jakiegokolwiek negatywne konsekwencje z powodu tej ingerencji⁵³. Dostęp organów władzy publicznej do takich informacji stanowi również ingerencję w prawo podstawowe do ochrony

⁴⁶ Zobacz podobnie wyrok La Quadrature du Net, pkt 122.

⁴⁷ Zobacz wyrok La Quadrature du Net, pkt 123.

⁴⁸ Zobacz wyrok La Quadrature du Net, pkt 124 i przytoczone tam orzecznictwo.

⁴⁹ Zobacz wyrok z dnia 18 czerwca 2020 r., Komisja/Węgry (Przejrzystość stowarzyszeń) (C-78/18, EU:C:2020:476, pkt 122 i przytoczone tam orzecznictwo).

⁵⁰ Zobacz w szczególności wyroki ETPC: z dnia 4 grudnia 2015 r. w sprawie Roman Zakharov (CE:ECHR:2015:1204JUD004714306, § 227); z dnia 18 maja 2010 r. w sprawie Kennedy przeciwko Zjednoczonemu Królestwu (CE:ECHR:2010:0518JUD002683905, § 130); z dnia 25 maja 2021 r. w sprawie Centrum för Rättvisa przeciwko Szwecji (CE:ECHR:2021:0525JUD003525208, § 246).

⁵¹ Zobacz wyroki ETPC: z dnia 4 grudnia 2015 r. w sprawie Roman Zakharov przeciwko Rosji (CE:ECHR:2015:1204JUD004714306, § 228); z dnia 4 maja 2000 r. w sprawie Rotaru przeciwko Rumunii (CE:ECHR:2000:0504JUD002834195, § 52); z dnia 4 grudnia 2008 r., S. i Marper przeciwko Zjednoczonemu Królestwu (CE:ECHR:2008:1204JUD003056204, § 95); z dnia 18 maja 2021 r. w sprawie Kennedy przeciwko Zjednoczonemu Królestwu (CE:ECHR:2010:0518JUD002683905, § 151); z dnia 25 maja 2021 r. w sprawie Centrum för Rättvisa przeciwko Szwecji (CE:ECHR:2021:0525JUD003525208, § 246).

⁵² Zobacz między innymi wyrok z dnia 18 czerwca 2020 r., Komisja/Węgry (C-78/18, EU:C:2020:476, pkt 124, 126 i przytoczone tam orzecznictwo); zob. także wyroki ETPC: z dnia 4 maja 2000 r. w sprawie Rotaru przeciwko Rumunii (CE:ECHR:2000:0504JUD00283419, § 48); z dnia 26 marca 1987 r. w sprawie Leander przeciwko Szwecji (CE:ECHR:1987:0326JUD000924881, § 46); z dnia 29 czerwca 2006 r. w sprawie Weber i Saravia przeciwko Niemcom (CE:ECHR:2006:0629DEC005493400, § 79).

⁵³ Zobacz m.in. wyrok Ministerio Fiscal, pkt 51 i przytoczone tam orzecznictwo.

danych osobowych zagwarantowane w art. 8 karty, ponieważ stanowi przetwarzanie danych osobowych⁵⁴. Podobnie, samoistną ingerencją w prawa zagwarantowane w art. 7 i 8 karty jest zatrzymywanie przez określony czas danych związanych z życiem prywatnym danej osoby⁵⁵.

71. Trybunał orzekł już również, że dane PNR, takie jak wymienione w załączniku I, zawierają informacje o zidentyfikowanych osobach fizycznych, mianowicie o pasażerach lotniczych, a zatem różne aspekty przetwarzania, jakiemu dane te mogą zostać poddane, dotyczą prawa podstawowego do poszanowania życia prywatnego, gwarantowanego w art. 7 karty. Te operacje przetwarzania wchodzą również w zakres art. 8 karty i w związku z tym muszą spełniać wynikające z niego wymogi w zakresie ochrony danych⁵⁶.

72. Tym samym przetwarzanie danych PNR, na które pozwala dyrektywa PNR, w tym istotne dla niniejszej sprawy przekazywanie tych danych przez przewoźników lotniczych do JIP, ich wykorzystywanie przez te jednostki, późniejsze przekazywanie danych do właściwych organów krajowych w rozumieniu art. 7 tej dyrektywy, a także ich przechowywanie stanowią ingerencję w prawa podstawowe zagwarantowane w art. 7 i 8 karty.

73. Co się tyczy wagi tych ingerencji, należy zauważyć, po pierwsze, że dyrektywa PNR przewiduje *systematyczne i ciągłe* przekazywanie do JIP danych PNR każdego pasażera lotniczego, zgodnie z definicją zawartą w art. 3 pkt 4 tej dyrektywy, odbywającego podróż lotem „pozaunijnym” w rozumieniu jej art. 3 pkt 2. W efekcie przekazania JIP ma uogólniony dostęp do wszystkich ujawnionych danych PNR⁵⁷. Wbrew temu, co twierdzą niektóre państwa członkowskie w niniejszym postępowaniu, tego stwierdzenia nie podważa okoliczność, że skoro dane te są przetwarzane w sposób zautomatyzowany, JIP mają dostęp jedynie do tych danych, których analiza doprowadziła do pozytywnego wyniku. W istocie bowiem z jednej strony okoliczność taka nie przeszkodziła Trybunałowi orzec, w odniesieniu do podobnych systemów zautomatyzowanego przetwarzania danych osobowych gromadzonych lub przechowywanych „hurtowo”, że dostęp odnośnych organów publicznych do takich danych ma charakter uogólniony. Z drugiej strony samo udostępnienie organom publicznym danych osobowych w celu ich przetwarzania i przechowywania przez te organy obejmuje a priori uogólniony i pełny dostęp owych organów do takich danych oraz ingerencję w prawa podstawowe do poszanowania życia prywatnego i ochrony danych osobowych.

74. Po drugie, zgodnie z art. 2 ust. 1 dyrektywy PNR państwa członkowskie mogą podjąć decyzję o stosowaniu tej dyrektywy do lotów „wewnątrzunijnych” w rozumieniu jej art. 3 pkt 3. W tym względzie pragnę zauważyć z jednej strony, że dyrektywa PNR nie ogranicza się do ustanowienia możliwości rozszerzenia przez państwa członkowskie jej stosowania na loty wewnątrzunijne, lecz określa również warunki zarówno formalne, jak i materialne regulujące korzystanie z tej możliwości⁵⁸, przy czym uściśla, że w przypadku gdy z możliwości tej skorzystano tylko w odniesieniu do wybranych lotów wewnątrzunijnych, wyboru tych lotów należy dokonać z uwzględnieniem celów realizowanych przez tę dyrektywę⁵⁹. Z drugiej strony dyrektywa PNR określa konsekwencje skorzystania z tej możliwości i przewiduje w art. 2 ust. 2, że w przypadku

⁵⁴ Zobacz między innymi wyrok z dnia 18 czerwca 2020 r., Komisja/Węgry (C-78/18, EU:C:2020:476, pkt 126); a także wyrok Ministerio Fiscal, pkt 51 i przytoczone tam orzecznictwo.

⁵⁵ Zobacz wyrok z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in. (C-293/12 i C-594/12, zwany dalej „wyrokiem Digital Rights”, EU:C:2014:238, pkt 34).

⁵⁶ Opinia 1/15, pkt 121–123.

⁵⁷ Zobacz analogicznie wyrok Privacy International, pkt 79, 80 i przytoczone tam orzecznictwo.

⁵⁸ Zobacz art. 2 ust. 1–3 dyrektywy PNR.

⁵⁹ Zobacz art. 2 ust. 3 dyrektywy PNR.

gdy państwo członkowskie postanowi stosować tę dyrektywę do lotów wewnątrzunijnych, wszystkie jej przepisy „stosuje się do lotów wewnątrzunijnych, tak jakby były one lotami pozaunijnymi, oraz do danych PNR dotyczących lotów wewnątrzunijnych, tak jakby były one danymi PNR dotyczącymi lotów pozaunijnych”.

75. W tych okolicznościach jestem zdania, inaczej niż niektóre rządy, które przedstawiły uwagi w niniejszej sprawie, że pomimo iż stosowanie dyrektywy PNR do lotów wewnątrzunijnych zależy od wyboru państw członkowskich, podstawę prawną ingerencji w prawa do poszanowania życia prywatnego i ochrony danych osobowych, związanych z przekazywaniem, przetwarzaniem i przechowywaniem danych PNR dotyczących tych lotów stanowi, w przypadku dokonania takiego wyboru, dyrektywa PNR.

76. Tymczasem, poza Królestwem Danii, które nie podlega tej dyrektywie⁶⁰, prawie wszystkie państwa członkowskie stosują ustanowiony w niej system do lotów „wewnątrzunijnych”⁶¹. Stąd wniosek, że system ten ma zastosowanie do wszystkich lotów rozpoczynających i kończących się w Unii, a także do prawie wszystkich lotów wykonywanych wewnątrz Unii.

77. Po trzecie, co się tyczy danych PNR podlegających przekazaniu, załącznik I wymienia 19 rubryk dotyczących danych biograficznych⁶², szczegółów podróży lotniczej⁶³ i innych danych zebranych w kontekście umowy przewozu lotniczego, takich jak numer telefonu, adres e-mail, formy płatności, biuro podróży lub agencja turystyczna, informacje o bagażu oraz uwagi ogólne⁶⁴. Tymczasem, jak wskazał Trybunał w pkt 128 opinii 1/15, wypowiadając się w przedmiocie rubryk zawartych w załączniku do projektu umowy między Kanadą a Unią Europejską o przekazywaniu i przetwarzaniu danych dotyczących przelotu pasażera (zwanego dalej „projektem umowy PNR Kanada–UE”), sformułowanych w sposób silnie analogiczny do pozycji znajdujących się w załączniku I, „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”.

78. Po czwarte, zgodnie z art. 6 dyrektywy PNR dane przekazywane przez przewoźników lotniczych są analizowane przez JIP za pomocą środków zautomatyzowanych, i to *w sposób systematyczny*, to znaczy niezależnie od tego, czy istnieje choćby najmniejsze podejrzenie, że

⁶⁰ Zgodnie z art. 1 i 2 protokołu (nr 22) w sprawie stanowiska Danii, ponieważ rzeczne państwo członkowskie nie uczestniczyło w przyjęciu dyrektywy PNR, nie jest nią związane ani nie podlega jej stosowaniu (zob. motyw 40 tej dyrektywy). Z uwag na piśmie przedstawionych przez rząd duński wynika jednak, że Królestwo Danii przyjęło w 2018 r. ustawę w sprawie gromadzenia, wykorzystywania i przechowywania danych PNR, której przepisy są w znacznym stopniu zgodne z przepisami dyrektywy PNR. Co się tyczy Irlandii, z motywu 39 dyrektywy PNR wynika, że zgodnie z art. 3 Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do traktatu UE i do traktatu TFUE, to państwo członkowskie powiadomiło o chęci uczestniczenia w przyjęciu i stosowaniu tej dyrektywy.

⁶¹ Komisja opublikowała zaktualizowaną listę państw członkowskich, które podjęły decyzję o stosowaniu dyrektywy PNR do lotów wewnątrzunijnych zgodnie z art. 2 dyrektywy [PNR] (Dz.U. 2020, C 358, s. 7), sprostowaną we wrześniu 2021 r. wraz z dodaniem Słowenii i wykreśleniem odesłania do Zjednoczonego Królestwa (Dz.U. 2021, C 360, s. 8). Na tej liście nie ma Irlandii i Austrii. Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady dotyczące przeglądu dyrektywy [PNR] z dnia 24 lipca 2020 r., COM(2020) 305 final (zwane dalej „sprawozdaniem Komisji z 2020 r.”, s. 11), wskazuje, że wszystkie państwa członkowskie, z jednym wyjątkiem, rozszerzyły gromadzenie danych PNR na loty wewnątrzunijne.

⁶² Zobacz w szczególności pkt 4 i 18 załącznika I, dotyczące nazwisk, płci, daty urodzenia, obywatelstwa i dokumentów tożsamości pasażera.

⁶³ Zobacz w szczególności pkt 2, 3, 7, 13 i 18 załącznika I do dyrektywy PNR, wymieniające między innymi numer lotu, lotniska odlotu i przylotu, jak również daty i godziny odlotu i przylotu.

⁶⁴ Zobacz pkt 5, 6, 9, 12 i 16 załącznika I.

osoby, których dane dotyczą, mogą uczestniczyć w przestępstwach terrorystycznych lub w poważnej przestępczości. W szczególności, w ramach wstępnej oceny pasażerów przewidzianej w art. 6 ust. 2 lit. a) tej dyrektywy i zgodnie z ust. 3 tego artykułu, dane te mogą zostać zweryfikowane poprzez porównanie z bazami danych, „które mają znaczenie” [art. 6 ust. 3 lit. a)], i być przetwarzane według wcześniej ustalonych kryteriów [art. 6 ust. 3 lit. b)]. Pierwszy rodzaj przetwarzania może zaś dostarczać dodatkowych informacji na temat życia prywatnego osób, których dane dotyczą⁶⁵, a w zależności od tego, jakie bazy danych wykorzystywano do porównania, może nawet umożliwić ustalenie *konkretnego profilu* tych osób. W tych okolicznościach zarzut podniesiony przez szereg rządów, zgodnie z którym dyrektywa PNR pozwala jedynie na dostęp do względnie ograniczonego zbioru danych osobowych, nie odzwierciedla prawidłowo potencjalnego zakresu ingerencji w prawa podstawowe chronione przez art. 7 i 8 karty, jaką dyrektywa ta przewiduje, zważywszy na szeroki zakres danych, do których dostęp dyrektywa ta może umożliwiać. Jeśli chodzi o drugi rodzaj przetwarzania danych, przewidziany w art. 6 ust. 3 lit. b) dyrektywy PNR, pragnę przypomnieć, że w pkt 169 i 172 opinii 1/15 Trybunał podkreślił, iż z każdym rodzajem analizy opartej na wcześniej ustalonych kryteriach wiąże się wystąpienie pewnego odsetka błędów, a w szczególności pewnej liczby fałszywych rezultatów pozytywnych. Zgodnie z danymi liczbowymi zawartymi w dokumencie roboczym służb Komisji⁶⁶ (zwanym dalej „dokumentem roboczym z 2020 r.”) załączonym do sprawozdania Komisji z 2020 r. liczba wyników pozytywnych, które w wyniku indywidualnej oceny przewidzianej w art. 6 ust. 5 dyrektywy PNR okazały się błędne, jest dość poważna i wynosiła w latach 2018 i 2019 co najmniej 5 na 6 zidentyfikowanych osób⁶⁷.

79. Po piąte, zgodnie z art. 12 ust. 1 dyrektywy PNR dane PNR są zatrzymywane w bazie danych JIP na okres pięciu lat od przekazania ich do JIP w państwie członkowskim, na którego terytorium ma miejsce przylot lub z którego terytorium ma miejsce odlot. Dyrektywa PNR daje zatem dostęp do informacji na temat życia prywatnego pasażerów lotniczych przez szczególnie długi czas⁶⁸. Ponadto, ponieważ przekazywanie danych PNR dotyczy prawie wszystkich lotów wykonywanych z i do Unii oraz w obrębie jej terytorium, a samolot stał się środkiem transportu raczej powszechnym, znaczna część pasażerów lotniczych mogłaby znaleźć się w sytuacji praktycznie permanentnego przechowywania ich danych z tego tylko powodu, że korzystają z samolotu co najmniej dwa razy na pięć lat.

80. Wreszcie, w ujęciu bardziej ogólnym dyrektywa PNR przewiduje środki, które rozpatrywane ogólnie mają na celu ustanowienie na poziomie Unii systemu nadzoru „nieukierunkowanego”, czyli takiego, który nie jest uruchamiany w oparciu o podejrzenie ciężące na jednej osobie lub szeregu konkretnych osób, a zatem „masowego”, ponieważ nadzór ów prowadzony jest na danych osobowych dużej liczby osób⁶⁹, obejmujących daną kategorię osób w całości⁷⁰, a także „aktywnego” – przez to, że jego działanie polega nie tylko na odpytywaniu bazy danych na temat niebezpieczeństw znanych, ale również na znajdowaniu i identyfikowaniu zagrożeń dotąd

⁶⁵ Zobacz podobnie opinia 1/15, pkt 131.

⁶⁶ SWD (2020) 128 final.

⁶⁷ Dokument roboczy z 2020 r. (s. 28 i przypis 55) mówi o wskaźniku wyników pozytywnych wynoszącym 0,59% w 2019 r., z których jedynie 0,11% było przedmiotem przekazania właściwym organom. W 2018 r. odpowiednie odsetki wynosiły, odpowiednio, 0,25% i 0,04%.

⁶⁸ Zobacz opinia 1/15, pkt 132.

⁶⁹ System ustanowiony dyrektywą PNR mógł przed kryzysem sanitarnym obejmować do miliarda pasażerów rocznie; dane dostępne pod adresem <https://ec.europa.eu/eurostat/databrowser/view/ttr00012/default/table?lang=fr>.

⁷⁰ To jest wszystkich osób, które odpowiadają pojęciu „pasażera” w rozumieniu art. 3 pkt 4 dyrektywy PNR i korzystają z „lotu pozaunijnego” lub de facto „lotu wewnątrzunijnego”.

nieznanych⁷¹. Tego rodzaju środki ze swej natury prowadzą do poważnych ingerencji w prawa podstawowe chronione przez art. 7 i 8 karty⁷², związanych w szczególności z ich charakterem prewencyjnym i prognostycznym, który wymaga oceny danych osobowych szerokich segmentów populacji, przy czym celem jest „zidentyfikowanie” osób, które – w zależności od wyniku tej oceny – należy poddać dokładniejszemu badaniu przez właściwe organy⁷³. Ponadto coraz popularniejsze przetwarzanie, w celu zapobiegania niektórym formom poważnej przestępczości, dużych ilości danych osobowych o zróżnicowanym charakterze, gromadzonych „hurtowo”, oraz ich zestawianie i zbiorowe przetwarzanie pociągają za sobą „skutek kumulatywny”, który zwiększa wagę ograniczeń praw podstawowych do poszanowania życia prywatnego i ochrony danych osobowych oraz może sprzyjać procesowi stopniowego osuwania się systemu w kierunku „społeczeństwa nadzoru”⁷⁴.

81. Na podstawie całości powyższych rozważań wyrażam stanowisko, że ingerencję, jaką stanowi dyrektywa PNR w prawa podstawowe chronione przez art. 7 i 8 karty, należy uznać co najmniej za „poważną”.

82. Prawdą jest, jak podnosi w szczególności Komisja, że wszystkie gwarancje i zabezpieczenia przewidziane w dyrektywie PNR, w szczególności służące uniknięciu nadużywania danych PNR, mogą zmniejszyć intensywność lub wagę tych ingerencji. Niemniej jednak każdy system, który przewiduje dostęp organów władzy publicznej do danych osobowych i ich przetwarzanie przez owe organy, charakteryzuje się pewną wagą, patrząc przez pryzmat ochrony praw podstawowych, która to waga jest nierozzerwalnie związana z jego obiektywnymi cechami. Wagę tę należy ustalić moim zdaniem przed przystąpieniem do oceny wystarczającego i odpowiedniego charakteru gwarancji przewidzianych przez ów system, w ramach analizy proporcjonalności tych ingerencji. Dotychczas Trybunał postępował, jak mi się wydaje, w ten właśnie sposób.

83. Aby wprowadzone dyrektywą PNR ingerencje w prawa podstawowe do poszanowania życia prywatnego i ochrony danych osobowych były zgodne z kartą, powinny spełniać warunki określone w pkt 65 i 66 niniejszej opinii, co zostanie zbadane poniżej w granicach zagadnień, które zostały przedstawione Trybunałowi przez sąd odsyłający.

⁷¹ W opracowaniu przyjętym przez Europejską Komisję na rzecz Demokracji przez Prawo (Komisję Wenecką) w 2015 r. stwierdzono, że takie środki są elementem „nadzoru strategicznego” i podążają za „ogólną tendencją” do „aktywnego nadzoru” ludności, zob. opracowanie *Mise à jour du rapport de 2007 sur le contrôle démocratique des services de sécurité et rapport sur le contrôle démocratique des agences de collecte de renseignements d'origine électromagnétique*, przyjęte przez Komisję Wenecką na 102. posiedzeniu plenarnym (Wenecja, 20–21 marca 2015 r.), [https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD\(2015\)006-f](https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2015)006-f), pkt 61.

⁷² Co się tyczy art. 8 EKPC, zob. wyrok ETPC z dnia 25 maja 2021 r. w sprawie Big Brother Watch i in. przeciwko Zjednoczonemu Królestwu (CE:ECHR:2021:0525JUD005817013, § 325, zwany dalej „wyrokiem Big Brother Watch”) w sprawie środków masowego przechwytywania, w którym ETPC stwierdza, że intensywność ingerencji tych środków w korzystanie z prawa do poszanowania życia prywatnego rośnie na kolejnych etapach tego procesu, którymi są początkowe przechwycenie i zatrzymanie komunikatów i powiązanych z nimi danych, zautomatyzowane przetwarzanie w drodze zastosowania selektorów, badanie przez analityków, późniejsze zatrzymanie danych i wykorzystanie „produktu końcowego”.

⁷³ Zobacz podobnie motywy 6 i 7 dyrektywy PNR; zob. w przedmiocie dogłębnej analizy celów i skutków w dziedzinie ochrony życia prywatnego i danych osobowych raport zatytułowany *Passenger Name Records (PNR), data mining and data protection: the need for strong safeguards*, opracowany przez D. Korffa z udziałem M. Georgesa, <https://rm.coe.int/16806a601b> (zwany dalej „raportem Korffa”).

⁷⁴ Jak wskazano w raporcie Korffa, „PNR is not an isolated issue, but a new symptom of a much wider disease”.

3. W przedmiocie uzasadnienia ingerencji wynikającej z dyrektywy PNR

84. Trzecie pytanie prejudycjalne dotyczy poszanowania warunku określonego w art. 52 ust. 1 zdanie pierwsze karty, zgodnie z którym każda ingerencja w prawo podstawowe musi być „przewidziana ustawą”, natomiast pytania prejudycjalne drugie, czwarte, szóste i ósme dotyczą w szczególności poszanowania zasady proporcjonalności, o której mowa w zdaniu drugim tego postanowienia.

a) W przedmiocie poszanowania wymogu, aby wszelkie ograniczenia w korzystaniu z prawa podstawowego zapisanego w karcie były przewidziane ustawą

85. Zgodnie z utrwalonym orzecznictwem Trybunału⁷⁵, opierającym się na orzecznictwie ETPC⁷⁶, wymóg, zgodnie z którym wszelkie ograniczenia w korzystaniu z prawa podstawowego muszą być „przewidziane ustawą”, nie odnosi się wyłącznie do „prawnego” źródła ingerencji – które nie jest przedmiotem niniejszej sprawy – lecz oznacza również, że podstawa prawna, która pozwala na taką ingerencję, powinna także w sposób *jasny i precyzyjny* określać jej zakres. Ponieważ ten drugi aspekt objęty wyrażeniem „przewidziane ustawą”, w rozumieniu zarówno art. 52 ust. 1 karty, jak i jej art. 8 ust. 2 oraz art. 8 EKPC, związany jest z „jakością prawa”, a zatem dostępnością i przewidywalnością rozpatrywanego środka⁷⁷, służy nie tylko zapewnieniu przestrzegania zasady legalności i ochrony przed arbitralnością⁷⁸, lecz odpowiada również wymogowi pewności prawa. Wymóg ten uzyskał potwierdzenie również w opinii Komitetu Doradczego Konwencji nr 108⁷⁹ z dnia 19 sierpnia 2016 r. o skutkach przetwarzania danych pasażerów w dziedzinie ochrony danych (zwanej dalej „opinią z dnia 19 sierpnia 2016 r.”)⁸⁰.

86. Prawodawca Unii poprzez przyjęcie dyrektywy PNR ograniczył prawa ustanowione w art. 7 i 8 karty. Ingerencji w te prawa, które dyrektywa umożliwia, nie można zatem uznać za konsekwencję wyboru państw członkowskich⁸¹, niezależnie od zakresu uznania, z którego mogły korzystać w chwili jej transpozycji do prawa krajowego, lecz znajdują one podstawę prawną w samej dyrektywie PNR. W tych okolicznościach, w celu zastosowania się do orzecznictwa

⁷⁵ Zobacz między innymi wyroki: z dnia 16 lipca 2020 r., Facebook Ireland i Schrems (C-311/18, EU:C:2020:559, pkt 175); z dnia 8 września 2020 r., Recorded Artists Actors Performers (C-265/19, EU:C:2020:677, pkt 86 i przytoczone tam orzecznictwo); a także wyrok Privacy international, pkt 65.

⁷⁶ Zobacz między innymi wyroki ETPC: z dnia 8 czerwca 2006 r. w sprawie Lupsa przeciwko Rumunii (CE:ECHR:2006:0608JUD001033704, §§ 32, 33); z dnia 15 grudnia 2020 r. w sprawie Pişkin przeciwko Turcji (CE:ECHR:2020:1215JUD003339918, § 206); zob. także ww. wyrok w sprawie Big Brother Watch, § 333. W przedmiocie konieczności nadania wyrażeniu „przewidziane ustawą” w art. 52 ust. 1 karty takiej samej wykładni jak przyjęta przez ETPC zob. opinia rzecznika generalnego M. Watheleta w sprawie zakończonej wyrokiem WebMindLicenses (C-419/14, EU:C:2015:606, pkt 134–143).

⁷⁷ Zobacz ostatnio wyrok w sprawie Big Brother Watch, pkt 333.

⁷⁸ Zobacz wyrok z dnia 17 grudnia 2015 r., WebMindLicenses (C-419/14, EU:C:2015:832, pkt 81); zob. także wyrok ETPC z dnia 1 lipca 2008 r. w sprawie Liberty i in. przeciwko Zjednoczonemu Królestwu (CE:ECHR:2008:0701JUD005824300, § 69); a także wyrok Big Brother Watch, pkt 333.

⁷⁹ Konwencja Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, przyjęta w Strasburgu w dniu 28 stycznia 1981 r. i ratyfikowana przez wszystkie państwa członkowskie, znana szerzej jako „konwencja nr 108”. W 2018 r. w celu modernizacji tej konwencji opracowano protokół zmian do niej. Decyzją Rady (UE) 2019/682 z dnia 9 kwietnia 2019 r. (Dz.U. 2019, L 115, s. 7) państwa członkowskie zostały upoważnione do ratyfikacji, w interesie Unii, wspomnianego protokołu zmian w zakresie, w jakim jego postanowienia należą do wyłącznej kompetencji Unii. W dalszej części niniejszej opinii będę odwoływał się również do tekstu zmodernizowanej konwencji nr 108, która mimo że nie została jak dotąd ratyfikowana przez wszystkie państwa członkowskie ani nie weszła jeszcze w życie, przewiduje, jak wynika z decyzji 2019/682, gwarancje oparte na tych samych zasadach, co ustanowione w RODO i w dyrektywie policyjnej.

⁸⁰ <https://rm.coe.int/t-pd-2016-18rev-avis-pnr-fr/16807b6c09>, s. 3 i 5. Sprawozdanie wyjaśniające do protokołu zmian do konwencji nr 108 (zwane dalej „sprawozdaniem wyjaśniającym do zmodernizowanej konwencji nr 108”) kładzie również nacisk na wymóg, aby środek przewidujący ingerencję w prawa do poszanowania życia prywatnego i do ochrony danych osobowych był „dostępny”, „przewidywalny”, „wystarczająco szczegółowy” i „jasno sformułowany” [tłumaczenie nieoficjalne], zob. pkt 91 rzeczonego sprawozdania wyjaśniającego, <https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726>.

⁸¹ Zobacz a contrario wyrok z dnia 3 grudnia 2019 r., Republika Czeska/Parlament i Rada (C-482/17, EU:C:2019:1035, pkt 135).

przypomnianego w pkt 85 niniejszej opinii oraz do „wysokich standardów” ochrony praw podstawowych zapisanych w szczególności w karcie i w EKPC, do których odwołuje się motyw 15 dyrektywy PNR, prawodawca Unii miał obowiązek ustanowienia jasnych i precyzyjnych zasad określających zarówno zakres, jak i zastosowanie środków wiążących się z rzeczoną ingerencją.

87. O ile w trzecim pytaniu prejudycjalnym sąd odsyłający zastanawia się nad przestrzeganiem tego obowiązku konkretnie w odniesieniu do pkt 12 i 18 załącznika I, o tyle analiza pytań prejudycjalnych drugiego, czwartego i szóstego, w których sąd ten wyraża wątpliwości co do niezbędnego charakteru ingerencji, jaką dyrektywa PNR pociąga za sobą w odniesieniu do praw podstawowych określonych w art. 7 i 8 karty, wymaga zajęcia stanowiska również w przedmiocie wystarczająco jasnego i precyzyjnego charakteru rozpatrywanych przepisów dyrektywy PNR.

88. Mimo że, jak wskazałem w pkt 85 niniejszej opinii, analiza ta dotyczy zgodności z prawem ingerencji w rozumieniu art. 52 ust. 1 zdanie pierwsze karty, przeprowadzę ją w ramach badania proporcjonalności, o której mowa w zdaniu drugim tego ustępu, zgodnie z podejściem przyjętym zarówno przez Trybunał, jak i przez ETPC w sprawach, których przedmiotem były środki dotyczące przetwarzania danych osobowych⁸².

b) W przedmiocie poszanowania istoty praw zapisanych w art. 7 i 8 karty

89. Zgodnie z art. 52 ust. 1 zdanie pierwsze karty wszystkie ograniczenia w korzystaniu z praw podstawowych muszą opierać się nie tylko na wystarczająco precyzyjnej podstawie prawnej, ale również szanować *istotę* tych praw.

90. Jak wskazałem w pkt 66 niniejszej opinii, wymóg ten – który ujęto w konstytucjach różnych państw członkowskich⁸³ i który, choć nieuznany wyraźnie w EKPC, jest jednak dobrze ugruntowany w orzecznictwie ETPC⁸⁴ – zapisany jest w art. 52 ust. 1 karty⁸⁵. Wymóg ów, który Trybunał uznał na długo przed jego kodyfikacją⁸⁶, znajduje niezmiennie potwierdzenie w orzecznictwie sądów Unii, również po wejściu w życie traktatu z Lizbony.

91. W szczególności z wyroku z dnia 6 października 2015 r., Schrems⁸⁷, wynika, że nieprzestrzeganie istoty prawa podstawowego przez akt Unii skutkuje *automatycznie* nieważnością tego aktu, bez konieczności dokonywania zrównoważenia wchodzących w grę interesów. Trybunał uznaje zatem, że każde prawo podstawowe ma „rdzeń” gwarantujący każdemu człowiekowi sferę wolności chroniącą przed jakąkolwiek ingerencją ze strony władz publicznych i która nie może podlegać ograniczeniom⁸⁸, gdyż w przeciwnym wypadku doszłoby do podważenia zasad demokracji, państwa prawa i poszanowania godności ludzkiej, leżących u podstaw ochrony praw podstawowych. Ponadto zarówno z brzmienia art. 52 ust. 1 karty, jak i z orzecznictwa Trybunału, a w szczególności z wyroku Schrems I wynika, że ocenę istnienia

⁸² Zobacz m.in. wyrok La Quadrature du Net, pkt 132 i przytoczone tam orzecznictwo; zob. także wyrok ETPC w sprawie Big Brother Watch, pkt 334.

⁸³ Zobacz w tym względzie T. Tridimas, G. Gentile, *The essence of Rights: an unreliable Boundary?*, German Law Journal, 2019, s. 796; K. Lenaerts, *Limits on limitations: The Essence of Fundamental Rights in the EU*, German Law Journal, 2019, 20, s. 779 i nast.

⁸⁴ Poczawszy od wyroku ETPC z dnia 24 października 1979 r. w sprawie Winterwerp przeciwko Niderlandom (CE:ECHR:1979:1024JUD000630173, pkt 60).

⁸⁵ Zobacz Wyjaśnienia dotyczące Karty praw podstawowych (Dz.U. 2007, C 303, s. 17, w szczególności „Wyjaśnienie odnoszące się do artykułu 52”, s. 32, zwane dalej „wyjaśnieniami dotyczącymi karty”).

⁸⁶ Zobacz podobnie, w szczególności, już wyroki: z dnia 14 maja 1974 r., Nold/Komisja (4/73, EU:C:1974:51, pkt 14); z dnia 13 grudnia 1979 r., Hauer (44/79, EU:C:1979:290, pkt 23).

⁸⁷ C-362/14, zwany dalej „wyrokiem Schrems I”, EU:C:2015:650, pkt 94–98.

⁸⁸ Zobacz K. Lenaerts, op.cit., s. 781; T. Tridimas, G. Gentile, op.cit., s. 803.

ingerencji w istotę danego prawa podstawowego należy przeprowadzić przed oceną proporcjonalności kwestionowanego środka i niezależnie od niej. Innymi słowy, test ten ma charakter autonomiczny.

92. Jednakże określenie tego, co stanowi „istotę”, a co za tym idzie, nienaruszalną treść prawa podstawowego, którego wykonywanie może być ograniczone, jest operacją niezwykle złożoną. Chociaż aby pojęcie to mogło odgrywać swoją rolę, musi istnieć możliwość zdefiniowania go w sposób absolutny, w świetle istotnych cech danego prawa podstawowego, interesów subiektywnych i obiektywnych, których ochronę ma zapewnić, oraz, bardziej ogólnie rzecz biorąc, jego funkcji w społeczeństwie demokratycznym opartym na poszanowaniu godności ludzkiej⁸⁹, to w praktyce taka operacja jest prawie niemożliwa, przynajmniej bez uwzględnienia kryteriów, które stosuje się zwykle przy badaniu proporcjonalności ingerencji w dane prawo, takich jak waga tej ingerencji, jej zakres lub rozciągłość czasowa, czyli bez wzięcia pod uwagę specyfiki poszczególnych przypadków.

93. Co się tyczy w szczególności prawa podstawowego do poszanowania życia prywatnego, należy wziąć pod uwagę nie tylko wagę, jakie ma – dla zdrowia umysłowego i fizycznego każdej osoby, jej dobrostanu, autonomii, rozwoju osobistego, zdolności do tworzenia i utrzymywania relacji społecznych – posiadanie sfery prywatnej pozwalającej na rozwinięcie swojego osobistego świata wewnętrznego, lecz również rolę, jaką prawo to odgrywa w ochronie innych praw i wolności, takich jak w szczególności wolność myśli, sumienia, religii, wyrazu i informacji, których pełne wykorzystanie wymaga uznania pewnej sfery intymności. Mówiąc ogólniej, należy wziąć pod uwagę funkcję, jaką poszanowanie prawa do życia prywatnego pełni w społeczeństwie demokratycznym⁹⁰. Trybunał wydaje się oceniać istnienie naruszenia istoty tego prawa, biorąc pod uwagę zarówno *intensywność*, jak i *zakres* ingerencji, co pozwala dojść do wniosku, że takie naruszenie określa się raczej pod względem ilościowym niż jakościowym. I tak, po pierwsze, w wyroku Digital Rights Trybunał uznał zasadniczo, że obowiązek przechowywania danych przewidziany przez dyrektywę 2006/24/WE⁹¹ nie osiąga takiego stopnia wagi, aby wpływać na istotę prawa do poszanowania życia prywatnego, ponieważ nie pozwala on na „na zapoznanie się z samą treścią komunikatów elektronicznych”⁹². Po drugie, w opinii 1/15 Trybunał uznał zasadniczo, że ograniczenie dotyczące jedynie niektórych aspektów życia prywatnego osób, których dane dotyczą, nie może prowadzić do ingerencji w istotę tego prawa podstawowego⁹³.

94. Jeśli chodzi o podstawowe prawo do ochrony danych osobowych, Trybunał uważa, jak się wydaje, że istota tego prawa jest zachowana, jeżeli środek, który ustanawia ingerencję, określa cele przetwarzania i przewiduje zasady zapewniające bezpieczeństwo danych osobowych, w szczególności przed przypadkowym lub bezprawnym zniszczeniem, utratą lub zmianą⁹⁴.

⁸⁹ Wyjaśnienia dotyczące karty wyraźnie wskazują, że „godność człowieka jest częścią istoty praw zawartych w [k]arcie” i „dlatego też prawo to nie może zostać naruszone, nawet jeżeli oznaczałoby to ograniczenie innego prawa”.

⁹⁰ Odsyłam w tym względzie do rozważań zawartych we wspólnym częściowo odrębnym zdaniu sędziów P. Lemmensa, F. Vehabovića i M. Bošnjak w wyroku Big Brother Watch, §§ 3–10.

⁹¹ Dyrektywa Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (Dz.U. 2006, L 105, s. 54).

⁹² Zobacz wyrok Digital Rights, pkt 39; a także, w odniesieniu do dyrektywy 2002/58, zob. wyrok Tele2 Sverige, pkt 101.

⁹³ Zobacz opinia 1/15, pkt 150.

⁹⁴ Zobacz podobnie w szczególności wyrok Digital Rights, pkt 40.

95. Chociaż w niniejszej sprawie sąd odsyłający nie powołał się wyraźnie na wymóg poszanowania istoty praw określonych w art. 7 i 8 karty, to u podstaw pytań prejudycjalnych czwartego i szóstego leży moim zdaniem właśnie kwestia poszanowania rzeczzonego wymogu. Z tego powodu proponuję, aby Trybunał ustosunkował się do tego zagadnienia.

96. W tym względzie przypominam, że w pkt 150 opinii 1/15, Trybunał – chociaż przyznał, iż dane PNR „mogą w stosownych wypadkach ujawniać bardzo dokładne informacje o życiu prywatnym danej osoby”⁹⁵, przy czym informacje te umożliwiają bezpośrednio lub pośrednio zapoznanie się ze szczególnie chronionymi danymi odnośnej osoby⁹⁶ – stwierdził jednak, w odniesieniu do projektu umowy PNR Kanada–UE, że ponieważ „charakter tych informacji sprawia, że są one ograniczone do pewnych aspektów życia prywatnego, związanych w szczególności z podróżami lotniczymi między Kanadą a Unią”, to ingerencje w prawo podstawowe do poszanowania życia prywatnego nie są tego rodzaju, by mogły naruszać istotę rzeczzonego prawa.

97. Tymczasem pomijając okoliczność, że dane PNR, o których mowa w projekcie umowy PNR Kanada–UE, miały być przekazywane do państwa trzeciego, a ich późniejsze przetwarzanie powinno być prowadzone przez organy tego państwa trzeciego na jego terytorium, ingerencje w prawo podstawowe do poszanowania życia prywatnego wynikające z tego projektu umowy oraz ingerencje przewidziane w dyrektywie PNR są ze swej natury w znacznym stopniu zbieżne. Jest tak w szczególności w odniesieniu do objętych nimi danych PNR, systematycznego i uogólnionego charakteru przekazywania i przetwarzania tych danych, zautomatyzowanego sposobu ich przekazywania i przetwarzania, a także warunków przechowywania rzeczonych danych. Natomiast te dwie sprawy różnią się niejako „zasięgiem geograficznym” ingerencji. Jak bowiem wskazałem w pkt 77 niniejszej opinii, operacje przetwarzania danych rozpatrywane w niniejszej sprawie nie ograniczają się do połączeń lotniczych z jednym państwem trzecim, jak miało to miejsce w przypadku opinii 1/15, lecz dotyczą prawie wszystkich lotów kończących się i rozpoczynających w Unii oraz odbywających się w obrębie jej terytorium. Płyne stąd wniosek, że w porównaniu do projektu umowy PNR Kanada–UE dyrektywa PNR prowadzi do systematycznego przetwarzania znacznie większej liczby danych pasażerów lotniczych, przemieszczających się samolotami wewnątrz Unii i poza nią. Ponadto, biorąc pod uwagę wzrost ilości przetwarzanych danych oraz częstotliwość, z jaką są gromadzone, ich przetwarzanie prawdopodobnie może dostarczyć jednocześnie dokładniejszych i bardziej obszernych informacji na temat życia prywatnego osób, których dane dotyczą (nawyki podróżnicze, relacje osobiste, informacje o sytuacji finansowej itp.).

98. Niemniej jednak, jak miało to miejsce w przypadku opinii 1/15, informacje te, rozpatrywane odrębnie, dotyczą jedynie niektórych aspektów życia prywatnego, związanych z podróżami lotniczymi. Biorąc zaś pod uwagę konieczność zdefiniowania pojęcia „istoty” praw podstawowych w sposób zawężający, aby zachowało ono funkcję bastionu odpierającego ataki na istotę tych praw, jestem zdania, że wniosek, do którego Trybunał doszedł w pkt 150 opinii 1/15, można zastosować w niniejszej sprawie.

99. W opinii 1/15 Trybunał również wykluczył naruszenie istoty prawa do ochrony danych osobowych⁹⁷. Wniosek ten można moim zdaniem przenieść na grunt niniejszej sprawy. W istocie bowiem, podobnie jak w przypadku projektu umowy PNR Kanada–UE, dyrektywa PNR w art. 1 ust. 2 określa cele przetwarzania danych PNR. Ponadto dyrektywa ta, jak również inne akty Unii,

⁹⁵ Zobacz podobnie opinia 1/15, pkt 128.

⁹⁶ Zobacz opinia 1/15, pkt 164, 165.

⁹⁷ Zobacz opinia 1/15, pkt 150.

do których odsyła, w szczególności RODO i dyrektywa policyjna, zawierają przepisy szczególne mające na celu zapewnienie w szczególności bezpieczeństwa, poufności i integralności tych danych, a także ich ochrony przed niezgodnym z prawem dostępem i przetwarzaniem. O ile nie można uznać, że przepisy takie jak przewidziane w dyrektywie PNR dotyczą istoty praw podstawowych chronionych przez art. 7 i 8 karty, o tyle jednak muszą one przejść ścisłą i rygorystyczną kontrolę proporcjonalności.

c) W przedmiocie poszanowania wymogu, zgodnie z którym ingerencja musi odpowiadać celowi interesu ogólnego

100. Dyrektywa PNR ma w szczególności na celu zapewnienie bezpieczeństwa wewnętrznego Unii oraz ochronę życia i bezpieczeństwa ludzkiego dzięki przekazywaniu danych PNR właściwym organom państw członkowskich w celu wykorzystania ich w ramach walki z terroryzmem i poważną przestępczością⁹⁸.

101. Zwłaszcza z art. 1 ust. 2 dyrektywy PNR w związku z jej motywami 6 i 7, jak również z wniosku Komisji, który doprowadził do przyjęcia tej dyrektywy (zwanego dalej „projektem dyrektywy PNR”)⁹⁹, wynika, że w ramach realizacji takiego celu organy ścigania¹⁰⁰ wykorzystują dane PNR na różne sposoby. Po pierwsze, dane te są wykorzystywane do identyfikacji osób uczestniczących lub podejrzanych o udział w popełnionych już przestępstwach terrorystycznych i poważnej przestępczości, do gromadzenia dowodów, a – w odpowiednich przypadkach – do wykrywania współsprawców przestępstw i rozpracowywania siatek przestępczych (wykorzystanie w „trybie reaktywnym”). Po drugie, dane PNR mogą być oceniane przed przybyciem lub wyjazdem pasażerów w celu zapobieżenia popełnieniu przestępstwa oraz identyfikacji osób, które dotychczas nie były podejrzewane o udział w przestępstwach terrorystycznych lub w poważnej przestępczości i które na podstawie wyników takiego sprawdzenia powinny być poddane dalszemu sprawdzeniu przez organy ścigania (wykorzystanie w „trybie czasu rzeczywistego”). Wreszcie, dane PNR wykorzystuje się do określenia kryteriów oceny, które można następnie zastosować przy analizie zagrożenia, jakie stanowią pasażerowie przed ich przybyciem i przed ich wyjazdem (wykorzystanie w „trybie aktywnym”). Takie aktywne wykorzystanie danych PNR powinno umożliwić organom ścigania reagowanie na zagrożenie przestępstwami terrorystycznymi i poważną przestępczością z innej perspektywy niż w przypadku przetwarzania innych kategorii danych osobowych¹⁰¹.

102. Z orzecnictwa Trybunału wynika, że cel ochrony bezpieczeństwa publicznego, obejmujący w szczególności zapobieganie, dochodzenie, wykrywanie i ściganie zarówno przestępstw terrorystycznych, jak i przestępstw kwalifikujących się jako poważna przestępczość stanowi cel interesu ogólnego Unii w rozumieniu art. 52 ust. 1 karty, który może uzasadniać ingerencje, nawet poważne, w prawa podstawowe ustanowione w art. 7 i 8 karty¹⁰².

⁹⁸ Zobacz w szczególności motywy 5, 6, 15 i 22 dyrektywy PNR.

⁹⁹ Propozycja Komisji z dnia 2 lutego 2011 r. w sprawie wykorzystania danych dotyczących przelotu pasażera w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania [COM(2011) 32 wersja ostateczna, s. 4].

¹⁰⁰ Dla uproszczenia w niniejszej opinii będę używał wyrażen „służby ścigania” lub „organy ścigania” na oznaczenie w sposób ogólny każdego organu, któremu przysługują uprawnienia w dziedzinach wykrywania, zapobiegania, ścigania lub prowadzenia dochodzeń w odniesieniu do terroryzmu lub poważnej przestępczości objętych dyrektywą PNR.

¹⁰¹ Zobacz motyw 7 dyrektywy PNR. Zobacz również projekt dyrektywy PNR, s. 5.

¹⁰² Zobacz podobnie opinia 1/15 oraz wyrok z dnia 2 marca 2021 r., Prokurator (Warunki dostępu do danych dotyczących łączności elektronicznej) (C-746/18, zwany dalej „wyrokiem Prokurator”, EU:C:2021:152, pkt 33 i przytoczone tam orzecznictwo)

103. Trybunał uznał również, że cele ochrony bezpieczeństwa publicznego i zwalczania poważnej przestępczości przyczyniają się do ochrony praw i wolności innych osób¹⁰³. Tak więc w ramach harmonijnego wyważenia z jednej strony tychże celów i, z drugiej strony, praw podstawowych ustanowionych w art. 7 i 8¹⁰⁴ karty należy również uwzględnić wagę praw zapisanych w art. 3, 4, 6 i 7 karty. W tym względzie, o ile w wyroku *La Quadrature du Net* Trybunał uznał, że art. 6 karty „nie może być interpretowany w ten sposób, że nakłada on na organy publiczne obowiązek przyjęcia szczególnych środków w celu ukarania za określone przestępstwa”¹⁰⁵, o tyle jeśli chodzi w szczególności o skuteczną walkę z przestępstwami, których ofiarą są zwłaszcza małoletni i inne osoby podatne na zagrożenia, podkreślił, że ciążące na organach publicznych pozytywne obowiązki przyjęcia środków prawnych w celu ochrony życia prywatnego i rodzinnego mogą wynikać zarówno z art. 7 karty, jak i z jej art. 3 i 4 w odniesieniu do ochrony integralności fizycznej i psychicznej osób, jak również zakazu tortur i niehumanitarnego lub poniżającego traktowania¹⁰⁶.

104. Wreszcie, Trybunał uznał, że waga celu ochrony *bezpieczeństwa narodowego* przewyższa wagę celów zwalczania przestępstw w ogólności, choćby poważnych, a także ochrony bezpieczeństwa publicznego, i może więc uzasadnić środki związane z dalej idącą ingerencją w prawa podstawowe niż środki, które mogłyby być uzasadnione tymi innymi celami¹⁰⁷. Ponieważ działalność terrorystyczna może stanowić zagrożenie dla bezpieczeństwa narodowego państw członkowskich, system wprowadzony dyrektywą PNR przyczynia się do realizacji celu w postaci ochrony bezpieczeństwa narodowego państw członkowskich, ponieważ stanowi instrument zwalczania takich działań.

d) W przedmiocie przestrzegania zasady proporcjonalności

105. Zgodnie z art. 52 ust. 1 zdanie drugie karty, z zastrzeżeniem zasady proporcjonalności, ograniczenia w wykonywaniu uznanego w niej prawa podstawowego 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.

106. W tej kwestii trzeba przypomnieć, że zgodnie z utrwalonym orzecznictwem Trybunału zasada proporcjonalności wymaga, by akty prawne instytucji Unii były odpowiednie do realizacji uzasadnionych celów, którym akty te służą, i nie wykraczały poza to, co jest konieczne do ich osiągnięcia¹⁰⁸.

107. Zgodnie z utrwalonym orzecznictwem Trybunału, ochrona prawa podstawowego do poszanowania życia prywatnego na poziomie Unii wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia ograniczały się do tego, co absolutnie konieczne. Ponadto nie można dążyć do celu interesu ogólnego bez uwzględnienia okoliczności, że należy pogodzić go z prawami podstawowymi, których dotyczy środek, dokonując zbilansowanego wyważenia między celem interesu ogólnego z jednej strony a rozpatrywanymi prawami z drugiej strony¹⁰⁹.

¹⁰³ Zobacz podobnie opinia 1/15, pkt 149 i przytoczone tam orzecznictwo; a także wyrok *La Quadrature du Net*.

¹⁰⁴ Zobacz poniżej analiza proporcjonalności ingerencji.

¹⁰⁵ Zobacz wyrok *La Quadrature du Net*, pkt 125.

¹⁰⁶ Zobacz wyrok *La Quadrature du Net*, pkt 126 i przytoczone tam orzecznictwo.

¹⁰⁷ Zobacz wyrok *La Quadrature du Net*, pkt 136.

¹⁰⁸ Zobacz wyrok *Digital Rights*, pkt 46 i przytoczone tam orzecznictwo.

¹⁰⁹ Zobacz opinia 1/15, pkt 140; wyrok *La Quadrature du Net*, pkt 130 i przytoczone tam orzecznictwo. Wymóg, aby przetwarzanie danych osobowych odzwierciedlało na każdym etapie „sprawiedliwą równowagę między wszystkimi obecnymi w danej sytuacji interesami, bez względu na to, czy są one publiczne, czy prywatne, oraz wchodzącymi w grę prawami i wolnościami” [tłumaczenie nieoficjalne], jest również określony w art. 5 konwencji nr 108.

Konkretniej rzecz ujmując, proporcjonalność ograniczenia praw zapisanych w art. 7 i 8 karty należy oceniać, badając wagę ingerencji, jaką stanowi takie ograniczenie, oraz sprawdzając, czy znaczenie celu interesu ogólnego, do którego zmierza to ograniczenie, pozostaje w relacji do tej wagi¹¹⁰.

108. Z orzecznictwa Trybunału wynika, że aby spełnić wymóg proporcjonalności, dyrektywa PNR jako podstawa prawna będąca źródłem ingerencji w prawa podstawowe ustanowione w art. 7 i 8 karty, opisane w pkt 70–83 niniejszej opinii, musi zawierać jasne i dokładne zasady dotyczące zakresu i sposobu stosowania środków prowadzących do takich ingerencji, a także ustanawiać minimalne wymogi służące temu, aby osoby, których dane zostały przekazane, miały wystarczające gwarancje rzeczywistej ochrony ich danych osobowych przed ryzykiem nadużyć oraz ich bezprawnym udostępnianiem i wykorzystywaniem¹¹¹. Konieczność posiadania takich gwarancji jest jeszcze bardziej istotna, gdy, jak w niniejszej sprawie, dane osobowe są przetwarzane w sposób zautomatyzowany i gdy rzecz dotyczy owej szczególnej kategorii danych osobowych, którą stanowią dane szczególnie chronione¹¹².

109. Co się tyczy zakresu kontroli sądowej poszanowania wymogów wynikających z zasady proporcjonalności, to mając na uwadze znaczącą rolę, jaką odgrywa ochrona danych osobowych w świetle prawa podstawowego do poszanowania życia prywatnego oraz ingerencji w to prawo, której źródłem jest dyrektywa PNR, uprawnienia dyskrecyjne prawodawcy Unii są ograniczone, skutkiem czego kontrola tych uprawnień musi mieć charakter ścisły¹¹³.

1) W przedmiocie przydatności operacji przetwarzania danych PNR, o których mowa w dyrektywie PNR, do realizacji zamierzonego celu

110. W pkt 153 opinii 1/15 Trybunał stwierdził w odniesieniu do projektu umowy PNR Kanada–UE, że przekazywanie danych PNR do Kanady i ich późniejsze przetwarzanie są przydatne do zapewnienia osiągnięcia celu związanego z zapewnieniem ochrony publicznej i bezpieczeństwa publicznego. Wydaje mi się, że rzeczony przydatności gromadzenia i dalszego przetwarzania danych PNR, uznanej od dawna zarówno na poziomie Unii, jak i w skali światowej¹¹⁴, nie można podważyć ani w odniesieniu do lotów pozaunijnych, ani w przypadku lotów wewnątrzunijnych¹¹⁵.

111. Niemniej jednak skuteczność ustanowionego przez dyrektywę systemu PNR można badać jedynie w sposób konkretny, oceniając wyniki jego stosowania¹¹⁶. W tym kontekście istotne jest, aby skuteczność tę oceniać w sposób ciągły, na podstawie możliwie najbardziej dokładnych i wiarygodnych danych statystycznych¹¹⁷. Zatem Komisja powinna w regularnych odstępach czasu przeprowadzać kontrolę analogiczną do przewidzianej już w art. 19 dyrektywy PNR.

¹¹⁰ Zobacz podobnie wyrok z dnia 2 października 2018 r., Ministerio Fiscal (C-207/16, EU:C:2018:788, pkt 55 i przytoczone tam orzecznictwo); a także wyroki: La Quadrature du Net, pkt 131; Prokuratuur, pkt 32.

¹¹¹ Zobacz podobnie wyroki: Digital Rights, pkt 54; Schrems I, pkt 91; opinia 1/15, pkt 141.

¹¹² Zobacz opinia 1/15, pkt 141 i przytoczone tam orzecznictwo.

¹¹³ Zobacz podobnie wyrok Digital Rights, pkt 48.

¹¹⁴ Zobacz podobnie pkt 201–203 niniejszej opinii.

¹¹⁵ Odsyłam w tym względzie do danych zawartych w dokumencie roboczym z 2020 r.

¹¹⁶ Zobacz podobnie opinia z dnia 19 sierpnia 2016 r., s. 5.

¹¹⁷ W przedmiocie znaczenia statystyk dla oceny skuteczności systemu PNR ustanowionego dyrektywą PNR zob. w szczególności opinia 1/2011 z dnia 14 czerwca 2011 r. w sprawie projektu dyrektywy PNR, https://fra.europa.eu/sites/default/files/fra_uploads/1786-FRA-PNR-Opinion-2011_FR.pdf, pkt 2.1.2.1 (zwana dalej „opinią 1/2011 FRA”).

2) W przedmiocie absolutnie koniecznego charakteru ingerencji

112. Mimo że Cour constitutionnelle (trybunał konstytucyjny) nie przedstawił wyraźnie wątpliwości, czy dyrektywa PNR zawiera zasady jasne, precyzyjne i ograniczone do tego, co absolutnie konieczne, jeśli chodzi o określenie celów przetwarzania danych PNR¹¹⁸, analiza proporcjonalności systemu przewidzianego przez tę dyrektywę, o którą zwrócił się sąd odsyłający, nie może moim zdaniem pomijać tej kwestii¹¹⁹.

i) W przedmiocie określenia celów przetwarzania danych PNR

113. Wyraźne określenie celów pozwalających właściwym organom na dostęp do danych osobowych oraz na ich późniejsze wykorzystanie stanowi istotny wymóg każdego systemu przetwarzania danych, w szczególności służącego ściganiu przestępczości. Spełnienie tego wymogu jest ponadto konieczne, aby umożliwić Trybunałowi ocenę proporcjonalności rozpatrywanych środków za pomocą „zubożonego” testu wagi ingerencji w stosunku do znaczenia zamierzonego celu, ustalonego w jego orzecznictwie¹²⁰.

114. Trybunał podkreślił znaczenie jasnego określenia celów środków będących źródłem ograniczeń praw podstawowych do poszanowania życia prywatnego i do ochrony danych osobowych, w szczególności, w wyroku Digital Rights, w którym stwierdził nieważność dyrektywy 2006/24. W pkt 60 tego wyroku Trybunał zauważył, że dyrektywa ta nie przewiduje „żadnego obiektywnego kryterium, które pozwoliłoby zagwarantować, że właściwe organy krajowe będą miały dostęp do danych i będą mogły je wykorzystywać wyłącznie w celu zapobiegania [przestępstwom], wykrywania i ścigania przestępstw, które z uwagi na zakres i wagę ingerencji w prawa podstawowe ustanowione w art. 7 i 8 karty można uznać za wystarczająco poważne, by taką ingerencję uzasadnić”, a wręcz przeciwnie, dyrektywa ta ogranicza się „do ogólnego odesłania, w art. 1 ust. 1, do pojęcia »poważnych przestępstw« określonych w ustawodawstwie każdego państwa członkowskiego”.

115. Artykuł 1 ust. 2 dyrektywy PNR ustanawia ogólne kryterium ograniczające cele, zgodnie z którym „[d]ane PNR zebrane zgodnie z niniejszą dyrektywą mogą być przetwarzane wyłącznie w celach zapobiegania przestępstwom terrorystycznym i poważnej przestępczości oraz ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania”. Jednakże, w przeciwieństwie do dyrektywy 2006/24, dyrektywa PNR nie ogranicza się do tego stwierdzenia, lecz w art. 3 pkt 8 i 9 definiuje zarówno pojęcie „przestępstw terrorystycznych”, jak i „poważnej przestępczości”, przy czym pierwsze z nich poprzez odesłanie do art. 1–4 decyzji ramowej Rady 2002/475/WSiSW z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu (Dz.U. 2002, L 164, s. 3) [zastąpionej dyrektywą (UE) 2017/541]¹²¹, a drugie z nich, z jednej strony, poprzez wymienienie w załączniku II kategorii przestępstw karnych odpowiadających temu pojęciu, a z drugiej strony, ustanawiając próg ich wagi w kategoriach górnej granicy kary pozbawienia wolności lub środków zabezpieczających, którymi przestępstwa te są zagrożone.

¹¹⁸ Pytanie to zadał natomiast w sposób jasny Verwaltungsgericht Wiesbaden (sąd administracyjny w Wiesbaden, Niemcy) w sprawie C-215/20.

¹¹⁹ Komisja została wezwana do przedstawienia uwag w tym względzie w ramach pytania do odpowiedzi na piśmie. Pozostali uczestnicy mogli zająć stanowisko podczas rozprawy.

¹²⁰ Zobacz pkt 107 in fine niniejszej opinii.

¹²¹ Dyrektywa Parlamentu Europejskiego i Rady z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW (Dz.U. 2017, L 88, s. 6).

116. O ile odesłanie do właściwych przepisów dyrektywy 2017/541 pozwala określić w sposób wystarczająco jasny i precyzyjny czyny, które mogą zostać zakwalifikowane jako przestępstwa terrorystyczne na podstawie art. 3 pkt 8 dyrektywy PNR, i ocenić ich wagę na potrzeby wyważenia celu ochrony bezpieczeństwa publicznego, realizowanego przez tę dyrektywę, oraz wagi ingerencji, jaką dyrektywa ta wprowadza w odniesieniu do praw podstawowych ustanowionych w art. 7 i 8 karty, o tyle ten sam wniosek nie nasuwa się z taką samą oczywistością w odniesieniu do wszystkich przestępstw wymienionych w załączniku II.

117. W pkt 177 opinii 1/15 Trybunał uznał, że projekt umowy PNR Kanada–UE definiował wyrażenie „poważne przestępstwa międzynarodowe” z jasnością i precyzją, przewidując wymóg, by były to przestępstwa „podlegające karze pozbawienia wolności w maksymalnym wymiarze co najmniej czterech lat lub karze surowszej”, i odsyłając „do przestępstw zdefiniowanych w prawie kanadyjskim” oraz wymieniając „różne sytuacje, w których przyjmuje się, że przestępstwo ma charakter międzynarodowy”.

118. W porównaniu z postanowieniami zbadanymi przez Trybunał w tejże opinii dyrektywa PNR: po pierwsze, przy definiowaniu odnośnych przestępstw nie bierze pod uwagę ich transgranicznego charakteru; po drugie, zawiera wyczerpujący katalog przestępstw, które ze względu na swój charakter stanowią poważną przestępczość, pod warunkiem że zagrożone są co najmniej karą o górnej granicy przewidzianej w art. 3 pkt 9 tej dyrektywy; po trzecie, obniża co do zasady próg wagi naruszenia, przyjmując kryterium oparte na górnej granicy kary i ustalając ten próg na trzy lata.

119. Co się tyczy, po pierwsze, braku kryterium ograniczenia opartego na charakterze transgranicznym, prawdą jest, że zawężenie przedmiotowego zakresu stosowania dyrektywy PNR wyłącznie do poważnej przestępczości „transgranicznej” pozwoliłoby na ukierunkowanie jej na przestępstwa, które ze swej natury, przynajmniej potencjalnie, mogą mieć obiektywny związek z podróżami lotniczymi, a w konsekwencji z kategoriami danych gromadzonych i przetwarzanych na podstawie dyrektywy PNR¹²². Podzielał jednak co do zasady stanowisko wyrażone przez Komisję, zgodnie z którym inaczej niż w kontekście umowy międzynarodowej istotność i konieczność zastosowania takiego kryterium są mniej oczywiste w przypadku mechanizmu walki z przestępczością, którego celem jest ochrona bezpieczeństwa wewnętrznego Unii. Ponadto, jak podnosi Komisja, brak elementów transgranicznych nie jest sam w sobie poszlaką pozwalającą wykluczyć wagę naruszenia.

120. Po drugie, jeśli chodzi o kryterium w postaci progu wagi rozpatrywanych przestępstw – które w celu umożliwienia oceny *ex ante* tej wagi należy interpretować w ten sposób, że odnosi się ono do górnej granicy wymiaru kary pozbawienia wolności lub środka zabezpieczającego przewidzianego w ustawie, a nie do kary, jaka może być nałożona w konkretnym przypadku – to, mimo że owo kryterium opiera się ono na progu minimalnej górnej granicy kary, a nie minimalnej dolnej granicy, nie jest samo w sobie nieprzydatne do określenia wystarczającej wagi przestępstwa, która może uzasadniać ingerencję w prawa fundamentalne zapisane w art. 7 i 8 karty, z jaką wiążą się operacje przetwarzania danych przewidziane w dyrektywie PNR. Jednakże moim zdaniem należy je interpretować jako kryterium określające „minimalną” wagę naruszenia. Tak więc, o ile

¹²² Pragnę zauważyć w tym względzie, że pojęcie „przestępstwa międzynarodowego” zdefiniowane na przykład w projekcie umowy PNR Kanada–UE było wystarczająco szerokie, aby obejmować również przestępstwa popełnione w jednym i tym samym państwie, podczas gdy sprawca „przebywa w innym państwie lub też zamierza przemieścić się do innego państwa”, zob. art. 3 ust. 3 lit. e) projektu umowy PNR Kanada–UE, którego brzmienie jest powtórzone w pkt 30 opinii 1/15. Pragnę również zauważyć, że w opinii 1/2011 (pkt 2.2.3.1 i 3.7) FRA zasugerowała ograniczenie systemu PNR Unii wyłącznie do poważnej przestępczości międzynarodowej. Projekt dyrektywy PNR przewidywał natomiast zróżnicowanie przetwarzania w sposób zautomatyzowany w zależności od tego, czy przestępstwo ma charakter transgraniczny, czy nie, zob. art. 4 ust. 2 lit. a) tego projektu.

takie kryterium zakazuje państwom członkowskim uznania za „poważną przestępczość” tych przestępstw ujętych w załączniku II, które zgodnie z ich krajowym prawem karnym są zagrożone karą pozbawienia wolności lub środkiem zabezpieczającym o czasie trwania poniżej trzech lat, o tyle nie zobowiązuje ich do automatycznego uznawania takiej kwalifikacji w odniesieniu do wszystkich przestępstw mogących widnieć w tym załączniku, których zagrożenie karą przekracza próg ustanowiony w art. 3 pkt 9 dyrektywy PNR, jeżeli biorąc pod uwagę specyfikę ich systemu karnego, taka kwalifikacja prowadziłaby do stosowania systemu ustanowionego dyrektywą PNR w celach zapobiegania przestępstwom pospolitym oraz ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania niezgodnie z celami realizowanymi przez ową dyrektywę.

121. Po trzecie, co się tyczy katalogu z załącznika II, należy przede wszystkim zauważyć, że okoliczność, iż dyrektywa PNR wymienia wyczerpująco przestępstwa wchodzące w zakres definicji „poważnej przestępczości”, stanowi podstawową gwarancję formalną i materialną pozwalającą zapewnić zgodność z prawem systemu ustanowionego przez dyrektywę PNR i zagwarantować pasażerom pewność prawa. Należy jednak stwierdzić, że wspomniany katalog obejmuje zarówno przestępstwa, które ze względu na swój charakter odznaczają się bezsprzecznie dużą wagą – jak na przykład handel ludźmi, wykorzystywanie seksualne dzieci i pornografia dziecięca, nielegalny handel bronią, nielegalny handel materiałami jądrowymi lub promieniotwórczymi, bezprawne zawładnięcie statkiem powietrznym lub wodnym, przestępstwa podlegające jurysdykcji Międzynarodowego Trybunału Karnego, zabójstwo, zgwałcenie, uprowadzenie, bezprawne pozbawienie wolności i wzięcie zakładników¹²³ – jak i przestępstwa, w przypadku których tak duża waga jest mniej oczywista, jak, przykładowo, oszustwo, podrabianie i piractwo produktów, fałszowanie dokumentów urzędowych i handel nimi czy handel skradzionymi pojazdami¹²⁴. Ponadto niektóre spośród przestępstw wymienionych w załączniku II mogą ze swej natury częściej mieć charakter transgraniczny, jak na przykład handel ludźmi, nielegalny handel narkotykami lub bronią, wykorzystywanie seksualne dzieci, ułatwianie bezprawnego wjazdu i pobytu, bezprawne zawładnięcie statkiem powietrznym, a także cechować się związkiem z lotniczym przewozem osób.

¹²³ Pragnę ponadto zauważyć, że część przestępstw, o których mowa w załączniku II, wchodzi w zakres dziedzin przestępczości zakwalifikowanej jako „poważna” w art. 83 ust. 1 akapit pierwszy TFUE i wymienionych w akapicie drugim tego ustępu. Jest to w szczególności handel ludźmi oraz seksualne wykorzystywanie dzieci, nielegalny handel narkotykami, nielegalny handel bronią, pranie pieniędzy, korupcja, fałszowanie środków płatniczych, przestępczość komputerowa i przestępczość zorganizowana. W wielu spośród tych dziedzin prawodawca Unii przyjął na podstawie art. 83 ust. 1 TFUE dyrektywy ustanawiające „normy minimalne odnoszące się do definicji przestępstw i określania sankcji”, zob. w szczególności dyrektywa Parlamentu Europejskiego i Rady 2011/36/UE z dnia 5 kwietnia 2011 r. w sprawie zapobiegania handlowi ludźmi i zwalczania tego procederu oraz ochrony ofiar, zastępująca decyzję ramową Rady 2002/629/WSiSW (Dz.U. 2011, L 101, s. 1), dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz.U. 2011, L 335, s. 1; sprostowanie Dz.U. 2012, L 18, s. 7), dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.U. 2013, L 218, s. 8), dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/713 z dnia 17 kwietnia 2019 r. w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi, zastępująca decyzję ramową Rady 2001/413/WSiSW (Dz.U. 2019, L 123, s. 18), dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/1371 z dnia 5 lipca 2017 r. w sprawie zwalczania za pośrednictwem prawa karnego nadużyć na szkodę interesów finansowych Unii (Dz.U. 2017, L 198, s. 29), a także dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1673 z dnia 23 października 2018 r. w sprawie zwalczania prania pieniędzy za pomocą środków prawno-karnych (Dz.U. 2018, L 284, s. 22).

¹²⁴ Pragnę jednak zauważyć, że wszystkie przestępstwa wymienione w załączniku I, z wyjątkiem „szpiegostwa przemysłowego”, znajdują się w art. 2 ust. 2 decyzji ramowej Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami członkowskimi (Dz.U. 2002, L 190, s. 1). Chociaż nie zakwalifikowano ich jako poważnej przestępczości, to jednak w przypadku osiągnięcia tego samego progu zagrożenia karą pozbawienia wolności co przewidziany w art. 3 pkt 9 dyrektywy PNR skutkują one przekazaniem sprawy na podstawie europejskiego nakazu aresztowania bez weryfikacji podwójnej karalności czynu. Prawie wszystkie wspomniane przestępstwa, z wyjątkiem „sabotażu”, „bezprawnego zawładnięcia statkiem powietrznym” i „szpiegostwa przemysłowego”, wymienione są również w załączniku I do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1727 z dnia 14 listopada 2018 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust) oraz zastąpienia i uchylenia decyzji Rady 2002/187/WSiSW (Dz.U. 2018, L 295, s. 138), który zawiera wykaz „form poważnej przestępczości” podlegających właściwości Eurojustu.

122. Jeśli chodzi o wystarczająco jasny i precyzyjny charakter rubryk zawartych w załączniku II, również w tym przypadku poziom jest bardzo zróżnicowany. Tak więc chociaż wykaz zawarty w tym załączniku należy uznać za wyczerpujący, kilka z jego rubryk ma charakter „otwarty”¹²⁵, a inne z kolei odnoszą się do pojęć ogólnych, które mogą obejmować bardzo dużą liczbę przestępstw o różnej wadze, mimo że zawsze z zastrzeżeniem progu górnej granicy kary, przewidzianego w art. 3 pkt 9 dyrektywy PNR¹²⁶.

123. W tym względzie pragnę zauważyć, po pierwsze, że istotne informacje pozwalające na zidentyfikowanie przynajmniej niektórych poważnych przestępstw, które mogą należeć do odpowiednich rubryk załącznika II, dostarczają dyrektywy harmonizujące przyjęte w dziedzinach, o których mowa w art. 83 ust. 1 TFUE, wspomniane w przypisie 123 do niniejszej opinii. I tak, w szczególności, dyrektywa 2013/40 definiuje w art. 3–8 różne przestępstwa objęte pojęciem „cyberprzestępczości”, o którym mowa w pkt 9 tego załącznika II, jednocześnie w każdym przypadku wykluczając czyny stanowiące „przypadki mniejszej wagi”¹²⁷. Podobnie dyrektywa 2019/713 definiuje pewne rodzaje przestępstw oszustwa, a dyrektywa 2017/1371 określa znamiona „nadużyć na szkodę interesów finansowych Unii”. W tym kontekście należy również wspomnieć przyjętą na podstawie art. 175 ust. 1 WE dyrektywę 2008/99/WE w sprawie ochrony środowiska poprzez prawo karne¹²⁸, która definiuje w art. 3 szereg poważnych przestępstw związanych z ochroną środowiska, mogących podlegać rubryce 10 załącznika II, w tym czyny kwalifikujące się jako „nielegalny handel zagrożonymi gatunkami zwierząt oraz zagrożonymi gatunkami i odmianami roślin”, z wyłączeniem czynów mających nieznaczný wpływ na chronione dobro. Wreszcie, przypomnę dyrektywę 2002/90/WE¹²⁹, która definiuje ułatwianie nielegalnego wjazdu, tranzytu i pobytu, decyzję ramową 2002/946/WSiSW¹³⁰ mającą na celu wzmocnienie systemu karnego w celu ścigania tych przestępstw, decyzję ramową 2003/568/WSiSW¹³¹, która definiuje przestępstwa kwalifikowane jako „czynna i bierna korupcja w sektorze prywatnym”, oraz decyzję ramową 2008/841/WSiSW¹³², która definiuje przestępstwa związane z udziałem w organizacji przestępczej.

124. Po drugie, pragnę zauważyć, że jak słusznie wskazała Komisja, w braku pełnej harmonizacji materialnego prawa karnego nie można zarzucić prawodawcy Unii, że nie sprecyzował on w większym stopniu przestępstw, o których mowa w załączniku II. Tym samym, w odróżnieniu od tego, co stwierdzę w niniejszej opinii w odniesieniu do wykazu danych PNR zawartego w załączniku I, transpozycja do prawa krajowego katalogu przestępstw z załącznika II wymaga w sposób nieunikniony określenia przez państwa członkowskie odnośnych przestępstw w zależności od specyfiki ich systemów karnych. Działanie to należy jednak przeprowadzić z pełnym poszanowaniem kryterium, zgodnie z którym wszelkie ingerencje w prawa podstawowe ustanowione w art. 7 i 8 karty powinny być ograniczone do tego, co absolutnie konieczne. I tak na przykład, nie jest moim zdaniem wykluczone, że państwa członkowskie ograniczą wykorzystywanie danych PNR w odniesieniu do określonych przestępstw, takich jak na przykład

¹²⁵ Chodzi w szczególności o pkt 7, 8, 10 i 16.

¹²⁶ Jest tak na przykład w przypadku „oszustwa” (pkt 7), „korupcji” (pkt 6), „przestępczości komputerowej i cyberprzestępczości” (pkt 9) „przestępstw przeciwko środowisku” (pkt 10). To właśnie nad przestępstwami oszustwa zastanawia się Verwaltungsgericht Wiesbaden (sąd administracyjny w Wiesbaden, Niemcy) w zawieszłej sprawie C-215/20.

¹²⁷ Dyrektywa ta precyzuje ponadto w art. 9 minimalną górną granicę kary pozbawienia wolności, której podlegają wspomniane przestępstwa, który to próg jedynie w pewnych okolicznościach wynosi trzy lata.

¹²⁸ Dyrektywa Parlamentu Europejskiego i Rady z dnia 19 listopada 2008 r. (Dz.U. 2008, L 328, s. 28).

¹²⁹ Dyrektywa Rady z dnia 28 listopada 2002 r. definiująca ułatwianie nielegalnego wjazdu, tranzytu i pobytu (Dz.U. 2002, L 328, s. 17).

¹³⁰ Decyzja ramowa Rady z dnia 28 listopada 2002 r. w sprawie wzmocnienia systemu karnego w celu zapobiegania ułatwianiu nielegalnego wjazdu, tranzytu i pobytu (Dz.U. 2002, L 328, s. 1).

¹³¹ Decyzja ramowa Rady z dnia 22 lipca 2003 r. w sprawie zwalczania korupcji w sektorze prywatnym (Dz.U. 2003, L 192, s. 54).

¹³² Decyzja ramowa Rady z dnia 24 października 2008 r. w sprawie zwalczania przestępczości zorganizowanej (Dz.U. 2008, L 300, s. 42).

wskazane w pkt 7, 16, 17, 18, 25 załącznika II, do przypadków, w których przestępstwa te mają charakter transgraniczny lub zostały popełnione w ramach organizacji przestępczej, lub też w których występują pewne okoliczności obciążające. Do sądów państw członkowskich, pod kontrolą Trybunału, należy wykładnia przepisów krajowych transponujących wspomniany katalog do prawa krajowego w sposób zgodny zarówno z dyrektywą PNR, jak i z kartą, tak aby przetwarzanie danych PNR było w odniesieniu do każdej rubryki ograniczone do przestępstw, które odznaczają się dużą wagą wymaganą przez tę dyrektywę, jak również do przestępstw, w odniesieniu do których takie przetwarzanie jest istotne¹³³.

125. Z zastrzeżeniem uściśleń dokonanych w pkt 120 i 124 niniejszej opinii uważam, że art. 3 pkt 9 dyrektywy PNR oraz katalog przestępstw znajdujący się w załączniku II do tej dyrektywy spełniają wymogi jasności i precyzji oraz nie wykraczają poza granice tego, co absolutnie konieczne.

126. Należy jednak przyznać, że rozwiązanie przedstawione w pkt 124 niniejszej opinii nie jest w pełni zadowalające. Po pierwsze bowiem, pozostawia ono państwom członkowskim znaczny zakres uznania, przez co przedmiotowy zakres stosowania przetwarzania danych PNR może znacząco różnić się w poszczególnych państwach członkowskich, stojąc w sprzeczności z celem harmonizacji, do którego dąży prawodawca Unii¹³⁴. Po drugie, rozwiązanie to oznacza, że kontrola proporcjonalności w odniesieniu do zasadniczego elementu systemu, takiego jak ograniczenie celów tego przetwarzania, jest wykonywana ex post w stosunku do krajowych środków transpozycji, a nie ex ante względem samej dyrektywy PNR. Zatem gdyby Trybunał zdecydował się, jak proponuję, uznać art. 3 pkt 9 dyrektywy PNR, a także katalog przestępstw zawarty w załączniku II do tej dyrektywy za zgodny z art. 7, 8 i 51 ust. 2 karty, byłoby dobrze, aby zwrócił on uwagę prawodawcy Unii na fakt, że taka ocena jest jedynie tymczasowa i wymaga od prawodawcy weryfikacji w świetle dokonanej przez państwa członkowskie transpozycji tego przepisu i rzeczonego katalogu, a także na podstawie danych statystycznych, o których mowa w art. 20 dyrektywy PNR, czy nie jest konieczne: po pierwsze, doprecyzowanie kategorii przestępstw, o których mowa w tym katalogu, poprzez ograniczenie ich zakresu; po drugie, usunięcie z niego przestępstw, w odniesieniu do których przetwarzanie danych PNR okazuje się albo nieproporcjonalne, albo nieistotne lub nieskuteczne; po trzecie, wskazanie progu wagi przestępstw, o których mowa w art. 3 pkt 9 dyrektywy PNR¹³⁵. W tym względzie pragnę zauważyć, że o ile art. 19 ust. 2 lit. b) dyrektywy PNR nakłada na Komisję obowiązek dokonania przeglądu wszystkich elementów tej dyrektywy, ze szczególnym uwzględnieniem „konieczności i proporcjonalności gromadzenia i przetwarzania danych PNR w odniesieniu do każdego celu” w niej określonego, o tyle ani sprawozdanie Komisji z 2020 r., ani towarzyszący mu dokument roboczy z 2020 r. nie zawiera moim zdaniem zadowalającej analizy tego zagadnienia.

ii) W przedmiocie kategorii danych PNR objętych dyrektywą PNR (pytania prejudycjalne drugie i trzecie)

127. Dyrektywa PNR przewiduje przekazywanie do JIP 19 kategorii danych PNR gromadzonych przez przewoźników lotniczych na potrzeby rezerwacji lotów. Kategorie te, wymienione w załączniku I, odpowiadają kategoriom funkcjonującym w systemach rezerwacji linii lotniczych

¹³³ Zobacz w szczególności motyw 7 i 22 dyrektywy PNR.

¹³⁴ Zobacz motyw 35 dyrektywy PNR.

¹³⁵ Zobacz analogicznie wyroki: z dnia 16 grudnia 2008 r., Arcelor Atlantique et Lorraine i in. (C-127/07, EU:C:2008:728, pkt 61, 62); z dnia 17 października 2013 r., Schaible (C-101/12, EU:C:2013:661, pkt 91, 94).

i kategoriom wymienionym w załączniku I do wytycznych dotyczących danych PNR, przyjętych przez Organizację Międzynarodowego Lotnictwa Cywilnego (ICAO) w 2010 r.¹³⁶ (zwanym dalej „wytycznymi ICAO”).

128. W drugim pytaniu prejudycjalnym sąd odsyłający zastanawia się nad ważnością załącznika I w świetle art. 7, 8 i art. 52 ust. 1 karty, biorąc pod uwagę, po pierwsze, zakres danych osobowych wymienionych w tym załączniku – a w szczególności danych API, o których mowa w pkt 18 tego załącznika, w zakresie, w jakim wykraczają one poza dane wymienione w art. 3 ust. 2 dyrektywy API – a po drugie, nad kwestią tego, czy dane te, rozpatrywane łącznie, nie ujawniają danych szczególnie chronionych i nie wykraczają poza to, co „absolutnie konieczne”. W trzecim pytaniu prejudycjalnym – które dotyczy, jak już miałem okazję podkreślić, poszanowania pierwszego z trzech warunków określonych w art. 52 ust. 1 karty, zgodnie z którym każda ingerencja w prawo podstawowe musi być „przewidziana ustawą” – Cour constitutionnelle (trybunał konstytucyjny) zwraca się do Trybunału z pytaniem o ważność pkt 12 i 18 załącznika I, zważywszy w szczególności na ich „otwarty” charakter.

129. Ponieważ badanie, jakie należy przeprowadzić w ramach drugiego pytania prejudycjalnego, zakłada wcześniejsze zbadanie wystarczająco jasnego i precyzyjnego charakteru kategorii danych osobowych, o których mowa w załączniku I, w pierwszej kolejności zajmę się trzecim pytaniem prejudycjalnym.

– *W przedmiocie wystarczająco jasnego i precyzyjnego charakteru pkt 12 i 18 załącznika I (trzecie pytanie prejudycjalne)*

130. Tytułem wstępu należy zauważyć, że zakres i waga ingerencji w prawa podstawowe ustanowione w art. 7 i 8 karty, jaką stanowi środek wprowadzający ograniczenia w wykonywaniu tych praw, zależą przede wszystkim od zakresu i charakteru danych osobowych, które stanowią przedmiot przetwarzania. Określenie tych danych stanowi zatem element zasadniczy, który musi być zrealizowany w każdym akcie stanowiącym podstawę prawną takiego środka w sposób możliwie najbardziej jasny i precyzyjny.

131. W odniesieniu do przetwarzania danych PNR wymóg ten został uznany w opinii 1/15. W opinii tej Trybunał, odnosząc się do rubryk znajdujących się w załączniku do projektu umowy PNR Kanada–UE, zawierającym wykaz danych PNR objętych przewidywaną umową, stwierdził w szczególności, że posłużenie się ogólnymi kategoriami informacji, które nie określają w wystarczającym stopniu zakresu danych podlegających przekazaniu, a także posłużenie się przykładowymi wykazami danych w żaden sposób nieograniczającymi charakteru i zakresu informacji, które mogą znaleźć się w danej rubryce, nie spełnia wymogów jasności i precyzji.

132. Trzecie pytanie prejudycjalne należy rozpatrzyć w świetle tych właśnie zasad.

¹³⁶ Zobacz dokument 9944, zatwierdzony przez Sekretarza Generalnego ICAO i opublikowany pod jego zwierzchnictwem. Wersja w języku francuskim tego dokumentu jest dostępna pod adresem: https://www.icao.int/Security/FAL/ANNEX9/Documents/9944_cons_fr.pdf. Zgodnie z pkt 9.22 załącznika 9 (Ułatwienia) do Konwencji o międzynarodowym lotnictwie cywilnym podpisanej w Chicago dnia 7 grudnia 1944 r. (zwanej dalej „konwencją z Chicago”) państwa będące stronami tej konwencji, wymagające danych PNR, mają obowiązek dostosowania swoich wymogów dotyczących gromadzenia i przetwarzania tych danych do wskazanych wytycznych.

133. Jeśli chodzi o pkt 12 załącznika I, ma on następujące brzmienie:

„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)”.

134. Ponieważ punkt ten dotyczy „uwag ogólnych”, stanowi on, podobnie jak rubryka 17 załącznika do projektu umowy PNR Kanada–UE, pozycję „tekstu dowolnego”, służącą ujęciu wszelkich informacji zebranych przez przewoźników lotniczych w ramach ich działalności usługowej, w uzupełnieniu informacji wyraźnie wymienionych w innych punktach załącznika I. Należy zaś stwierdzić, jak uczynił to Trybunał w pkt 160 opinii 1/15, że rubryka tego rodzaju „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, ponieważ uściślenie w nawiasach zawarte w pkt 12 załącznika I, dotyczącym informacji o małoletnim bez opieki, zostało podane jedynie tytułem przykładu, o czym świadczy użycie terminu „takie jak”, punkt ten nie ustanawia żadnego ograniczenia co do charakteru i zakresu informacji, które mogą w nim figurować¹³⁷.

135. W tym stanie rzeczy nie można uznać, że pkt 12 załącznika I jest zakresłony w sposób wystarczająco jasny i precyzyjny.

136. O ile Komisja i Parlament wydają się podzielać ten wniosek, o tyle państwa członkowskie, które przedstawiły uwagi w przedmiocie trzeciego pytania prejudycjalnego, a także Rada sprzeciwiają się mu, wysuwając argumenty, które w znacznym stopniu się pokrywają.

137. W pierwszej kolejności pierwsza seria argumentów zmierza, ogólnie rzecz biorąc, do podważenia możliwości zastosowania w niniejszej sprawie wniosków, do których Trybunał doszedł w opinii 1/15.

138. W tym względzie, mając świadomość różnicy kontekstu charakteryzującego obie sprawy, ograniczę się w tym miejscu do stwierdzenia, że wniosek, do którego doszedł Trybunał w pkt 160 opinii 1/15 w odniesieniu do rubryki 17 załącznika do projektu umowy PNR Kanada–UE, opierał się wyłącznie na wykładni semantycznej i strukturalnej tej rubryki. Taką wykładnię można zaś doskonale przenieść na grunt pkt 12 załącznika I, którego brzmienie jest w części nieprzykładowej identyczne z brzmieniem owej rubryki i ma analogiczną strukturę. Ponadto, jak zobaczymy bardziej szczegółowo poniżej, obie omawiane zasady sytuują się w tym samym wielostronnym kontekście prawnym, złożonym w szczególności z wytycznych ICAO, do których Trybunał zresztą odniósł się wyraźnie w pkt 156 opinii 1/15. W tych okolicznościach nie tylko nic nie stoi na przeszkodzie temu, aby w odniesieniu do pkt 12 załącznika I przyjąć taką samą wykładnię, jaką Trybunał przyjął w pkt 160 opinii 1/15 w odniesieniu do rubryki 17 załącznika do projektu umowy PNR Kanada–UE, ale przede wszystkim nie ma żadnych powodów, aby od niej odejść.

¹³⁷ Podobnie zob. opinia 1/15, pkt 160.

139. W drugiej kolejności wiele państw członkowskich podkreśla, że poszczególne punkty załącznika I, w tym pkt 12, odpowiadają rubrykom załącznika I do wytycznych ICAO, które przewoźnicy lotniczy dobrze znają i którym potrafią przyporządkować konkretną treść. Ów punkt 12 odpowiada w szczególności dwóm ostatnim rubrykom wspomnianego załącznika, zatytułowanym, odpowiednio, „Uwagi ogólne” i „Tekst dowolny/pola kodów w OSI [Other Supplementary Information], SSR [Special Service Request], SSI [Special Service Information], Uwagi/dane historyczne”, a dotyczącym „informacji dodatkowych” lub „dotyczących żądanych usług”¹³⁸.

140. W tym względzie pragnę zauważyć przede wszystkim, że zgodność między rubrykami załącznika I do projektu umowy PNR Kanada–UE z jednej strony a rubrykami załącznika I do wytycznych ICAO z drugiej strony nie przeszkodziła Trybunałowi stwierdzić w opinii 1/15, że niektóre rubryki znajdujące się w załączniku I do owego projektu umowy nie spełniają wymogów jasności i precyzji, którym powinien odpowiadać środek ograniczający wykonywanie praw podstawowych. Następnie pragnę zauważyć, że wbrew temu, co wydają się sugerować niektóre państwa członkowskie, odesłanie do wytycznych ICAO, zresztą nie w sposób wyraźny¹³⁹, nie pozwala na lepsze sprecyzowanie charakteru i zakresu informacji objętych ewentualnie pkt 12 załącznika I. Wręcz przeciwnie, lektura tych wytycznych tym bardziej każe myśleć, że rubryka z „tekstem dowolnym”, taka jak wspomniany pkt 12, obejmuje bliżej nieokreśloną ilość różnorodnych informacji, które ponadto mogą wykraczać poza informacje uwzględniane z urzędu w PNR¹⁴⁰.

141. W trzeciej kolejności trzeba zauważyć, że zdaniem niektórych rządów na państwach członkowskich spoczywa obowiązek sprecyzowania informacji, które mogą odpowiadać pkt 12 załącznika I, za pomocą wewnętrznych środków ustawodawczych, z poszanowaniem ograniczeń określonych w art. 7, 8 i art. 52 ust. 1 karty. W istocie bowiem dyrektywa z definicji pozostawia państwom członkowskim zakres uznania co do środków koniecznych do wdrożenia ustanowionych w niej norm.

142. W tym względzie jestem zdania, jak już wskazałem w pkt 86 niniejszej opinii, że w przypadku gdy środki prowadzące do ingerencji w prawa podstawowe ustanowione w karcie mają swoje źródło w akcie ustawodawczym Unii, do prawodawcy Unii należy określenie dokładnego zakresu tych ingerencji z poszanowaniem wspomnianych powyżej kryteriów jasności i precyzji, a także zasady proporcjonalności. Wynika z tego, że jeżeli instrumentem wybranym przez prawodawcę jest dyrektywa, to moim zdaniem nie dochodzi do oddelegowania na państwa członkowskie zadania określenia w ramach transpozycji tej dyrektywy do ich praw krajowych istotnych elementów definiujących zakres ingerencji, takich jak, w odniesieniu do ograniczeń praw podstawowych określonych w art. 7 i 8 karty, charakter i zakres danych osobowych podlegających przetwarzaniu.

143. W czwartej kolejności niektóre państwa członkowskie zauważają, że pkt 12 załącznika I należy rozumieć w ten sposób, iż dotyczy on wyłącznie informacji mających związek ze świadczeniem usługi przewozu. Przy takiej wykładni punkt ów jest zgodny z art. 7, 8 i art. 52 ust. 1 karty.

¹³⁸ Zobacz pkt 2.1.2, 2.1.5 wytycznych ICAO [tłumaczenie nieoficjalne, tak jak dalsze cytaty z tych wytycznych].

¹³⁹ Jedyne odniesienie do wytycznych ICAO w dyrektywie PNR znajduje się w jej motywie 17 i dotyczy tylko „formatów danych [...] obsługiwanych na potrzeby przekazywania danych PNR przez przewoźników lotniczych państwom członkowskim”.

¹⁴⁰ I tak, pkt 2.1.5 wspomnianych wytycznych wymienia „informacje dodatkowe” lub „dotyczące żądanych usług”, które mogą odnosić się do „prośb o opiekę medyczną lub posiłki specjalne, »małoletnich podróżujących samodzielnie«, prośb o pomoc, itp.”. Punkt 2.1.6 wyjaśnia natomiast, że „pole »uwagi ogólne« może również zawierać » pewne informacje, takie jak korespondencja lub wewnętrzne kontakty między pracownikami przedsiębiorstw lotniczych i agentami rezerwacji”.

144. Również i to twierdzenie mnie nie przekonuje. Przede wszystkim informacje, które mogą znaleźć się w rubryce „uwagi ogólne” oraz pod kodami OSI, SSI i SSR, mają bowiem bardzo różnorodny charakter (opieka medyczna, specjalne posiłki lub preferencje żywnościowe, wszelkie prośby o pomoc, informacje dotyczące małoletnich podróżujących samodzielnie itd.)¹⁴¹, przy czym wszystkie są związane z usługą przewozu, ponieważ służą w szczególności do tego, aby umożliwić przewoźnikowi lotniczemu dostosowanie tej usługi do wymogów poszczególnych pasażerów. Kryterium interpretacyjne oparte na istotności tych informacji dla usługi przewozu nie pozwala zatem na dalsze doprecyzowanie zakresu tego punktu 12. Następnie pragnę zauważyć, że Trybunał, chociaż zastosował to kryterium w pkt 159 opinii 1/15 w celu dokonania wykładni zgodnej z wymogiem jasności i precyzji innej rubryki załącznika do projektu umowy PNR Kanada–UE, to jednak wykluczył taką możliwość w odniesieniu do rubryki 17 owego załącznika, odpowiadającej pkt 12 załącznika I.

145. W piątej kolejności niektóre państwa członkowskie kładą nacisk na fakt, że informacje, które może obejmować pkt 12 załącznika I, są przekazywane przewoźnikom lotniczym dobrowolnie przez samych pasażerów, należycie poinformowanych o dalszym przekazywaniu tych danych organom publicznym. Koncepcja leżąca u podstaw takiego argumentu, jak mi się wydaje, polega na założeniu istnienia swego rodzaju dorozumianej zgody danego pasażera na to, aby dane dostarczone przez niego przedsiębiorstwom lotniczym były następnie przekazywane organom władzy publicznej.

146. W tym względzie Trybunał miał już okazję wyjaśnić, że nie może być mowy o „zgodzie”, jeżeli osoba, której dane dotyczą, nie może swobodnie sprzeciwić się przetwarzaniu jej danych osobowych¹⁴². Tymczasem w przypadku znacznej części informacji, które mogą znaleźć się w pkt 12 załącznika I, zainteresowany pasażer nie ma realnego wyboru, lecz musi je dostarczyć, aby móc skorzystać z usługi przewozu. Jest tak w szczególności w przypadku osób niepełnosprawnych lub o ograniczonej mobilności, a także osób wymagających opieki medycznej lub małoletnich bez opieki. Przypominam ponadto, że w pkt 142 i 143 opinii 1/15 Trybunał wyraźnie stwierdził, iż przetwarzania danych PNR przez organy publiczne, realizującego inny cel niż cel, dla którego dane te są gromadzone przez przewoźników lotniczych, nie można uznać za uzasadnione jakąkolwiek formą zgody udzielonej przez pasażerów na ich gromadzenie.

147. Wreszcie, większość państw członkowskich podnosi, że przetwarzanie danych przewidziane w dyrektywie PNR jest obwarowane wieloma gwarancjami, do których należy, w odniesieniu do przekazywania danych do JIP, obowiązek usuwania przez te organy danych niewymienionych w załączniku I, a także danych mogących wskazywać pochodzenie rasowe lub etniczne danej osoby, jej opinie polityczne, religię lub przekonania filozoficzne, przynależność do związku zawodowego, stan zdrowia, życie seksualne lub orientację seksualną.

148. W tym względzie na wstępie pragnę zaznaczyć, że moim zdaniem ocenę wystarczająco jasnego i precyzyjnego charakteru przepisów określających zakres i charakter danych, które mogą być przedmiotem przekazania organom władzy publicznej, w celu ustalenia, czy środek powodujący ingerencję w prawa podstawowe określone w art. 7 i 8 karty jest zgodny z zasadami legalności i pewności prawa, należy przeprowadzić bez uwzględnienia gwarancji związanych z przetwarzaniem, któremu dane te zostaną poddane przez rzeczne organy, jako że środki te bierze się pod uwagę jedynie przy badaniu proporcjonalności rozpatrywanego środka. W ten

¹⁴¹ Zobacz pkt 2.1.5 i 2.1.6 wytycznych ICAO.

¹⁴² Zobacz wyrok z dnia 17 października 2013 r., Schwarz (C-291/12, EU:C:2013:670, pkt 32), dotyczący przypadku osoby występującej o paszport, która, aby móc dysponować dokumentem umożliwiającym jej przemieszczanie się do państwa trzeciego, musi poddać się pobraniu odcisków palców.

zresztą sposób Trybunał dokonał w pkt 155–163 opinii 1/15 oceny rubryk w projekcie umowy PNR Kanada–UE. W sposób bardziej ogólny chciałbym zaś dodać, że szczególną uwagę należy zwrócić na konieczność zachowania wyraźnego rozróżnienia między poszczególnymi etapami analizy środka ingerującego w prawa podstawowe, ponieważ zatarcie granic tych różnych etapów moim zdaniem jest zawsze szkodliwe dla skutecznej ochrony tychże praw.

149. Niezależnie od tego ograniczę się w tym miejscu do stwierdzenia, po pierwsze, że obowiązek usuwania danych innych niż wymienione w załączniku I, ciążyący na JIP zgodnie z art. 6 ust. 1 dyrektywy PNR, ma sens tylko wtedy, gdy załącznik ten zawiera jasny i zamknięty katalog danych podlegających przekazaniu. To samo dotyczy określonego w art. 13 ust. 4 dyrektywy PNR obowiązku usuwania przez JIP danych określanych jako „szczególnie chronione”¹⁴³. Zbyt niekonkretna, nieprecyzyjna lub otwarta definicja informacji, które należy przekazać, zwiększa bowiem zarówno prawdopodobieństwo tego, że takie dane staną się pośrednio przedmiotem przekazania, jak i ryzyko, że nie będą natychmiast zidentyfikowane i usunięte. Innymi słowy, wspomniane gwarancje mogą skutecznie spełniać swoją funkcję tylko wtedy, gdy zasady określające charakter i zakres danych PNR, które przewoźnicy lotniczy przekazują do JIP, są wystarczająco jasne i precyzyjne, a wykaz tych danych ma charakter zamknięty i wyczerpujący.

150. Na podstawie całości powyższych rozważań i zgodnie z moją wcześniejszą zapowiedzią w pkt 135 niniejszej opinii jestem zdania, że pkt 12 załącznika I, w części, w której wśród danych przekazywanych do JIP przez przewoźników lotniczych zgodnie z dyrektywą PNR ujemuje „uwagi ogólne”, nie spełnia wymogów jasności i precyzji przewidzianych w art. 52 ust. 1 karty, zgodnie z jego wykładnią dokonaną przez Trybunał¹⁴⁴, a w związku z tym należy go uznać w tym zakresie za nieważny.

151. W swoich uwagach na piśmie Komisja i Parlament zasugerowały Trybunałowi, aby posłużył się raczej „wykładnią zgodną” pkt 12 załącznika I, odczytując go w ten sposób, że dotyczy on jedynie informacji o małoletnim, które są tam wyraźnie wymienione w nawiasach. Przyznaję, że trudno byłoby mi uznać, iż taka interpretacja respektowałaby granice zwykłej wykładni zgodnej. Niewątpliwie, zgodnie z ogólną zasadą wykładni akt prawny Unii powinien być interpretowany, tak dalece, jak to możliwe, w sposób, który nie podważa jego ważności, i w zgodzie z całością prawa pierwotnego, w tym w szczególności z postanowieniami karty¹⁴⁵. Nie ulega też wątpliwości, że w przypadku dyrektywy PNR takiej wykładni, jak się wydaje, sprzyja nacisk położony w szczególności w wielu motywach tej dyrektywy na pełne poszanowanie praw podstawowych, prawa do poszanowania życia prywatnego oraz zasady proporcjonalności¹⁴⁶. Jednakże z utrwalonego orzecznictwa wynika również, że wykładnia zgodna jest dopuszczalna tylko wtedy, gdy przepis wtórnego prawa Unii można interpretować na więcej niż jeden ze sposobów, a zatem można dać pierwszeństwo wykładni zapewniającej zgodność tych przepisów z prawem pierwotnym, a nie wykładni prowadzącej do stwierdzenia jego niezgodności z nim¹⁴⁷.

¹⁴³ Powróć do tej kategorii danych w dalszej części niniejszej opinii.

¹⁴⁴ FRA wyraziła się podobnie w swojej opinii 1/2011, s. 13. W swojej opinii z dnia 25 marca 2011 r. w sprawie projektu dyrektywy PNR, https://edps.europa.eu/sites/edp/files/publication/11-03-25_pnr_en.pdf, pkt 47 (zwanej dalej „opinią EIOD z dnia 25 marca 2011 r.”), EIOD zaproponował wyłączenie rubryki „Uwagi ogólne” z wykazu znajdującego się w załączniku I.

¹⁴⁵ Zobacz w szczególności wyroki: z dnia 19 listopada 2009 r., *Sturgeon i in.* (C-402/07 i C-432/07, EU:C:2009:716, pkt 47 i przytoczone tam orzecznictwo); z dnia 19 września 2013 r., *Komisja/Strack* (Szczególna procedura kontroli orzeczenia) (C-579/12 RX-II, EU:C:2013:570, pkt 40); a także z dnia 14 maja 2019 r., *M i in.* (Cofnięcie statusu uchodźcy) (C-391/16, C-77/17 i C-78/17, EU:C:2019:403, pkt 77 i przytoczone tam orzecznictwo).

¹⁴⁶ Zobacz w szczególności motyw 5, 7, 11, 15, 16, 20, 22, 23, 25, 27, 28, 31, 36 i 37 dyrektywy PNR.

¹⁴⁷ Zobacz wyroki: z dnia 26 czerwca 2007 r., *Ordre des barreaux francophones et germanophone i in.* (C-305/05, EU:C:2007:383, pkt 28); a także z dnia 14 maja 2019 r., *M i in.* (Cofnięcie statusu uchodźcy) (C-391/16, C-77/17 i C-78/17, EU:C:2019:403, pkt 77).

152. Tymczasem pkt 12 załącznika I nie można moim zdaniem interpretować w sposób sugerowany przez Komisję i Parlament, gdyż byłaby to wykładnia „contra legem”. Punkt ten dotyczy bowiem, jak wskazałem powyżej, szerokiej kategorii danych o różnorodnym charakterze i a priori niemożliwych do zidentyfikowania, w której dane dotyczące małoletnich stanowią jedynie podkategorię. Odczytanie owego punktu jako odnoszącego się tylko do tejże podkategorii oznaczałoby nie tylko pominięcie części jego treści, ale także zburzyłoby porządek logiczny tego punktu. Taką czynność, która polegałaby zasadniczo na usunięciu tej części treści pkt 12 załącznika I, którą uznaje się za niezgodną z wymogami jasności i precyzji, można moim zdaniem przeprowadzić jedynie poprzez stwierdzenie częściowej nieważności.

153. Co się tyczy pozostałej części pkt 12 załącznika I, który wymienia szereg danych dotyczących małoletnich bez opieki, jestem zdania, że spełnia ona wymogi jasności i precyzji, pod warunkiem interpretowania jej w taki sposób, że część ta obejmuje wyłącznie informacje dotyczące małoletnich bez opieki, które mają bezpośredni związek z danym lotem i są wyraźnie wymienione w tym punkcie.

154. Co się tyczy pkt 18 załącznika I, ma on następujące brzmienie:

„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)”.

155. Punkt ten ma strukturę analogiczną do struktury pkt 12 załącznika I. Określa on również ogólną kategorię danych, a mianowicie uprzednie informacje o pasażerach (Advance Passenger Information – API), po czym przedstawia w nawiasach wykaz danych, które uznaje się za objęte tą kategorią ogólną, mający charakter wyłącznie przykładowy, o czym świadczy użycie wyrażenia „w tym”.

156. Jednakże, w przeciwieństwie do pkt 12 załącznika I, jego pkt 18 odsyła do kategorii danych, które można lepiej zidentyfikować zarówno pod kątem ich rodzaju, jak i zakresu. Z motywu 4 dyrektywy PNR wynika bowiem, że tam, gdzie dyrektywa odnosi się do tej kategorii danych, odwołuje się ona do informacji, które zgodnie z dyrektywą API, do której motyw ten wyraźnie odsyła, są przekazywane przez przewoźników lotniczych właściwym organom krajowym w celu ulepszenia kontroli granicznych i zwalczania nielegalnej imigracji. Dane te wymieniono w art. 3 ust. 2 tej ostatniej dyrektywy.

157. Ponadto z motywu 9¹⁴⁸ dyrektywy PNR oraz z art. 3 ust. 2 dyrektywy API i przykładowego wykazu zawartego w pkt 18 załącznika I wynika, że dane API, o których mowa w tym punkcie, są to, po pierwsze, dane biograficzne umożliwiające weryfikację tożsamości pasażera lotniczego, a po drugie, dane dotyczące zarezerwowanego lotu. Jeśli chodzi konkretnie o pierwszą z tych kategorii,

¹⁴⁸ Co się tyczy niniejszej sprawy, motyw 9 przewiduje, że „[w]ykorzystywanie danych PNR wraz z danymi API stanowi wartość dodaną w zakresie pomocy państwom członkowskim w weryfikacji tożsamości osób, zwiększając tym samym przydatność wyników tych działań dla ścigania przestępczości i minimalizując ryzyko dokonywania sprawdzeń i prowadzenia postępowań przygotowawczych w stosunku do osób niewinnych”.

czyli dane biograficzne, informacje wymienione w art. 3 ust. 2 dyrektywy API i w pkt 18 załącznika I obejmują dane generowane przy rejestracji, które można pobrać z fragmentu paszportu (lub innego dokumentu podróży) nadającego się do odczytu maszynowego¹⁴⁹.

158. I tak, pkt 18 załącznika I, interpretowany w świetle motywów 4 i 9 dyrektywy PNR, określa charakter danych, których dotyczy, co do zasady w sposób wystarczająco jasny i precyzyjny.

159. Co się tyczy ich zakresu, należy stwierdzić, po pierwsze, że art. 3 ust. 2 dyrektywy API również sformułowano w sposób „otwarty”, ponieważ znajdujący się w nim wykaz jest poprzedzony wyrażeniem „informacje określone powyżej zawierają”¹⁵⁰, a po drugie, że kategoria danych API zdefiniowana w wielostronnych instrumentach harmonizacji w tej dziedzinie obejmuje również dane inne niż te, o których mowa zarówno w dyrektywie API, jak i w pkt 18 załącznika I¹⁵¹.

160. W tych okolicznościach, aby pkt 18 załącznika I odpowiadał wymogom jasności i precyzji stawianym podstawom prawnym ingerencji w art. 7 i 8 karty, należy go interpretować w ten sposób, że obejmuje on jedynie te dane API, które są wyraźnie wymienione w tym punkcie oraz w art. 3 ust. 2 dyrektywy API, przy czym zostały one zebrane przez przewoźników lotniczych w normalnym toku ich działalności¹⁵².

161. Na tym etapie należy pokrótce omówić pozostałe punkty załącznika I, które ze względu na swoje brzmienie mają również charakter „otwarty” lub niewystarczająco precyzyjny, nawet jeśli sąd odsyłający nie zwrócił się do Trybunału wprost z pytaniami na ich temat¹⁵³.

162. Odnosząc się najpierw do pkt 5 załącznika I, wymieniającego „adres i dane kontaktowe (numer telefonu, adres e-mail)”, należy stwierdzić, że chociaż odnosi się on jedynie do danych kontaktowych wyraźnie wymienionych w nawiasach, a zatem ma charakter wyczerpujący, nie precyzuje jednak – inaczej niż odnośna rubryka projektu umowy PNR Kanada–UE¹⁵⁴ – czy dane te odnoszą się jedynie do podróżnego, czy też do osób trzecich, które dokonały rezerwacji lotu dla pasażera lotniczego, do osób trzecich, za pośrednictwem których można się skontaktować z danym pasażerem lotniczym, lub nawet osób trzecich, które należy informować w nagłych przypadkach¹⁵⁵. Biorąc pod uwagę fakt, że wykładnia pkt 5 załącznika I, zgodnie z którą obejmuje on również wyżej wymienione kategorie osób trzecich, rozszerzałaby ingerencję wprowadzoną

¹⁴⁹ Zobacz podobnie również projekt dyrektywy PNR, s. 7, pkt 1. Te same dane znajdują się w wytycznych dotyczących uprzednich informacji o pasażerach (API) opracowanych przez Światową Organizację Celną (WCO), Międzynarodowe Zrzeszenie Przewoźników Powietrznych (IATA) i ICAO, http://www.wcoomd.org/~media/wco/public/fr/pdf/topics/facilitation/instruments-and-tools/tools/api-guidelines-and-pnr-doc/api-guidelines-_f.pdf?db=web [(zwanych dalej „wytycznymi API”, pkt 8.1.5, lit. a)], jako „główne elementy danych, które mogą znajdować się w strefie odczytu maszynowego w urzędowych dokumentach podróży” [tłumaczenie nieoficjalne].

¹⁵⁰ Artykuł 3 ust. 2 dyrektywy API stanowi, co następuje: „Informacje określone powyżej zawierają: numer i rodzaj wykorzystanego dokumentu podróży, obywatelstwo, pełne imię i nazwisko, data urodzenia, przejście graniczne wejścia na terytorium państw członkowskich, kod transportu, czas wylotu i przylotu tego transportu, całkowita liczba pasażerów tego transportu, punkt początkowy załadunku”. Warto podkreślić, że w swoim programie prac na rok 2022, COM(2021) 645 final, s. 9, Komisja przewidziała aktualizację dyrektywy API. We wrześniu 2020 r. instytucja ta opublikowała ocenę tej dyrektywy, stanowiącą podstawę jej przyszłego przeglądu, w dokumencie SWD (2020), 174 final (zwanym dalej „dokumentem roboczym z 2020 r. dotyczącym dyrektywy API”). We wspomnianym dokumencie Komisja podkreśla w szczególności fakt, że wykaz danych zawarty w art. 3 ust. 2 dyrektywy API nie jest zgodny z międzynarodowymi standardami dotyczącymi danych API, zwłaszcza ze względu na to, że nie obejmuje wszystkich danych znajdujących się w części dokumentów tożsamości nadającej się do odczytu maszynowego (zob. w szczególności s. 48).

¹⁵¹ Zobacz wytyczne API, pkt 8.1.5 lit. b) i c).

¹⁵² Analogiczną wykładnię odpowiedniej rubryki projektu umowy PNR Kanada–UE można znaleźć w pkt 161 opinii 1/15.

¹⁵³ Pragnę zauważyć, że obecnie Trybunał rozpatruje serię pytań prejudycjalnych dotyczących konkretnie wystarczająco precyzyjnego charakteru szeregu punktów załącznika I, a w szczególności pkt 4, 8, 12, 18 (zob. zawiśła sprawa C-215/20).

¹⁵⁴ Zobacz opinia 1/15, pkt 158.

¹⁵⁵ Pragnę zauważyć, że informacje dotyczące biur podróży lub agencji turystycznej są już wymienione w pkt 5 załącznika I.

przez dyrektywę PNR na podmioty inne niż pasażerowie linii lotniczych w rozumieniu art. 3 pkt 4 dyrektywy PNR, proponuję, aby w braku dokładnych danych umożliwiających stwierdzenie, że systematyczne i ogólne gromadzenie danych kontaktowych tych osób trzecich stanowi element ściśle niezbędny dla skuteczności systemu przetwarzania danych PNR, Trybunał interpretował ów punkt jako dotyczący wyłącznie danych kontaktowych, które wyraźnie w nim wskazano i które dotyczą pasażera lotniczego, w imieniu którego dokonano rezerwacji. Niewątpliwie dyrektywa PNR nie wyklucza, że do JIP mogą być przekazywane również dane osobowe podmiotów innych niż pasażerowie lotniczy¹⁵⁶. Co jednak ważne, przypadki, w których jest to możliwe, powinny być wskazane w sposób jasny i wyraźny, jak ma to miejsce w odniesieniu do agencji turystycznych wymienionych w pkt 9 załącznika I, lub opiekunów małoletnich podróżujących samodzielnie, o których mowa w pkt 12 tego załącznika. Tylko bowiem w razie spełnienia tego warunku można uznać, że decyzję o włączeniu tych danych do danych przekazywanych do JIP poprzedziło wyważenie różnych wchodzących w grę interesów w rozumieniu motywu 15 dyrektywy PNR, a zainteresowane osoby trzecie mogą być odpowiednio poinformowane o przetwarzaniu ich danych osobowych.

163. Następnie, co się tyczy pkt 6 załącznika I, którego przedmiotem są „[w]szystkie informacje o formie płatności, w tym adres na fakturze”, to zgodnie z tym, co Trybunał orzekł w pkt 159 opinii 1/15 w odniesieniu do odnośnej rubryki załącznika do projektu umowy PNR Kanada–UE, aby punkt ten spełniał wymogi jasności i precyzji, należy go interpretować w ten sposób, że rubryka ta „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”. Informacje te nie mogą zatem obejmować na przykład danych dotyczących sposobów zapłaty za inne usługi, które nie są bezpośrednio związane z lotem, takie jak wynajem samochodu po przylocie¹⁵⁷.

164. Jeśli chodzi o pkt 8, dotyczący „[i]nformacji o programach lojalnościowych”, zgodnie z jego definicją w normach ICAO odnosi się on do numeru konta i statusu osoby często latającej samolotem¹⁵⁸. Tak interpretowany, punkt ów spełnia wymogi jasności i precyzji.

165. W odniesieniu do pkt 10 załącznika I, w którym wskazane są „dane o statusie podróży pasażera, w tym potwierdzenia, stan odprawy biletowo-bagażowej, dane typu: pasażer nie stawił się lub pasażer nabył bilet w czasie odprawy bez wcześniejszej rezerwacji”, oraz do pkt 13 tego załącznika, obejmującego „informacje o wystawieniu biletu, w tym numer biletu, data wystawienia biletu i bilety w jedną stronę, informacja o automatycznie skalkulowanej taryfie”, mimo ich otwartego ujęcia, dotyczą wyłącznie informacji bardzo precyzyjnych i jasno określonych, a także bezpośrednio związanych z lotem. To samo dotyczy pkt 14 załącznika I, w którym mowa o „numerze miejsca na pokładzie i innych informacjach o miejscu” oraz pkt 16 tego załącznika, dotyczącego „wszystkich informacji o bagażu”.

¹⁵⁶ Zobacz definicję danych PNR w art. 3 pkt 5 dyrektywy PNR.

¹⁵⁷ Zobacz podobnie również opinia rzecznika generalnego P. Mengozziego w postępowaniu w przedmiocie wydania opinii 1/15 [(Umowa PNR UE–Kanada), EU:C:2016:656], pkt 218.

¹⁵⁸ Zobacz odpowiednią rubrykę dodatku I do wytycznych ICAO.

– W przedmiocie zakresu danych wymienionych w załączniku I (drugie pytanie prejudycjalne)

166. Wśród elementów, które Trybunał bierze pod uwagę przy ocenie proporcjonalnego charakteru środka będącego źródłem ingerencji w prawa ustanowione w art. 7 i 8 karty, znajduje się adekwatny, stosowny i nienadmierny charakter przetwarzanych danych osobowych (zasada „minimalizacji danych”)¹⁵⁹. Ten sam test jest przewidziany w orzecznictwie ETPC¹⁶⁰ i zalecany w konwencji nr 108¹⁶¹.

167. Z motywu 15 dyrektywy PNR wynika, że wykaz danych PNR przekazywanych do JIP sporządzono zarówno celem zaspokojenia uzasadnionych potrzeb organów publicznych w związku z zapobieganiem przestępstwom terrorystycznym lub poważnej przestępczości, jak i z myślą o ochronie praw podstawowych do poszanowania życia prywatnego i ochrony danych osobowych dzięki zastosowaniu „wysokich standardów” zgodnie z kartą, konwencją nr 108 i EKPC. W tym samym motywie wyjaśniono, że dane PNR powinny zawierać w szczególności wyłącznie informacje dotyczące rezerwacji i tras podróży pasażerów, które umożliwią właściwym organom identyfikację pasażerów lotniczych stanowiących zagrożenie dla bezpieczeństwa wewnętrznego.

168. Co się tyczy w pierwszej kolejności adekwatnego i istotnego charakteru danych PNR wskazanych w załączniku I, poszczególne punkty tego załącznika, w tym pkt 5, 6, 8 i 18 w sugerowanej przeze mnie wykładni¹⁶² oraz pkt 12, z wyjątkiem części, którą proponuję uznać za nieważną¹⁶³, dotyczą jedynie danych stanowiących informacje bezpośrednio związane z podróżami lotniczymi wchodzącymi w zakres stosowania dyrektywy PNR. Dane te wykazują ponadto obiektywny związek z celami realizowanymi przez tę dyrektywę. W szczególności dane API mogą być wykorzystywane między innymi „w trybie reaktywnym” w celu zidentyfikowania osoby znanej już organom ścigania, na przykład ze względu na to, że jest podejrzewana o udział w przestępstwach terrorystycznych lub czynach poważnej przestępczości, które zostały już lub mają zostać popełnione, natomiast dane PNR mogą być używane raczej „w trybie czasu rzeczywistego” lub „w trybie aktywnym” do identyfikacji zagrożeń pochodzących od osób jeszcze nieznanymi organom ścigania.

169. W drugiej kolejności, jeśli chodzi o zakres danych PNR wymienionych w załączniku I, dane te, w tym dane objęte pkt 5, 6, 8 12 i 18 tego załącznika zgodnie z ich wykładnią zaproponowaną przez mnie w pkt 134–164 niniejszej opinii, nie wydają się nadmierne w świetle, po pierwsze, wagi realizowanego przez dyrektywę PNR celu bezpieczeństwa publicznego, a po drugie, przydatności systemu ustanowionego przez tę dyrektywę do osiągnięcia takiego celu.

170. Co się tyczy zwłaszcza danych API, nad którymi sąd odsyłający zastanawia się w sposób szczególny, pragnę zauważyć, że dane te, o charakterze biograficznym i dotyczące podróży, co do zasady pozwalają na uzyskanie jedynie ograniczonych informacji na temat życia prywatnego danych pasażerów. Ponadto, o ile prawdą jest, że pkt 18 załącznika I odnosi się do informacji, które nie należą do informacji wyraźnie wymienionych w art. 3 ust. 2 dyrektywy API, o tyle

¹⁵⁹ Zobacz podobnie wyrok Digital Rights, pkt 57. W przedmiocie wymogu, by kategorie danych objęte środkiem dostępu były ograniczone do tego, co jest ściśle niezbędne do zamierzonego celu, zob. ostatnio wyrok Prokuratuur, pkt 38. Zasada minimalizacji danych jest wymieniona między innymi w art. 5 ust. 1 lit. c) RODO i w art. 4 ust. 1 lit. c) dyrektywy policyjnej.

¹⁶⁰ Zobacz w szczególności wyrok ETPC z dnia 18 kwietnia 2013 r. w sprawie M.K. przeciwko Francji (CE:ECHR:2013:0418JUD001952209, § 35).

¹⁶¹ Zobacz sprawozdanie wyjaśniające do konwencji nr 108 z 1981 r., (<https://rm.coe.int/16800ca471>), art. 5 pkt 40, jak również sprawozdanie wyjaśniające do zmodernizowanej konwencji nr 108, art. 5 pkt 51.

¹⁶² Zobacz pkt 154–158 i 162–164 niniejszej opinii.

¹⁶³ Zobacz pkt 133–153 niniejszej opinii.

informacje te, dotyczące tożsamości pasażera linii lotniczych (płeć), dokumentu podróży, którym się posługuje (kraj wydania, data wygaśnięcia każdego dokumentu tożsamości), lub lotu, którym podróżuje (linia lotnicza, numer lotu, data i port lotniczy odlotu i przylotu), częściowo się pokrywają lub mogą zostać pobrane z danych PNR wskazanych w innych punktach załącznika I, przykładowo w pkt 3, 7 i 13. Poza tym w zakresie, w jakim informacje te dotyczą danych biograficznych lub wykorzystywanych dokumentów podróży, mogą one pomóc organom ścigania w sprawdzeniu tożsamości danej osoby i w ten sposób, jak wynika z motywu 9 dyrektywy PNR, zmniejszają ryzyko dokonywania sprawdzeń i prowadzenia postępowań przygotowawczych w stosunku do osób niewinnych. Wreszcie, należy podkreślić, że sam fakt, iż pkt 18 załącznika I obejmuje dane dodatkowe w stosunku do danych figurujących w art. 3 ust. 2 dyrektywy API, nie powoduje automatycznie nadmiernego charakteru tych danych, ze względu na odmienną celów realizowanych przez tę dyrektywę i przez dyrektywę PNR.

171. Jeśli chodzi o dane małoletnich bez opieki, wymienione w pkt 12 załącznika I, dotyczą one kategorii osób o specjalnych potrzebach i korzystających ze szczególnej ochrony, również w zakresie poszanowania ich życia prywatnego i ochrony danych osobowych¹⁶⁴. Niemniej ograniczenie tych praw może okazać się konieczne, w szczególności w celu ochrony dzieci przed poważną przestępczością, której mogą być ofiarami, takiej jak handel i wykorzystywanie seksualne dzieci lub uprowadzenie dziecka. Nie można zatem a priori uznać, że pkt 12 załącznika I, w zakresie, w jakim w odniesieniu do małoletnich bez opieki wymaga on przekazania większej liczby danych osobowych, wykracza poza to, co jest absolutnie konieczne.

172. Chociaż moim zdaniem dane osobowe, które przewoźnicy lotniczy są zobowiązani przekazywać do JIP zgodnie z dyrektywą PNR, odpowiadają wymogom adekwatności i znaczenia, a ich zakres nie wykracza poza to, co jest absolutnie konieczne do funkcjonowania systemu ustanowionego przez tę dyrektywę, nie zmienia to faktu, że przekazywaniu podlega znaczna liczba różnorodnych danych osobowych każdego zainteresowanego pasażera, a także ekstremalnie duża liczba takich danych w wartościach bezwzględnych. W tych okolicznościach kluczowe znaczenie ma to, aby takie przekazywanie było obwarowane dostatecznymi gwarancjami mającymi na celu, po pierwsze, zapewnienie, że przekazywane są wyłącznie dane wskazane w przepisach, a po drugie, zagwarantowanie bezpieczeństwa i poufności przekazywanych danych.

173. W tym względzie należy zauważyć w pierwszej kolejności, że prawodawca Unii przewidział przede wszystkim szereg gwarancji umożliwiających ograniczenie kategorii danych PNR udostępnianych przez organy ścigania i zapewnienie, by dostęp ten był ograniczony wyłącznie do danych, których przetwarzanie uważane jest za konieczne do celów realizowanych przez dyrektywę PNR. I tak, po pierwsze, dyrektywa ta wymienia w sposób wyczerpujący i precyzyjny (z zastrzeżeniem rozważań przedstawionych w ramach odpowiedzi na trzecie pytanie prejudycjalne) dane, które mogą być przekazywane do JIP. Po drugie, dyrektywa PNR wyraźnie wskazuje, że przekazywane do JIP mogą być jedynie dane zawarte w tym wykazie, będącym rezultatem wyważenia różnych interesów i wymogów wymienionych w motywie 15 tej dyrektywy (art. 6 ust. 1 dyrektywy PNR). Po trzecie, dyrektywa ta uściśla, że jeżeli wśród przekazanych danych PNR znajdują się dane inne niż wymienione w załączniku I, JIP usuwa je „w sposób trwały niezwłocznie po ich otrzymaniu” (art. 6 ust. 1 dyrektywy PNR). Po czwarte, wspomniana dyrektywa przewiduje, że dane PNR, o których mowa w załączniku I, mogą zostać przekazane, tylko jeśli przewoźnicy lotniczy zgromadzili je w normalnym toku swojej działalności (art. 8 ust. 1 dyrektywy PNR i motyw 8 tej dyrektywy), co oznacza, że wszystkie dane wskazane

¹⁶⁴ Prawo dziecka do poszanowania życia prywatnego zostało w szczególności potwierdzone w art. 16 Konwencji nowojorskiej o prawach dziecka, przyjętej w dniu 20 listopada 1989 r., która weszła w życie w dniu 2 września 1990 r.

w załączniku I nie są systematycznie dostępne JIP, lecz jedynie te, które znajdują się w systemie rezerwacyjnym danego operatora. Po piąte, art. 8 ust. 1 dyrektywy PNR przy przekazywaniu danych PNR do JIP nakłada na przewoźników lotniczych obowiązek stosowania metody „push”. Metoda ta, zalecana przez wytyczne ICAO¹⁶⁵, oznacza, że przewoźnicy sami przekazują dane PNR do baz danych JIP. W porównaniu do metody „pull”, dzięki której właściwe organy mogą uzyskiwać dostęp do systemów operatorów i pobierać z baz danych kopie wymaganych danych, metoda „push” oferuje więcej gwarancji, ponieważ nadaje przewoźnikowi lotniczemu rolę strażnika i kontrolera danych PNR. Wreszcie, zgodnie z wytycznymi ICAO oraz zasadą „jednego okienka”¹⁶⁶, dyrektywa PNR przewiduje, że przekazywanie danych PNR następuje za pośrednictwem jednego podmiotu, czyli JIP, działającego pod nadzorem inspektora, o którym mowa w art. 5 tej dyrektywy, a przede wszystkim pod nadzorem krajowego organu nadzorczego, wskazanego w art. 15 wspomnianej dyrektywy.

174. W drugiej kolejności trzeba zauważyć, że dyrektywa PNR przewiduje pewne gwarancje mające na celu ochronę *bezpieczeństwa* danych PNR. Odsyłam w tym względzie do art. 13 ust. 2 tej dyrektywy, który stanowi, że do wszelkich operacji przetwarzania danych osobowych dokonywanych na jej podstawie stosuje się art. 28 i 29 dyrektywy policyjnej w odniesieniu do poufności przetwarzania oraz bezpieczeństwa danych, a także do ust. 3 tego artykułu, który w odniesieniu do przetwarzania danych PNR przez przewoźników lotniczych przypomina obowiązki spoczywające na nich zgodnie z RODO, w szczególności w odniesieniu do odpowiednich środków technicznych i organizacyjnych, jakie należy podjąć w celu ochrony bezpieczeństwa i poufności tych danych¹⁶⁷.

175. Wreszcie, należy podkreślić, że w motywach 29 i 37 dyrektywy PNR uznano prawo pasażerów do otrzymania „w sposób łatwo dostępny i zrozumiały dokładnych informacji”, między innymi o gromadzeniu danych PNR, i zwrócono się do państw członkowskich o zapewnienie przestrzegania tego prawa. O ile uznanie tego prawa nie znajduje odzwierciedlenia w tekście dyrektywy PNR w postaci przepisu mającego moc wiążącą, o tyle przypominam, że – jak wskazałem w ramach analizy pierwszego pytania prejudycjalnego – przekazywanie danych PNR do JIP jest objęte przepisami RODO. Przewoźnicy lotniczy są zatem zobowiązani przestrzegać przy ich przekazywaniu między innymi art. 13 i 14 RODO, ustanawiających prawo do informacji przysługujące osobom, których dotyczy przetwarzanie danych osobowych. W ramach transpozycji dyrektywy PNR państwa członkowskie powinny wyraźnie ustanowić prawo pasażerów lotniczych do informacji, w postaci uznanej w motywach 29 i 37 tej dyrektywy, przy czym w żadnym razie nie mogą one ograniczyć zakresu art. 13 i 14 RODO na podstawie art. 23 ust. 1 tego rozporządzenia, ponieważ byłoby to sprzeczne z duchem rzeczony dyrektywy. Aby prawo to było skuteczne, musi ono bowiem dotyczyć również kategorii danych PNR podlegających przekazaniu.

¹⁶⁵ Zobacz pkt 2.7.3 wytycznych ICAO.

¹⁶⁶ Zobacz pkt 2.7.4 wytycznych ICAO.

¹⁶⁷ Wymóg zagwarantowania bezpieczeństwa i wiarygodności przekazywania danych do JIP przypomniano zresztą w art. 16 ust. 1 dyrektywy PNR w odniesieniu do środków elektronicznych używanych do ich przekazywania, przy czym wymóg ów był też jednym z kryteriów, którymi Komisja kierowała się przy przyjmowaniu zgodnie z ust. 3 tego artykułu wspólnych protokołów i formatów danych, które przewoźnicy lotniczy powinni wykorzystywać podczas przekazywania; zob. decyzja wykonawcza Komisji (UE) 2017/759 z dnia 28 kwietnia 2017 r. w sprawie wspólnych protokołów i formatów danych, z których mają korzystać przewoźnicy lotniczy podczas przekazywania danych dotyczących przelotu pasażera jednostkom do spraw informacji o pasażerach (Dz.U. 2017, L 113, s. 48).

176. Biorąc pod uwagę całość powyższych rozważań, jestem zdania, że dane PNR, których przetwarzanie jest przewidziane w dyrektywie PNR, z zastrzeżeniem sugerowanych ograniczeń i uściśleń dokonanych w ramach trzeciego pytania prejudycjalnego, są adekwatne, stosowne i nienadmierne w świetle celów realizowanych przez tę dyrektywę, a ich zakres nie wykracza poza to, co jest absolutnie konieczne do realizacji tych celów.

– *W przedmiocie danych szczególnie chronionych*

177. Dyrektywa PNR zakazuje w sposób ogólny przetwarzania w jakikolwiek sposób „danych szczególnie chronionych”¹⁶⁸.

178. Chociaż dyrektywa ta nie zawiera definicji pojęcia „danych szczególnie chronionych”, to z jej art. 13 ust. 4 wynika, że obejmuje ono co najmniej „dane PNR ujawniające rasę lub pochodzenie etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, stan zdrowia, życie seksualne lub orientację seksualną danej osoby”¹⁶⁹. W pkt 165 opinii 1/15 Trybunał wyjaśnił, że każdy środek oparty na założeniu, że jedna lub kilka z jego cech „mogłaby sama przez się i niezależnie od indywidualnego zachowania danego pasażera mieć znaczenie w odniesieniu do celu przetwarzania danych PNR [...], naruszałby prawa zagwarantowane w art. 7 i 8 karty w związku z jej art. 21”. Zatem dzięki zakazowi jakichkolwiek operacji przetwarzania danych, o których mowa w jej art. 13 ust. 4, dyrektywa PNR respektuje ograniczenia nałożone przez Trybunał na wykorzystywanie tych kategorii danych w ramach systemu przetwarzania danych PNR, niezależnie od tego, czy podlega on prawu krajowemu, prawu Unii czy umowie międzynarodowej zawartej przez Unię.

179. Ogólny zakaz przetwarzania szczególnie chronionych danych ustanowiony w dyrektywie PNR obejmuje również ich gromadzenie. I tak, jak wyraźnie wskazuje motyw 15 tej dyrektywy, dziewiętnaście rubryk określonych w załączniku I nie opiera się na danych PNR, o których mowa w jej art. 13 ust. 4.

180. Chociaż żadna z tych rubryk nie odnosi się wyraźnie do takich danych, mogłyby one jednak znaleźć się w szczególności w rubryce „Uwagi ogólne”, wskazanej w pkt 12 załącznika I, która stanowi „pole otwarte”, mogące obejmować, jak już miałem okazję zauważyć w ramach badania trzeciego pytania prejudycjalnego, nieokreśloną ilość informacji o różnorodnym charakterze. Istnieje bowiem konkretne ryzyko, jak Trybunał zauważył zresztą w pkt 164 opinii 1/15, że informacje zawarte w rzeczonyj rubryce, dotyczące na przykład preferencji dietetycznych, próśb o pomoc, zryczałtowanych cen przysługujących niektórym kategoriom osób lub stowarzyszeń, ujawniają bezpośrednio dane szczególnie chronione w rozumieniu art. 13 ust. 4 dyrektywy PNR, dotyczące w szczególności przekonań religijnych zainteresowanych pasażerów, ich stanu zdrowia lub przynależności do partii politycznej.

181. Ponieważ przetwarzanie tych danych jest w każdym razie wykluczone przez dyrektywę PNR, ich przekazywanie przez przewoźników lotniczych nie tylko wykracza w sposób oczywisty poza to, co jest absolutnie konieczne, lecz również jest całkowicie bezużyteczne. W tym względzie należy podkreślić, że okoliczność, iż zgodnie z art. 13 ust. 4 zdanie drugie dyrektywy PNR JIP są w każdym razie zobowiązane do niezwłocznego usunięcia danych PNR ujawniających jedną z informacji wymienionych w zdaniu pierwszym tego ustępu, nie umożliwia zezwolenia ani nie

¹⁶⁸ Zobacz motyw 37 dyrektywy PNR.

¹⁶⁹ Wszystkie kategorie danych osobowych wymienione w art. 13 ust. 4 dyrektywy PNR należą do kategorii danych osobowych objętych pojęciem „szczególnych kategorii danych osobowych”, o którym mowa w art. 9 ust. 1 RODO.

uzasadnia przekazywania tych danych¹⁷⁰, ponieważ ustanowiony w tej dyrektywie zakaz przetwarzania takich danych musi działać już na pierwszym etapie przetwarzania danych PNR. Obowiązek usunięcia danych szczególnie chronionych stanowi zatem jedynie dodatkową gwarancję przewidzianą w tej dyrektywie, na wypadek gdyby wyjątkowo takie dane przekazano do JIP w wyniku błędu.

182. Pragnę ponadto zauważyć, jak wskazał rzecznik generalny P. Mengozzi w pkt 222 opinii przedstawionej na potrzeby opinii Trybunału 1/15¹⁷¹, że ponieważ informacje zawarte w rubrykach z „tekstem dowolnym”, takich jak rubryka „Uwagi ogólne”, o której mowa w pkt 12 załącznika I, mogące zawierać dane szczególnie chronione w rozumieniu art. 13 ust. 4 dyrektywy PNR, są przekazywane przez pasażerów wyłącznie nieobowiązkowo, jest mało prawdopodobne, aby osoby zaangażowane w przestępstwa terrorystyczne lub zakwalifikowane do poważnej przestępczości spontanicznie udzielały takich informacji, a zatem systematyczne przekazywanie tych danych będzie najpewniej dotyczyć w większości przypadków jedynie osób, które wystąpiły o usługę dodatkową i które w rzeczywistości nie są w żaden sposób interesujące dla organów ścigania¹⁷².

183. W ramach analizy trzeciego pytania prejudycjalnego doszedłem do wniosku, że pkt 12 załącznika I, dotyczący rubryki „Uwagi ogólne”, nie spełnia wymogów jasności i precyzji ustanowionych w art. 52 ust. 1 zdanie pierwsze karty. Z powodów, które właśnie wyjaśniłem, uważam, że włączenie tej rubryki do kategorii danych podlegających systematycznemu przekazywaniu do JIP, bez jakiegokolwiek uściślenia rodzaju informacji, których może ona dotyczyć, nie spełnia również kryterium konieczności przewidzianego w art. 52 ust. 1 zdanie drugiej karty, zgodnie z jego wykładnią dokonaną przez Trybunał¹⁷³.

184. Jednakże wyłączenie rubryk z „tekstem dowolnym” z wykazu danych PNR przekazywanych organom państwowym w ramach systemu przetwarzania danych PNR nie wystarczy do eliminacji ryzyka, że dane szczególnie chronione zostaną jednak tym organom udostępnione. Dane takie można bowiem nie tylko wywieść bezpośrednio z informacji zamieszczonych w takich rubrykach, lecz również pośrednio wywnioskować z informacji w rubrykach „kodowanych” lub potwierdzić je na ich podstawie. I tak, przykładowo, nazwisko pasażera lotniczego może dostarczyć wskazówek lub przynajmniej pozwolić na wysunięcie hipotez co do pochodzenia etnicznego lub przynależności religijnej danego pasażera. To samo dotyczy obywatelstwa. Danych tych nie można co do zasady wykluczyć z wykazu danych PNR podlegających przekazaniu, przy czym nie mogą ich też usunąć organy upoważnione do odbioru danych. W związku z tym, aby uniknąć ryzyka stygmatyzacji na podstawie chronionych cech dużej liczby osób, które nie są przy tym podejrzewane o popełnienie przestępstwa, system przetwarzania danych PNR powinien przewidywać wystarczające gwarancje pozwalające wykluczyć na każdym etapie przetwarzania gromadzonych danych możliwość bezpośredniego lub pośredniego uwzględnienia takich cech w operacjach przetwarzania, na przykład poprzez stosowanie w zautomatyzowanej analizie selektorów opartych na tych cechach. Powrócę do tej kwestii w dalszej części mojego wyводу.

¹⁷⁰ W tym względzie moim zdaniem pozbawione znaczenia są argumenty wysunięte przez kilka państw członkowskich, które przedstawiły uwagi w przedmiocie drugiego pytania prejudycjalnego, oparte na istnieniu środków technicznych pozwalających na łatwe usunięcie danych szczególnie chronionych przekazanych przez przewoźników lotniczych.

¹⁷¹ Opinia rzecznika generalnego P. Mengozziego w postępowaniu w przedmiocie wydania opinii 1/15 (Umowa PNR UE–Kanada, EU:C:2016:656).

¹⁷² Pragnę zauważyć, że nawet wytyczne ICAO, chociaż nie wykluczają przydatności danych szczególnie chronionych, które można uzyskać z rubryk z „tekstem dowolnym”, przy ocenie ryzyka związanego z poszczególnymi pasażerami, zalecają jednak, aby umawiające się państwa zapewniły ich uwzględnianie tylko wtedy, gdy istnieją konkretne wskazówki przemawiające za ich wykorzystaniem do celów realizowanych przez systemy PNR.

¹⁷³ Przypominam, że wykluczenie tych danych zaproponował już EIOD w swojej opinii z dnia 25 marca 2011 r., pkt 47.

185. Na podstawie całości powyższych rozważań uważam, z zastrzeżeniem wniosku, do którego doszedłem w pkt 183 powyżej, że na etapie przekazywania danych PNR do JIP dyrektywa PNR przewiduje wystarczające gwarancje służące ochronie danych szczególnie chronionych.

iii) W przedmiocie pojęcia „pasażera” (czwarte pytanie prejudycjalne)

186. W czwartym pytaniu prejudycjalnym sąd odsyłający zwraca się w istocie do Trybunału o ustalenie, czy system ustanowiony przez dyrektywę PNR, w zakresie, w jakim zezwala na przekazywanie i przetwarzanie danych PNR każdej osoby odpowiadającej pojęciu „pasażera” w rozumieniu art. 3 pkt 4 tej dyrektywy, niezależnie od jakiegokolwiek obiektywnego czynnika pozwalającego na uznanie, że osoba ta może stanowić zagrożenie dla bezpieczeństwa publicznego, jest zgodny z art. 7, 8 i art. 52 ust. 1 karty. Sąd ten zastanawia się w szczególności nad możliwością zastosowania do systemu przetwarzania danych osobowych ustanowionego dyrektywą PNR orzecznictwa Trybunału w dziedzinie przechowywania i dostępu do danych w sektorze łączności elektronicznej.

187. W zakresie istotnym dla postępowania w niniejszej sprawie Trybunał stwierdził w tym orzecznictwie, że uregulowań, które w celu zwalczania poważnej przestępczości przewidują uogólnione i niezróżnicowane *przechowywanie* prewencyjne danych o ruchu związanych z łącznością elektroniczną i danych dotyczących lokalizacji¹⁷⁴ na potrzeby organów ścigania, bez jakiegokolwiek zróżnicowania, ograniczeń ani wyjątków w zależności od zamierzonego celu, nie można co do zasady uznać za uzasadnione w społeczeństwie demokratycznym¹⁷⁵. Podobnie Trybunał orzekł w odniesieniu do uregulowań krajowych, które w celu zwalczania terroryzmu przewidywały *zautomatyzowaną analizę wszystkich wspomnianych danych* w drodze filtrowania przez dostawców usług łączności elektronicznej na żądanie właściwych organów krajowych i przy zastosowaniu określonych przez nie parametrów¹⁷⁶. Zdaniem Trybunału tego rodzaju środki mogą być uzasadnione jedynie w sytuacjach, gdy dane państwo członkowskie stoi w obliczu poważnego zagrożenia dla bezpieczeństwa narodowego, które okaże się rzeczywiste oraz aktualne lub przewidywalne, i gdy decyzja przewidująca ich wykonanie jest przedmiotem skutecznej kontroli sądu lub niezależnego organu administracyjnego¹⁷⁷. Odwołanie się do rzeczonych środków w takich sytuacjach powinno ponadto zdaniem Trybunału być ograniczone w czasie do tego, co absolutnie konieczne, a w każdym razie nie może mieć charakteru systemowego¹⁷⁸.

188. Pragnę ponadto zauważyć, że chociaż w tym orzecznictwie Trybunał nie posunął się, jak w wyroku Schrems I, do stwierdzenia w sposób wyraźny naruszenia istoty prawa do poszanowania życia prywatnego, to jednak uznał, że ingerencja wynikająca z rozpatrywanych środków osiąga wagę takiego stopnia, że – z wyjątkiem ograniczonego przypadku szczególnych zagrożeń dla bezpieczeństwa narodowego państwa członkowskiego – nie można ich uznać za

¹⁷⁴ Chodzi tu o dane, które mogą dostarczyć informacji o komunikatach elektronicznych użytkownika środka łączności elektronicznej lub o lokalizacji urządzeń końcowych, z których ten korzysta.

¹⁷⁵ Zobacz podobnie wyroki: La Quadrature du Net, pkt 141–145; Tele2 Sverige, pkt 105, 106, wydane w związku z wykładnią art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty, a także wyrok Digital Rights, pkt 57, 58, w którym Trybunał stwierdził nieważność dyrektywy 2006/24.

¹⁷⁶ Zobacz wyrok La Quadrature du Net, pkt 177.

¹⁷⁷ Zobacz wyrok La Quadrature du Net, pkt 134–139, 177. Zdaniem Trybunału odpowiedzialność spoczywająca na państwach członkowskich w dziedzinie bezpieczeństwa narodowego „obejmuje pierwszorzędny interes w ochronie podstawowych funkcji państwa i podstawowych interesów społeczeństwa, a także zapobieganie i ściganie działalności mogącej poważnie zdestabilizować podstawowe struktury konstytucyjne, polityczne lub społeczne kraju, w szczególności bezpośrednio zagrozić społeczeństwu, ludności lub państwu jako takiemu, zwłaszcza takiej jak działalność terrorystyczna”; zob. wyroki: La Quadrature du Net, pkt 135; Privacy International, pkt 74.

¹⁷⁸ Zobacz wyrok La Quadrature du Net, pkt 138, 178.

ograniczone do tego, co jest absolutnie konieczne, a zatem za zgodne z kartą¹⁷⁹, niezależnie od ewentualnych gwarancji ustanowionych w celu ochrony przed ryzykiem nadużycia i bezprawnego dostępu do odnośnych danych¹⁸⁰.

189. Miałem już okazję podkreślić, że przepisy takie jak przewidziane w dyrektywie PNR łączy ze środkami tego rodzaju, co badane przez Trybunał w orzecznictwie przypomnianym w poprzedzających punktach niniejszej opinii, pewna liczba wspólnych elementów, które nadają im charakter ingerencji szczególnie silnej. Dyrektywa ta ustanawia zatem uogólniony i niezróżnicowany system gromadzenia i zautomatyzowanej analizy danych osobowych istotnej części populacji, mający zastosowanie w sposób ogólny do wszystkich osób odpowiadających pojęciu „pasażera” zapisanemu w art. 3 pkt 4 wspomnianej dyrektywy, a w konsekwencji również do tych, w odniesieniu do których nie istnieje żadna przesłanka mogąca sugerować, że ich zachowanie może mieć związek, choćby pośredni lub daleki, z działaniami terrorystycznymi lub z poważną przestępczością. W tych okolicznościach sąd odsyłający zastanawia się, czy orzecznictwo to znajduje zastosowanie do systemu przetwarzania danych PNR, takiego jak ustanowiony w dyrektywie PNR.

190. W tym względzie pragnę zauważyć, że w opinii 1/15 Trybunał w ramach badania w pkt 186–189 zakresu stosowania *ratione personae* projektu umowy PNR Kanada–UE nie narysował żadnej paraleli między z jednej strony środkami służącymi przechowywaniu treści komunikatów elektronicznych i uogólnionemu i niezróżnicowanemu dostępowi do nich, danych o ruchu i danych dotyczących lokalizacji, a z drugiej strony przekazywaniem danych PNR i ich zautomatyzowanym przetwarzaniem w ramach wstępnej oceny pasażerów, przewidzianej w tejże umowie. Jednakże w chwili wydania tej opinii istniało już utrwalone orzecznictwo, potwierdzone zaledwie kilka miesięcy wcześniej w wyroku *Tele2 Sverige*, wskazanym przez sąd odsyłający, w którym środki te – poza szczególnymi, sporadycznymi sytuacjami¹⁸¹ – uznano za niezgodne z kartą¹⁸². Najnowsze wyroki Trybunału w tej dziedzinie, a w szczególności wyrok *La Quadrature du Net*, podążają tropem tego orzecznictwa, przy czym uściślają je, a w pewnych aspektach uszczegóławiają.

191. We wspomnianych punktach opinii 1/15 Trybunał wyraźnie uznał, że umowa PNR Kanada–UE nie wydaje się wykraczać poza granice tego, co absolutnie konieczne, pozwalając na *przekazywanie i zautomatyzowane przetwarzanie* danych PNR wszystkich pasażerów lotniczych do Kanady dla celów ich wstępnej oceny, i to pomimo faktu, że rzeczone przekazywanie i przetwarzanie ma się odbywać „niezależnie od jakiegokolwiek obiektywnego elementu pozwalającego na uznanie, że pasażerowie mogą stanowić zagrożenie dla bezpieczeństwa publicznego w Kanadzie”¹⁸³. W pkt 187 tej opinii Trybunał stwierdził, że „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”¹⁸⁴.

¹⁷⁹ Zobacz w szczególności wyrok w sprawie *Quadrature du Net*, pkt 141–145.

¹⁸⁰ Zobacz wyrok *La Quadrature du Net*, pkt 115, 116; zob. także opinia rzecznika generalnego M. Camposa Sánchez-Bordony w sprawach połączonych *SpaceNet i Telekom Deutschland* (C-793/19 i C-794/19, EU:C:2021:939, pkt 74, 75).

¹⁸¹ Zobacz wyrok *Tele2 Sverige*, pkt 119.

¹⁸² Zobacz podobnie wyrok *Tele2 Sverige*, pkt 103–107, 119 i przytoczone tam orzecznictwo.

¹⁸³ Zobacz opinia 1/15, pkt 186, 187.

¹⁸⁴ W wyrokach *Digital Rights* (pkt 59) i *Tele2 Sverige* (pkt 111), tak jak w późniejszym orzecznictwie (zob. w szczególności wyrok *La Quadrature du Net*, pkt 143–150), to właśnie fakt, że rozpatrywane uregulowanie nie opierało się na „obiektywnych elementach” tego rodzaju jak wymienione przez Trybunał w pkt 187 opinii 1/15, umożliwiających wzięcie na cel osób, których dane mogły mieć związek, chociażby pośredni, z aktami poważnej przestępczości, sprawił, że uregulowanie to było nieproporcjonalne.

192. Tak więc, przynajmniej jeśli chodzi o uogólnione i niezróżnicowane przekazywanie danych PNR, Trybunał odstąpił od bardziej rygorystycznego podejścia przyjętego w dziedzinie przechowywania i dostępu do metadanych.

193. O ile nie ulega wątpliwości, że w swoim rozumowaniu Trybunał wziął pod uwagę, jak wynika w szczególności z pkt 152 i 188 opinii 1/15, po pierwsze, to, że zautomatyzowane przetwarzanie danych PNR ułatwia kontrolę bezpieczeństwa, w szczególności na granicach, a po drugie, to, że zgodnie z konwencją chicagowską pasażerowie lotniczy zamierzający wjechać na terytorium państwa członkowskiego tej konwencji są zobowiązani poddać się kontroli i przestrzegać warunków wjazdu i wyjazdu ustanowionych przez to państwo, w tym sprawdzeniu ich danych PNR, o tyle uważam, że za takim zróżnicowanym podejściem przemawiają inne powody, do których należy w pierwszej kolejności charakter danych podlegających przetwarzaniu.

194. Trybunał wielokrotnie podkreślał, że nie tylko treść komunikatów elektronicznych, ale również metadane mogą ujawnić informacje o „wielu aspektach życia prywatnego osób, których dane dotyczą, w tym informacje newralgiczne, takie jak orientacja seksualna, poglądy polityczne, przekonania religijne, filozoficzne, społeczne lub inne, jak również stan zdrowia”, że całokształt tych danych „umożliwia wyciągnięcie bardzo precyzyjnych wniosków dotyczących życia prywatnego osób, których dane są zatrzymywane, takich jak ich codzienne nawyki, miejsca stałego lub czasowego pobytu, codziennie lub okazjnie pokonywane trasy, podejmowane czynności, relacje towarzyskie i środowiska społeczne, w których osoby te się obracają”, przy czym dane te dają w szczególności możliwość ustalenia „profilu danych osób, która to informacja jest z punktu widzenia prawa do poszanowania życia prywatnego równie newralgiczna co sama treść komunikatów”¹⁸⁵. Przypominam ponadto, że przepisy badane dotychczas przez Trybunał, w tym uregulowania dyrektywy 2006/24, nie przewidywały żadnego wyjątku i miały zastosowanie również do komunikatów wymienianych z podmiotami o charakterze socjalnym lub religijnym lub z osobami podlegającymi obowiązkowi zachowania tajemnicy zawodowej. Trybunał zatem, chociaż nie stwierdził naruszenia istoty prawa do poszanowania życia prywatnego, wskazał jednak, że „z uwagi [...] na to, że informacje mogące wynikać z danych o ruchu i danych o lokalizacji są szczególnie chronione, ich poufność ma zasadnicze znaczenie dla prawa do poszanowania życia prywatnego”¹⁸⁶.

195. Natomiast, o ile Trybunał niewątpliwie uznał w opinii 1/15, że – jak przypomniałem w pkt 77 i 98 niniejszej opinii – dane PNR mogą w określonych wypadkach ujawniać bardzo dokładne informacje na temat życia prywatnego danej osoby¹⁸⁷, o tyle stwierdził też, że charakter tych informacji ogranicza się jedynie do niektórych aspektów życia prywatnego¹⁸⁸, co sprawia, że dostęp do takich danych jest ingerencją słabszą niż dostęp do treści komunikatów elektronicznych oraz danych o ruchu i danych dotyczących lokalizacji.

196. W drugiej kolejności nie tylko charakter danych PNR różni się od charakteru danych o ruchu i danych dotyczących lokalizacji, lecz również ilość i różnorodność informacji, które mogą podlegać ujawnieniu poprzez dane w tych kategoriach, przy czym informacje zawarte w danych PNR są zarówno pod względem ilościowym, jak i jakościowym bardziej ograniczone. Wynika to nie tylko z faktu, że systemy uogólnionego i niezróżnicowanego przetwarzania danych dotyczących komunikatów elektronicznych mogą obejmować swoim działaniem prawie całą odnośną populację, podczas gdy systemy przetwarzania danych PNR mają zastosowanie do

¹⁸⁵ Zobacz wyrok La Quadrature du Net (pkt 117 i przytoczone tam orzecznictwo); zob. także wyrok Prokuratuur (pkt 36).

¹⁸⁶ Wyrok La Quadrature du Net, pkt 142.

¹⁸⁷ Zobacz opinia 1/15, pkt 128, 150.

¹⁸⁸ Zobacz opinia 1/15, pkt 150.

bardziej ograniczonego kręgu osób, aczkolwiek istotnego liczbowo, lecz również z częstotliwości wykorzystywania środków łączności elektronicznej i wielości tych środków. Ponadto dyrektywa PNR przewiduje gromadzenie i przetwarzanie ograniczonej i wyczerpująco określonej liczby danych PNR, z wyłączeniem danych należących do kategorii wymienionych w art. 13 ust. 4 tej dyrektywy, zatem jeśli nawet nie ilość, to co najmniej wrażliwość informacji na temat życia prywatnego osób, płynących z danych PNR, można częściowo ocenić z wyprzedzeniem¹⁸⁹. Takie zaś ograniczenie typów gromadzonych danych, pozwalające na wykluczenie znacznej części danych mogących nieść informacje szczególnie chronione, jest w przypadku danych o ruchu i danych dotyczących lokalizacji możliwe jedynie częściowo, biorąc pod uwagę liczbę wchodzących w grę użytkowników i środków łączności¹⁹⁰.

197. W trzeciej kolejności wszelkie przetwarzanie metadanych komunikatów elektronicznych nie tylko może dotykać intymną sferę życia prawie całego społeczeństwa, lecz także wkracza w wykonywanie innych swobód, dzięki którym każda jednostka uczestniczy w życiu społecznym i demokratycznym danego kraju¹⁹¹, a w szczególności może wpłynąć zniechęcająco na wykonywanie przez użytkowników środków łączności elektronicznej ich wolności wypowiedzi¹⁹², która stanowi „jeden z istotnych fundamentów pluralistycznego i demokratycznego społeczeństwa”, na jakich opiera się Unia¹⁹³. Aspekt ten jest nierozdzielnie związany ze środkami dotyczącymi tych kategorii danych osobowych i, co do zasady, nie dotyczy systemów przetwarzania danych PNR.

198. W czwartej kolejności, głównie z uwagi na liczbę i różnorodność informacji o charakterze szczególnie chronionym, które można uzyskać z analizy treści komunikatów elektronicznych oraz danych o ruchu i danych dotyczących lokalizacji, pojawia się ryzyko arbitralności związane z przetwarzaniem tych danych, które jest znacząco wyższe niż w przypadku systemów przetwarzania danych PNR.

199. Ze względów, które właśnie przedstawiłem, jestem zdania, że bardziej rygorystyczne podejście Trybunału w dziedzinie komunikatów elektronicznych nie może znaleźć zastosowania, jako takie, do systemów przetwarzania danych PNR. Trybunał wypowiedział się już w ten sposób w opinii 1/15, przynajmniej w sposób dorozumiany, w kontekście umowy międzynarodowej ustanawiającej taki system w celu ochrony bezpieczeństwa państwa trzeciego. Moim zdaniem takie samo stanowisko jest tym bardziej uzasadnione w odniesieniu do dyrektywy PNR, której celem jest ochrona wewnętrznego bezpieczeństwa Unii.

200. Mimo to należy zauważyć, jak uczynił to rzecznik generalny P. Mengozzi w pkt 216 opinii przedstawionej w postępowaniu w przedmiocie wydania opinii Trybunału 1/15¹⁹⁴, że sensem systemów PNR, niezależnie od tego, czy są one przyjmowane w sposób jednostronny, czy stanowią przedmiot umowy międzynarodowej, jest właśnie zapewnienie masowego przekazywania danych pozwalających właściwym organom na zidentyfikowanie, za pomocą systemów zautomatyzowanego przetwarzania danych oraz scenariuszy lub określonych wcześniej kryteriów oceny, osób nieznanych organom ścigania, które mogą „wzbudzać zainteresowanie” lub

¹⁸⁹ W przedmiocie trudności takiej oceny w odniesieniu do metadanych zob. wyrok Prokurator, pkt 40.

¹⁹⁰ Starań w tym względzie dołożył ustawodawca niemiecki, przyjmując przepisy będące przedmiotem spraw połączonych C-793/19 i C-794/19, SpaceNet i Telekom Deutschland, w których rzecznik generalny M. Campos Sánchez-Bordona przedstawił swoją opinię (EU:C:2021:939, pkt 60, 61).

¹⁹¹ Odsyłam w tym względzie do rozważań przedstawionych w pkt 93 niniejszej opinii.

¹⁹² Zobacz wyrok La Quadrature du Net, pkt 118 i przytoczone tam orzecznictwo.

¹⁹³ Zobacz wyrok Tele2 Sverige, pkt 93.

¹⁹⁴ Opinia rzecznika generalnego P. Mengozziego w postępowaniu w przedmiocie wydania opinii 1/15 (Umowa PNR UE–Kanada, EU:C:2016:656).

stanowić zagrożenie dla bezpieczeństwa publicznego i które w związku z tym mogą zostać następnie poddane dokładniejszym indywidualnym kontrolom. Wymóg „uzasadnionego podejrzenia”, który można znaleźć w orzecznictwie ETPC dotyczącym ukierunkowanego przechwytywania stosowanego w ramach karnych postępowań przygotowawczych¹⁹⁵ oraz w orzecznictwie Trybunału dotyczącym przechowywania metadanych¹⁹⁶, jest zatem mniej istotny w kontekście tego rodzaju przekazywania i tego typu przetwarzania¹⁹⁷. W szczególności celów prewencji realizowanych przez takie systemy nie można by osiągnąć przy ograniczeniu ich stosowania do określonej kategorii osób, jak zresztą Trybunał stwierdził we wspomnianych w pkt 191 niniejszej opinii fragmentach opinii 1/15, w związku z czym należy stwierdzić, że zakres dyrektywy PNR wydaje się zapewniać skuteczną realizację tego celu¹⁹⁸.

201. Należy również podkreślić, że Komisja wielokrotnie kładła nacisk na strategiczne znaczenie przetwarzania danych PNR jako istotnego instrumentu wspólnej odpowiedzi Unii na terroryzm i poważną przestępczość, a także jako najważniejszego elementu unii bezpieczeństwa¹⁹⁹. Rola, jaką odgrywają systemy przetwarzania danych PNR w ramach „globalnego podejścia” do walki z terroryzmem, została uznana również przez Radę Bezpieczeństwa Narodów Zjednoczonych, która w rezolucji 2396 (2017)²⁰⁰ zobowiązała państwa członkowskie Organizacji Narodów Zjednoczonych do „wzmocnienia ich zdolności do gromadzenia, przetwarzania i analizowania w ramach norm i zalecanych praktyk ICAO danych [PNR] oraz zapewnienia przekazania tych danych wszystkim właściwym organom krajowym i wykorzystywania ich przez te organy, przy pełnym poszanowaniu praw człowieka i podstawowych wolności, do celów prewencji, wykrywania i ścigania przestępstw terrorystycznych i podróżujących terrorystów”²⁰¹. Obowiązek ten potwierdzono w rezolucji 2482/2019 w dziedzinie terroryzmu i poważnej przestępczości międzynarodowej²⁰².

202. W tym kontekście przyjęcie zharmonizowanego systemu przetwarzania danych PNR na poziomie Unii, zarówno w odniesieniu do lotów pozaunijnych, jak i wewnątrzunijnych w przypadku państw, które skorzystały z art. 2 dyrektywy PNR, pozwala na zapewnienie, że przetwarzanie tych danych odbywa się z poszanowaniem wysokiego poziomu ochrony praw

¹⁹⁵ Zobacz w szczególności wyrok ETPC z dnia 4 grudnia 2015 r. w sprawie Roman Zakharov przeciwko Rosji, CE:ECHR:2015:1204JUD004714306, § 260.

¹⁹⁶ Zobacz wyroki: La Quadrature du Net (pkt 146–151); Tele2 Sverige (pkt 119).

¹⁹⁷ Podobnie, jeśli chodzi o środki masowego przechwytywania, zob. wyrok w sprawie Big Brother Watch, § 348.

¹⁹⁸ Zobacz analogicznie wyrok z dnia 3 października 2019 r., A i in. (C-70/18, EU:C:2019:823, pkt 61).

¹⁹⁹ Zobacz ostatnio komunikat Komisji w sprawie strategii UE w zakresie unii bezpieczeństwa, [COM(2020) 605 final, s. 28], a także komunikat Komisji: Plan dla UE w dziedzinie zwalczania terroryzmu: przewidywanie, zapobieganie, ochrona i reagowanie [COM(2020) 795 final, s. 15 i nast.].

²⁰⁰ Rezolucja z dnia 21 grudnia 2017 r. [zwana dalej „rezolucją 2396 (2017)”, [https://undocs.org/fr/S/RES/2396\(2017\)](https://undocs.org/fr/S/RES/2396(2017))] [tłumaczenie nieoficjalne].

²⁰¹ Zobacz rezolucję 2396 (2017), pkt 12; w tymże pkt 12 Rada Bezpieczeństwa Narodów Zjednoczonych „zobowiązuje ICAO do pracy z jej państwami członkowskimi nad ustanowieniem standardu zbierania, wykorzystywania, przetwarzania i ochrony danych PNR” [tłumaczenie nieoficjalne]. W następstwie tego wezwania w dniu 23 czerwca 2020 r. ICAO przyjęła poprawkę nr 28 do załącznika 9 do konwencji chicagowskiej, która, jak już wskazałem, ustanawia międzynarodowe standardy dotyczące ułatwień, a której sekcja D rozdziału 9 dotyczy konkretnie danych PNR. W dniu 12 stycznia 2021 r. Komisja przyjęła wniosek w przedmiocie decyzji Rady w sprawie stanowiska, jakie ma być zajęte w imieniu Unii Europejskiej na forum ICAO w odniesieniu do tej poprawki [COM(2021) 16 final].

²⁰² Rezolucja z dnia 19 lipca 2019 r., pkt 15 lit. c), [https://undocs.org/fr/S/RES/2482\(2019\)](https://undocs.org/fr/S/RES/2482(2019)).

zapisanych w art. 7 i 8 karty, ustalonego w tej dyrektywie, i stanowi system prawny będący punktem odniesienia przy negocjowaniu umów międzynarodowych w sprawie przetwarzania i przekazywania danych PNR²⁰³.

203. Ponadto, o ile prawdą jest, że system wprowadzony dyrektywą PNR dotyczy bez różnicy wszystkich pasażerów lotniczych, jak słusznie podkreślił Parlament w swoich uwagach na piśmie i jak wskazała również Rada Bezpieczeństwa Narodów Zjednoczonych w rezolucji 2396 (2017), która powołuje się na konkretne ryzyko wykorzystania lotnictwa cywilnego na potrzeby terroryzmu zarówno jako środek transportu, jak i cel²⁰⁴, o tyle istnieje obiektywny związek między transportem lotniczym a zagrożeniem dla bezpieczeństwa publicznego w postaci zwłaszcza terroryzmu, ale również chociażby niektórych rodzajów poważnej przestępczości, takich jak w szczególności przemyt substancji odurzających i handel ludźmi, które wykazują zresztą istotne aspekty transgraniczne.

204. Należy wreszcie podkreślić, jak podniosły Parlament, Rada i kilka państw członkowskich, które złożyły uwagi na piśmie, że pasażerowie lotniczy przy wjeździe do Unii lub wyjeździe z Unii są zobowiązani do poddania się kontroli bezpieczeństwa²⁰⁵. Przekazywanie i przetwarzanie danych PNR przed ich przyjazdem lub przed ich wyjazdem ułatwia i przyspiesza tę kontrolę, jak również zauważył Trybunał w opinii 1/15, ponieważ umożliwia organom ścigania skupienie się na pasażerach, o których dysponują informacjami faktycznymi wskazującymi na rzeczywiste zagrożenie dla bezpieczeństwa²⁰⁶.

205. Wreszcie, co się tyczy w szczególności rozszerzenia systemu dyrektywy PNR na loty wewnątrzunijne, to o ile nie można a priori wykluczyć jakiegokolwiek wpływu na swobodę przemieszczania się obywateli Unii, ustanowioną w szczególności w art. 45 karty, o tyle ingerencja w życie prywatne wprowadzona w dyrektywie PNR, choć poważna, nie może moim zdaniem sama w sobie zniechęcić do korzystania z tej wolności, przy czym obywatele mogą nawet postrzegać przetwarzanie danych PNR jako środek niezbędny do zapewnienia bezpieczeństwa podróży lotniczych²⁰⁷. Nie zmienia to faktu, że możliwość pojawienia się takiego zniechęcającego skutku powinna być przedmiotem oceny i ciągłego monitorowania.

206. Jednakże, aby spełnić wymogi orzecznictwa przypomnianego w pkt 107 i 108 niniejszej opinii, dyrektywa PNR nie może ograniczyć się do wymogu, aby dostęp do danych PNR i zautomatyzowane przetwarzanie danych PNR wszystkich pasażerów lotniczych odpowiadały zamierzonemu celowi, ale musi również przewidywać w sposób jasny i precyzyjny warunki materialne i proceduralne regulujące dostęp do nich i ich przetwarzanie, jak również sposób późniejszego wykorzystania tych danych²⁰⁸, a także ustanowić odpowiednie gwarancje na każdym

²⁰³ Obecnie istnieją dwie umowy międzynarodowe zawarte przez Unię, odpowiednio, z Australią [Umowa między Unią Europejską a Australią o przetwarzaniu i przekazywaniu przez przewoźników lotniczych australijskiej służbie celnej i granicznej danych dotyczących przelotu pasażera (danych PNR) (Dz.U. 2012, L 186, s. 4)] i ze Stanami Zjednoczonymi Ameryki [Umowa między Stanami Zjednoczonymi Ameryki a Unią Europejską o wykorzystywaniu danych dotyczących przelotu pasażera oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (Dz.U. 2012, L 215, s. 5)]. Obie te umowy poddane są obecnie łącznej ocenie pod kątem zawierania nowych umów. W dniu 18 lutego 2020 r. Rada upoważniła ponadto Komisję do rozpoczęcia negocjacji z Japonią.

²⁰⁴ Zobacz rezolucja 2396 (2017), s. 4.

²⁰⁵ W tym osoby korzystające z prawa do swobodnego przemieszczania się na podstawie prawa Unii, zob. rozporządzenie (UE) 2017/458 Parlamentu Europejskiego i Rady z dnia 15 marca 2017 r. zmieniające rozporządzenie (UE) 2016/399 w odniesieniu do zintensyfikowania odpraw na granicach zewnętrznych z wykorzystaniem odpowiednich baz danych (Dz.U. 2017, L 74, s. 7).

²⁰⁶ Zobacz podobnie także opinia 1/15, pkt 187. Zobacz także komunikat Komisji w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwow trzecim [COM(2010) 492 wersja ostateczna, s. 6, pkt 2.2].

²⁰⁷ Takie jest właśnie w pewnym sensie rozumowanie Komisji w projekcie dyrektywy PNR, s. 3.

²⁰⁸ Zobacz podobnie wyrok Prokuratora, pkt 49 i przytoczone tam orzecznictwo.

etapie tego procesu. O gwarancjach związanych z przekazywaniem danych PNR do JIP wspomniałem już w ramach analizy drugiego pytania prejudycjalnego. W ramach analizy szóstego pytania prejudycjalnego zbadam te zabezpieczenia, które towarzyszą konkretnie zautomatyzowanemu przetwarzaniu tych danych, a także – w ramach badania ósmego pytania prejudycjalnego – zabezpieczenia związane z ich przechowywaniem.

207. Przed przystąpieniem do dalszej analizy pragnę jednak podkreślić fundamentalne znaczenie, jakie w ramach systemu gwarancji wprowadzonego dyrektywą PNR ma kontrola sprawowana przez niezależny organ, o którym mowa w art. 15 tej dyrektywy. Zgodnie z tym artykułem wszystkie operacje przetwarzania danych przewidziane w tej dyrektywie podlegają nadzorowi niezależnego organu nadzorczego, który ma uprawnienia do sprawdzania zgodności z prawem przetwarzania danych, prowadzenia postępowań, inspekcji i audytów oraz rozpatrywania skarg złożonych przez osoby, których dane dotyczą. Taka kontrola sprawowana przez podmiot zewnętrzny, któremu powierzono ochronę interesów potencjalnie pozostających w konflikcie z interesami realizowanymi przez podmioty przetwarzające dane PNR i którego rolą jest czuwanie nad przestrzeganiem wszelkich ograniczeń i zabezpieczeń związanych z rzeczonymi operacjami przetwarzania, stanowi istotną gwarancję wyraźnie przewidzianą w art. 8 ust. 3 karty, której skuteczność w zakresie ochrony danych praw podstawowych jest nawet wyższa od systemu środków odwoławczych dostępnych jednostkom. Fundamentalne znaczenie ma zatem moim zdaniem interpretowanie przez Trybunał zakresu uprawnień nadzorczych przewidzianych w art. 15 dyrektywy PNR w sposób rozszerzający oraz przyznanie przez państwa członkowskie krajowym organom nadzorczym pełnego wachlarza tych uprawnień, przy dokonywaniu transpozycji tej dyrektywy do prawa wewnętrznego, poprzez zapewnienie im zasobów materialnych i osobowych niezbędnych do wykonania jego zadań.

208. Na podstawie całości powyższych rozważań stwierdzam, że dyrektywa PNR nie wykracza poza granice tego, co absolutnie konieczne, przez to, że pozwala na zautomatyzowane przekazywanie i przetwarzanie danych każdej osoby objętej pojęciem „pasażera” w rozumieniu art. 3 pkt 4 tej dyrektywy.

iv) W przedmiocie wystarczająco jasnego, precyzyjnego i ograniczonego do tego, co absolutnie konieczne, charakteru wstępnej oceny pasażerów (szóste pytanie prejudycjalne)

209. W szóstym pytaniu prejudycjalnym sąd odsyłający zwraca się w istocie do Trybunału o wyjaśnienie, czy wstępna ocena, o której mowa w art. 6 dyrektywy PNR, jest zgodna z art. 7, 8 i art. 52 ust. 1 karty. Chociaż brzmienie tego pytania koncentruje się na systematycznym i uogólnionym charakterze zautomatyzowanego przetwarzania danych PNR wszystkich pasażerów lotniczych, z jakim wiąże się ta wstępna ocena, to z uzasadnienia postanowienia odsyłającego wynika, że Cour constitutionnelle (trybunał konstytucyjny) zwraca się do Trybunału w kontekście takiego przetwarzania o bardziej ogólną ocenę poszanowania wymogów zgodności z prawem i proporcjonalności. Poniżej przeprowadzę taką właśnie ocenę, odsyłając jednocześnie do analizy przeprowadzonej w ramach badania czwartego pytania prejudycjalnego, dotyczącej nieukierunkowanego charakteru wspomnianego przetwarzania zautomatyzowanego.

210. Artykuł 6 ust. 2 lit. a) dyrektywy PNR przewiduje, że JIP dokonują wstępnej oceny pasażerów lotniczych przed ich planowanym przylotem do państwa członkowskiego lub planowanym opuszczeniem przez nich owego państwa. Ocena ta służy identyfikacji osób, które wymagają dalszego sprawdzenia przez właściwe organy „ze względu na możliwość udziału takich osób w przestępstwach terrorystycznych lub w poważnej przestępczości”. Artykuł 6 ust. 6 dyrektywy

PNR stanowi, że JIP w państwie członkowskim przekazuje dane PNR osób zidentyfikowanych w ramach tej oceny lub wyniki przetwarzania tych danych właściwym organom, o których mowa w art. 7 tej dyrektywy, w tym samym państwie członkowskim „do dalszego sprawdzenia”.

211. Zgodnie z art. 6 ust. 3 dyrektywy PNR wstępna ocena na podstawie ust. 2 lit. a) tego artykułu wykonywana jest poprzez porównanie z bazami danych, „które mają znaczenie” [art. 6 ust. 3 lit. a)], i poprzez przetwarzanie według ustalonych kryteriów [art. 6 ust. 3 lit. b)].

212. Zanim zajmę się badaniem każdego z tych dwóch rodzajów przetwarzania danych, pragnę zauważyć, że z brzmienia wspomnianego art. 6 ust. 3 nie wynika jasno, czy państwa członkowskie są zobowiązane do tego, aby wstępna ocena pasażerów była dokonywana w sposób systematyczny i we wszystkich przypadkach w drodze analizy zautomatyzowanej zarówno pierwszego, jak i drugiego rodzaju, czy też, jak wydaje się potwierdzać użycie czasownika „móc” i łącznika „lub”, są one uprawnione do zorganizowania swoich systemów w taki sposób, aby analizę przewidzianą w przepisie lit. b) art. 6 ust. 3 zastrzec dla określonych przypadków. W tym względzie pragnę uściślić, że projekt dyrektywy PNR przewidywał, iż analizę tę przeprowadza się wyłącznie w ramach walki z poważnymi przestępstwami transgranicznymi²⁰⁹.

213. Podobnie jak Komisja, uważam, że z systematyki dyrektywy PNR wynika w szczególności, iż państwa członkowskie są zobowiązane wprowadzić dwa rodzaje zautomatyzowanego przetwarzania, również ze względów związanych z wymogiem zapewnienia jak najbardziej jednolitego stosowania systemu przetwarzania danych PNR Unii. Nie oznacza to jednak, że państwa członkowskie nie są upoważnione – a nawet zobowiązane w celu zagwarantowania, że przetwarzanie danych związane z wstępną oceną przeprowadzoną zgodnie z art. 6 ust. 2 lit. a) dyrektywy PNR będzie ograniczone do tego, co jest absolutnie konieczne – do prowadzenia analizy na podstawie art. 6 ust. 3 lit. b) dyrektywy PNR w sposób ograniczony, w zależności od wyników wstępnej oceny, pod kątem skuteczności w odniesieniu do każdego z przestępstw, o których mowa w tej dyrektywie, czy ewentualnie do zastrzeżenia jej jedynie dla niektórych z tych przestępstw. Za takim rozumieniem przemawia motyw 7 dyrektywy PNR, zgodnie z którym „aby ograniczyć przetwarzanie danych PNR do niezbędnego minimum, ustalanie i stosowanie kryteriów dokonywania sprawdzeń należy ograniczyć do przestępstw terrorystycznych i poważnej przestępczości, w przypadku których stosowanie takich kryteriów jest właściwe”.

– *W przedmiocie porównania z bazami danych w rozumieniu art. 6 ust. 3 lit. a) dyrektywy PNR*

214. Pierwsza część wstępnej oceny, jakiej dokonują JIP na podstawie art. 6 ust. 2 lit. a) dyrektywy PNR, zakłada, zgodnie z ust. 3 lit. a) tego artykułu, porównanie danych PNR („data matching”) z bazami danych w celu znalezienia ewentualnych wyników pozytywnych („hits”). Rzeczne „hits” są weryfikowane przez JIP zgodnie z art. 6 ust. 5 dyrektywy PNR oraz, w stosownych przypadkach, przekształcane w „match” i przekazywane właściwym organom.

215. Jak bowiem zauważył Trybunał w pkt 172 opinii 1/15, zakres ingerencji wynikający z tego rodzaju zautomatyzowanych analiz w prawa ustanowione w art. 7 i 8 karty zależy zasadniczo od baz danych, na których analizy te się opierają. W związku z tym istotne jest, aby przepisy wprowadzające takie operacje przetwarzania danych określały w sposób wystarczająco jasny i precyzyjny bazy danych dopuszczone do celów porównywania danych podlegających przetwarzaniu.

²⁰⁹ Zobacz art. 4 ust. 2 lit. a) projektu dyrektywy PNR.

216. Zgodnie z art. 6 ust. 3 lit. a) dyrektywy PNR JIP porównują dane PNR z „bazami danych, które mają znaczenie”²¹⁰ w świetle celów realizowanych przez tę dyrektywę. Przepis ów wymienia również szczególną kategorię baz danych, a mianowicie bazy dotyczące „osób lub przedmiotów poszukiwanych lub objętych wpisem”, które prawodawca Unii zatem wyraźnie zakwalifikował jako „mające znaczenie” w rozumieniu tego przepisu.

217. Poza tym wyjaśnieniem pojęcie „baz danych, które mają znaczenie” nie zostało w większym stopniu uściślone. W szczególności nie wskazano, czy aby można było uznać, że baza danych wykorzystywana do porównywania danych PNR „ma znaczenie”, muszą nią zarządzać organy ścigania, czy też ogólnie dowolny organ władzy publicznej, czy po prostu organy te muszą mieć bezpośredni lub pośredni dostęp do takiej bazy. Ani charakter danych, które takie bazy mogą zawierać, ani ich związek z celami dyrektywy PNR również nie został sprecyzowany²¹¹. Ponadto z brzmienia art. 6 ust. 3 lit. a) dyrektywy PNR wynika, że jako „bazy danych, które mają znaczenie” mogą zostać zakwalifikowane zarówno bazy krajowe i bazy Unii, jak i międzynarodowe bazy danych, co jeszcze bardziej rozszerza wachlarz baz danych potencjalnie objętych tym przepisem i zwiększa otwarty charakter tego pojęcia²¹².

218. W tych okolicznościach, na podstawie ogólnej zasady wykładni przypomnianej w pkt 151 niniejszej opinii, do Trybunału należy w miarę możliwości zinterpretowanie art. 6 ust. 3 lit. a) dyrektywy PNR, a w szczególności pojęcia „baz danych, które mają znaczenie”, zgodnie z wymogami jasności i precyzji określonymi w karcie. Ponadto zważywszy, że przepis ten przewiduje ingerencję w prawa podstawowe ustanowione w art. 7 i 8 karty, należy go interpretować w sposób zawężający i z uwzględnieniem wymogu zapewnienia wysokiego poziomu ochrony tych praw podstawowych, potwierdzonego w szczególności w motywie 15 dyrektywy PNR. Ponadto wykładni tego przepisu należy dokonywać w świetle zasady ograniczenia celów, do których dane PNR mogą być przetwarzane, ustanowionej w art. 1 ust. 2 dyrektywy PNR.

219. Biorąc pod uwagę te kryteria, pojęcie „baz danych, które mają znaczenie” należy moim zdaniem interpretować w ten sposób, że obejmuje ono wyłącznie krajowe bazy danych zarządzane przez właściwe organy na podstawie art. 7 ust. 1 dyrektywy PNR, jak również bazy danych Unii i międzynarodowe bezpośrednio wykorzystywane przez te organy w ramach wykonywania ich zadań. Rzeczne bazy danych powinny ponadto pozostawać w bezpośrednim i ścisłym związku z celami dyrektywy PNR polegającymi na zwalczaniu terroryzmu i poważnej przestępczości w tym znaczeniu, że zostały one opracowane do tych celów. Pojęcie to, interpretowane w powyższy sposób, odnosi się zasadniczo, jeśli nie wyłącznie, do baz danych dotyczących osób lub przedmiotów poszukiwanych lub objętych wpisem, wyraźnie wymienionych w art. 6 ust. 3 lit. a) dyrektywy PNR.

²¹⁰ O ile we francuskiej wersji językowej art. 6 ust. 3 lit. a) wymienia „bases de données utiles” [użyteczne bazy danych], o tyle w większości innych wersji językowych przepis ten dotyczy raczej „istotnych baz danych”: zob. między innymi wersje angielską „relevant”, włoską „pertinenti”, niemiecką „massgeblich”, hiszpańską „pertinentes”, niderlandzką „relevant”, portugalską „relevantes”.

²¹¹ Sposób sformułowania art. 6 ust. 3 lit. a) dyrektywy PNR pozwala, jak się wydaje, na prowadzenie analiz w drodze badania danych poprzez ich porównywanie z bardzo różnorodnymi danymi, pod warunkiem że badanie to w ostatecznym rezultacie posłuży do realizacji celów dyrektywy. W przedmiocie zagrożeń związanych z „data mining” w dziedzinie danych PNR zob. raport Korffa, s. 77. EIOD podkreślił z całą mocą brak precyzji i przewidywalności, jaki wiąże się z identyfikacją baz danych, z którymi można porównywać dane PNR, w opinii z dnia 25 marca 2011 r., pkt 18.

²¹² Niejasny i otwarty charakter sformułowań w art. 6 ust. 3 lit. a) dyrektywy PNR przekłada się na bardzo zróżnicowaną transpozycję do prawa krajowego, poczynawszy od ścisłej wykładni pojęcia „baz danych, które mają znaczenie”, ograniczającej przewidzianą analizę wyłącznie do porównania z bazami danych wyraźnie wymienionymi w tym przepisie (tak jest w przypadku Republiki Federalnej Niemiec, jak wynika z uwag przedstawionych przez rząd tego państwa przed Trybunałem), a skończywszy na wykładni szerszej, która obejmuje każdą bazę danych w dyspozycji właściwych organów lub dostępną dla nich w ramach ich zadań (tak sformułowany jest między innymi art. 24 § 1 pkt 1 ustawy PNR).

220. Ogólnie rzecz biorąc, z zakresu pojęcia „baz danych, które mają znaczenie” wyłączone są bazy danych zarządzane lub wykorzystywane przez służby wywiadowcze państw członkowskich, chyba że odpowiadają one ściśle warunkowi pozostawania w ścisłym związku z celami realizowanymi przez dyrektywę PNR, a dane państwo członkowskie przyznaje swoim służbom wywiadowczym szczególne kompetencje w dziedzinie ścigania²¹³.

221. Proponowana powyżej wykładnia jest zgodna z zaleceniami sformułowanymi przez Trybunał w pkt 172 opinii 1/15.

222. Jednakże art. 6 ust. 3 lit. a) dyrektywy PNR, nawet interpretowany w ten sposób, nie pozwala na wystarczająco dokładne zidentyfikowanie baz danych, które będą wykorzystywane przez państwa członkowskie do porównywania danych PNR, i nie można uznać, że spełnia on wymogi wynikające z art. 52 ust. 1 karty w wykładni nadanej mu przez Trybunał. Przepis ten należy zatem interpretować w ten sposób, że zobowiązuje on państwa członkowskie, w ramach transpozycji do prawa krajowego dyrektywy PNR, do opublikowania wykazu tych baz danych i do jego aktualizowania. Ponadto pożądane byłoby sporządzenie na poziomie Unii wykazu baz danych, „które mają znaczenie” w rozumieniu art. 6 ust. 3 lit. a) dyrektywy PNR, zarządzanych przez Unię we współpracy z państwami członkowskimi, oraz międzynarodowych baz danych, w celu zapewnienia w tym względzie jednolitości praktyki państw członkowskich.

– *W przedmiocie przetwarzania danych PNR w świetle wcześniej ustalonych kryteriów*

223. Druga część wstępnej oceny na podstawie art. 6 ust. 2 lit. a) dyrektywy PNR polega na zautomatyzowanej analizie w świetle wcześniej ustalonych kryteriów. W ramach tej analizy dane PNR są przetwarzane, głównie do celów o charakterze prognostycznym, poprzez stosowanie algorytmów mających umożliwić „identyfikację” pasażerów, którzy mogą brać udział w przestępstwach terrorystycznych lub w poważnej przestępczości. W tym kontekście JIP prowadzi zasadniczo działalność polegającą na profilowaniu²¹⁴. Ze względu na to, że takie przetwarzanie może mieć dla osób zidentyfikowanych przez algorytm poważne konsekwencje²¹⁵, wymaga ono dokładnego uregulowania zarówno co do sposobów jego realizacji, jak i gwarancji, jakimi powinno być obwarowane. Jak bowiem zauważył Trybunał w pkt 172 opinii 1/15, zakres wynikającej z tego rodzaju analiz ingerencji w prawa ustanowione w art. 7 i 8 karty zależy zasadniczo od stosowanych w tym celu modeli i wcześniej ustalonych kryteriów.

224. W tym względzie pragnę zauważyć w pierwszej kolejności, że art. 6 ust. 4 zdanie drugie dyrektywy PNR precyzuje, iż wcześniej ustalone kryteria, w świetle których przeprowadza się ocenę wstępną przewidzianą w art. 6 ust. 3 lit. b) tej dyrektywy, powinny być „ukierunkowane, proporcjonalne i szczegółowe”. Pierwszy z tych wymogów odnosi się do celu realizowanego przez

²¹³ W żadnym wypadku nie można uznać moim zdaniem, że na podstawie art. 6 ust. 3 lit. a) dyrektywy PNR państwo członkowskie ma obowiązek zezwolenia JIP na systematyczne porównywanie danych PNR z „bazami danych, które mają znaczenie” w rozumieniu tego przepisu, zarządzanymi przez jego służby wywiadowcze.

²¹⁴ Zgodnie z art. 3 ust. 4 dyrektywy policyjnej „profilowanie” oznacza „dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się”. Definicja ta znajduje się w art. 4 pkt 4 RODO i w pkt 1 lit. c) załącznika do zalecenia Komitetu Ministrów Rady Europy CM/Rec(2021)8 z dnia 3 listopada 2021 r. w sprawie ochrony osób w związku ze zautomatyzowanym przetwarzaniem danych osobowych w ramach profilowania [tłumaczenie nieoficjalne, tak jak dalsze cytaty z tego dokumentu], https://search.coe.int/cm/pages/result_details.aspx?ObjectId=0900001680a46148, (zwanego dalej „zaleceniem z 2021 r. w sprawie profilowania”).

²¹⁵ Punkt 1 lit. j) ppkt (i) zalecenia z 2021 r. w sprawie profilowania definiuje „profilowanie o wysokim ryzyku” jako „profilowanie, którego realizacja wywołuje skutki prawne lub które ma znaczny wpływ na podmiot danych lub grupę osób zidentyfikowanych w drodze profilowania”.

wstępną ocenę przewidzianą w ust. 2 lit. a) tego artykułu, jakim jest zidentyfikowanie osób, w odniesieniu do których wymagane jest bardziej szczegółowe sprawdzenie przez właściwe organy, i odpowiada w ten sposób podkreślonej przez Trybunał w opinii 1/15 konieczności, aby użyte kryteria były „ukierunkowywane” na osoby, na których może ciążyć „racjonalne podejrzenie” udziału w przestępstwach terrorystycznych lub poważnej przestępczości²¹⁶. Takie „ukierunkowanie” zakłada stosowanie abstrakcyjnych kryteriów oceny lub – aby posłużyć się wyrażeniem z zalecenia z 2021 r. w sprawie profilowania – „profili”²¹⁷, za pomocą których następuje „filtrowanie” danych PNR w celu identyfikacji pasażerów, którzy im odpowiadają i powinni w związku z tym być poddani dokładniejszej kontroli. Natomiast dyrektywa PNR nie zezwala na indywidualne profilowanie wszystkich pasażerów lotniczych, których dane są analizowane, na przykład poprzez przypisanie każdemu z nich kategorii ryzyka na określonej z góry skali, pod rygorem naruszenia zarówno art. 6 ust. 4 tej dyrektywy, jak i ograniczeń nałożonych przez Trybunał na zautomatyzowane przetwarzanie danych PNR w opinii 1/15.

225. Zgodnie z art. 6 ust. 4 zdanie drugie wcześniej ustalone kryteria, o których mowa w art. 6 ust. 3 lit. b) dyrektywy PNR, powinny być ponadto „szczegółowe”²¹⁸, a mianowicie dostosowane do zamierzonego celu i istotne w jego świetle, a także „proporcjonalne”²¹⁹, to znaczy niewykraczające poza granice owego celu. Aby spełnić te wymogi, a w szczególności „aby ograniczyć przetwarzanie danych PNR do niezbędnego minimum”, motyw 7 dyrektywy PNR, jak już podkreśliłem, stanowi, że „ustalanie i stosowanie kryteriów dokonywania sprawdzeń należy ograniczyć do przestępstw terrorystycznych i poważnej przestępczości, w przypadku których stosowanie takich kryteriów jest właściwe”.

226. Wreszcie zarówno z preambuły i przepisów dyrektywy PNR, jak i z wymogów określonych przez Trybunał w opinii 1/15 wynika, że wcześniej ustalone kryteria, o których mowa w art. 6 ust. 3 lit. b) dyrektywy PNR, powinny również być „wiarygodne”²²⁰, co oznacza, po pierwsze, że powinny być zaprojektowane z myślą o zminimalizowaniu ryzyka błędów²²¹, a po drugie, że powinny być „aktualne”²²². W tym względzie art. 6 ust. 4 zdanie trzecie dyrektywy PNR nakłada na państwa członkowskie obowiązek zapewnienia, by kryteria te były „ustanawiane i poddawane regularnym przeglądom przez JIP we współpracy z właściwymi organami, o których mowa w art. 7”²²³. W celu zapewnienia wiarygodności tych kryteriów i ograniczenia w miarę możliwości fałszywych wyników pozytywnych konieczne jest jeszcze, jak przyznała Komisja w odpowiedzi na pisemne pytanie Trybunału, ich skonstruowanie w taki sposób, aby uwzględniały zarówno elementy obciążające, jak i odciążające.

227. W drugiej kolejności dyrektywa PNR wyraźnie zakazuje korzystania z profilowania dyskryminacyjnego. I tak, art. 6 ust. 4 zdanie pierwsze tej dyrektywy przewiduje, że wstępna ocena dokonywana na podstawie ust. 3 lit. b) tego artykułu według wcześniej ustalonych kryteriów

²¹⁶ Zobacz opinia 1/15, pkt 272.

²¹⁷ Zgodnie z pkt 1.1 lit. d) załącznika do zalecenia z 2021 r. w sprawie profilowania pojęcie „profilu” oznacza „zbiór danych przypisany osobie, który charakteryzuje kategorię osób lub jest przeznaczony do stosowania wobec osób”. Jak wyjaśnia sprawozdanie w sprawie rozwoju sytuacji po przyjęciu zalecenia (2010)13 w sprawie profilowania, <https://rm.coe.int/t-pd-2019-07fin-fr-rapport-profilage-2770-2878-8993-1-final-clean-2755/1680a0925b>, s. 21, które poprzedziło wydanie zalecenia z 2021 r., pojęcie „profilu” zachowuje w pełni swoje znaczenie w systemach, które tak jak dyrektywa PNR rozróżniają operacje tworzenia profili [zob. w szczególności art. 6 ust. 2 lit. b) tej dyrektywy] od operacji ich stosowania, i pozwala na zapewnienie „przejrzystości kryteriów stosowanych w drugiej kolejności w operacjach profilowania”.

²¹⁸ Zobacz art. 6 ust. 4 dyrektywy PNR oraz opinia 1/15, pkt 172.

²¹⁹ Zobacz art. 6 ust. 4 dyrektywy PNR.

²²⁰ Zobacz opinia 1/15, pkt 172.

²²¹ Zobacz motyw 7 dyrektywy PNR.

²²² Zobacz opinia 1/15, pkt 174.

²²³ Ten sam wymóg znajduje się w pkt 174 opinii 1/15.

„odbywa się w sposób niedyskryminacyjny”. W tym względzie należy uściślić, że o ile art. 6 ust. 4 zdanie trzecie stanowi, iż wspomniane kryteria „w żadnym przypadku nie mogą opierać się na rasie ani pochodzeniu etnicznym, na poglądach politycznych, przekonaniach religijnych lub światopoglądowych, przynależności do związków zawodowych, stanie zdrowia, życiu seksualnym ani orientacji seksualnej danej osoby”, o tyle ogólny zakaz profilowania dyskryminacyjnego należy rozumieć w ten sposób, że obejmuje on wszystkie powody dyskryminacji, o których mowa w art. 21 karty, nawet niewymienione wprost²²⁴.

228. W trzeciej kolejności zarówno z brzmienia art. 6 ust. 3 lit. b) dyrektywy PNR, jak i z przewidzianego w niej systemu gwarancji związanych ze zautomatyzowanym przetwarzaniem danych PNR wynika, że funkcjonowanie algorytmów używanych w ramach analizy przewidzianej w tym przepisie powinno być przejrzyste, a wynik ich stosowania sprawdzalny. Ów wymóg przejrzystości nie oznacza oczywiście, że wykorzystywane „profile” należy podać do publicznej wiadomości. Wymaga on natomiast zapewnienia możliwości zidentyfikowania algorytmicznego sposobu podejmowania decyzji. Po pierwsze bowiem, wymóg, zgodnie z którym kryteria, na podstawie których należy przeprowadzić tę analizę, muszą być „wcześniej ustalone”, wyklucza możliwość ich modyfikacji bez interwencji człowieka i w związku z tym nie zezwala na stosowanie technologii opartych na sztucznej inteligencji, zwanych „machine learning”²²⁵, które choć mogą zapewniać najwyższy stopień precyzji, są trudne do zinterpretowania nawet dla podmiotów prowadzących zautomatyzowane przetwarzanie²²⁶. Po drugie, zabezpieczenie ustanowione w art. 6 ust. 5 i 6 dyrektywy PNR, zgodnie z którym każdy pozytywny wynik automatycznego przetwarzania danych PNR dokonanego na podstawie ust. 2 lit. a) tego artykułu jest indywidualnie oceniany w sposób niezautomatyzowany, wymaga dla swojej skuteczności – w odniesieniu do analizy, o której mowa w art. 6 ust. 3 lit. b) dyrektywy PNR – aby możliwe było zrozumienie przyczyn, dla których wykorzystywany program dał taki, a nie inny wynik, czego nie można osiągnąć w szczególności w przypadku korzystania z systemów uczących się maszynowo. To samo dotyczy kontroli zgodności z prawem tejże analizy, w tym również w odniesieniu do niedyskryminującego charakteru uzyskanych wyników, którą powierzono inspektorowi ochrony danych i krajowemu organowi nadzorczemu na podstawie, odpowiednio, art. 6 ust. 7 dyrektywy PNR i art. 15 ust. 3 lit. b) tej dyrektywy. Przejrzystość funkcjonowania wykorzystywanych algorytmów jest również warunkiem koniecznym do umożliwienia zainteresowanym skorzystania z przysługującego im prawa do wniesienia zażalenia, jak również ich prawa do skutecznego środka prawnego.

– *W przedmiocie gwarancji związanych ze zautomatyzowanym przetwarzaniem danych PNR*

229. W poprzednich punktach miałem już okazję wskazać niektóre gwarancje towarzyszące zautomatyzowanemu przetwarzaniu danych PNR w ramach oceny wstępnej na podstawie art. 6 ust. 2 lit. a) dyrektywy PNR, które spełniają wymogi określone przez Trybunał w opinii 1/15, a mianowicie zakaz przetwarzania danych na podstawie wcześniej ustalonych kryteriów dyskryminacyjnych (art. 6 ust. 4 zdania pierwsze i czwarte dyrektywy PNR; opinia 1/15, pkt 172),

²²⁴ Pragnę zauważyć, że wszystkie powody dyskryminacji wymienione w art. 21 karty powtórzono w motywie 20 dyrektywy PNR. W opinii 1/2011, s. 8, FRA zaproponowała ich uporządkowanie zgodnie z wykazem zakazanych powodów dyskryminacji, zapisanym w art. 21.

²²⁵ Zgodnie z pkt 1.1 lit. g) załącznika do zalecenia z 2021 r. w sprawie profilowania wyrażenie „machine learning” oznacza „przetwarzanie z wykorzystaniem szczególnych metod sztucznej inteligencji opartych na podejściu statystycznym, pozwalających wyposażyć komputery w zdolność »uczenia się« na podstawie danych, to znaczy podnoszenia swojej wydajności w rozwiązywaniu zadań bez zaprogramowania konkretnie do każdego z nich”.

²²⁶ W odniesieniu do wpływu nieprzejrzystości systemów algorytmicznych na możliwość kontroli przez człowieka w celu zapobiegania szkodliwym skutkom tych systemów i ich negatywnego oddziaływania na prawa człowieka zob. zalecenie CM/Rec(2020)1 Komitetu Ministrów Rady Europy dla państw członkowskich w przedmiocie wpływu systemów algorytmicznych na prawa człowieka.

regularną aktualizację wcześniej ustalonych kryteriów służących ocenie wstępnej, o której mowa w art. 6 ust. 3 lit. b) tej dyrektywy (art. 6 ust. 4 zdanie trzecie dyrektywy PNR; opinia 1/15, pkt 174), ocenę w sposób nieautomatyzowany każdego pozytywnego wyniku uzyskanego w wyniku automatycznego przetwarzania danych PNR (art. 6 ust. 5 i 6 dyrektywy PNR; opinia 1/15, pkt 173) oraz kontrolę zgodności z prawem przetwarzania danych przez inspektora ochrony danych i przez krajowy organ nadzorczy [art. 6 ust. 7 dyrektywy PNR i art. 15 ust. 3 lit. b) dyrektywy PNR]. W tym kontekście zasadnicze znaczenie ma to, by kontrola przeprowadzana przez niezależny organ, taki jak organ, o którym mowa w art. 15 dyrektywy PNR, po pierwsze, mogła dotyczyć każdego aspektu związanego ze zautomatyzowanym przetwarzaniem danych PNR, w tym identyfikacji baz danych wykorzystywanych do celów porównania w rozumieniu art. 6 ust. 3 lit. a) tej dyrektywy i opracowania wcześniej ustalonych kryteriów stosowanych w analizie na podstawie art. 6 ust. 3 lit. b) wspomnianej dyrektywy, a po drugie, mogła być przeprowadzana zarówno *ex ante*, jak i *ex post*.

230. Należy podkreślić, że powyższe gwarancje należy uznać za mające zastosowanie przekrojowo do obu rodzajów analiz, o których mowa w art. 6 ust. 3 dyrektywy PNR, i to niezależnie od sposobu określenia tychże gwarancji. I tak, o ile art. 6 ust. 4 zdanie pierwsze tej dyrektywy przypomina wymóg przestrzegania zasady niedyskryminacji jedynie w stosunku do wstępnej oceny przeprowadzonej w świetle wcześniej ustalonych kryteriów, o tyle wymóg ten obowiązuje na każdym etapie procesu przetwarzania danych PNR, a zatem również wtedy, gdy dane te są porównywane z odpowiednimi bazami danych w ramach wstępnej oceny w rozumieniu art. 6 ust. 3 lit. a) tej dyrektywy. To samo dotyczy wymogu, zgodnie z którym wcześniej ustalone kryteria użyte w ramach analizy wskazanej w art. 6 ust. 3 lit. b) dyrektywy PNR powinny być wiarygodne i aktualizowane, co dotyczy również, jak należy rozumieć, danych zawartych w bazach wykorzystywanych do celów porównania przewidzianego w art. 6 ust. 3 lit. a) tej dyrektywy. W tym względzie pragnę ogólnie zauważyć, że wszystkie gwarancje mające zastosowanie do zautomatyzowanego przetwarzania danych osobowych przewidziane w dyrektywie policyjnej mają również zastosowanie w ramach dyrektywy PNR, ponieważ należy stwierdzić, iż analizy zautomatyzowane przeprowadzane w ramach tej dyrektywy wchodzą również w zakres stosowania dyrektywy policyjnej.

231. Do gwarancji wymienionych w pkt 229 powyżej dochodzi gwarancja przewidziana w art. 7 ust. 6 dyrektywy PNR, która uzupełnia, po pierwsze, zakaz podejmowania decyzji wyłącznie na podstawie wyników zautomatyzowanego przetwarzania danych PNR, a po drugie, zakaz dyskryminacji przy przetwarzaniu i wykorzystywaniu tych danych. I tak, przepis ten stanowi, że „właściwe organy nie podejmują żadnych decyzji, które miałyby negatywne skutki prawne dla danej osoby lub znacząco wpływałyby na jej sytuację, wyłącznie na podstawie automatycznego przetwarzania danych PNR”, a decyzje te „nie mogą zostać podjęte w oparciu o rasę ani pochodzenie etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, stan zdrowia, życie seksualne ani orientację seksualną danej osoby”. Podobnie jak wskazałem w pkt 227 niniejszej opinii w odniesieniu do art. 6 ust. 4 zdanie czwarte dyrektywy PNR, ów katalog powodów dyskryminacji należy uzupełnić poprzez dodanie do niego podstaw wymienionych w art. 21 karty, których wyraźnie nie wskazano.

232. Co się zaś tyczy bezpieczeństwa danych PNR, art. 6 ust. 8 dyrektywy PNR przewiduje, że przechowywanie, przetwarzanie i analiza tych danych przez JIP odbywa się wyłącznie w bezpiecznym miejscu lub bezpiecznych miejscach na terytorium państw członkowskich.

– *Wnioski w przedmiocie szóstego pytania prejudycjalnego*

233. Biorąc pod uwagę całość powyższych rozważań, i z zastrzeżeniem wykładni zaproponowanej w szczególności w pkt 213, 219, 220, 222, 227, 228, 230 i 231 niniejszej opinii, jestem zdania, że zautomatyzowane przetwarzanie danych PNR w ramach wstępnej oceny, o której mowa w art. 6 ust. 2 lit. a) dyrektywy PNR, spełnia wymogi jasności i precyzji oraz jest ograniczone do tego, co absolutnie konieczne.

v) W przedmiocie przechowywania danych PNR (ósmie pytanie prejudycjalne)

234. W ósmym pytaniu prejudycjalnym sąd odsyłający zwraca się do Trybunału o wyjaśnienie, czy art. 12 dyrektywy PNR w związku z art. 7, 8 i art. 52 ust. 1 karty należy interpretować w ten sposób, że stoi on na przeszkodzie ustawodawstwu krajowemu, które przewiduje ogólny termin przechowywania danych PNR 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.

235. Artykuł 12 ust. 1 dyrektywy PNR przewiduje, że dane PNR są zatrzymywane w bazie danych „przez okres pięciu lat od przekazania ich do JIP w państwie członkowskim, na którego terytorium ma miejsce przylot lub z którego terytorium ma miejsce odlot”. Zgodnie z ust. 2 tego artykułu po upływie sześciomiesięcznego „początkowego okresu zatrzymania”²²⁷ dane PNR są depersonalizowane przez maskowanie pewnych informacji, które mogłyby posłużyć do bezpośredniej identyfikacji osoby, której dane dotyczą. Zgodnie z ust. 3 tego artykułu, po upływie rzeczonoego sześciomiesięcznego okresu ujawnienie pełnych danych PNR, w tym elementów zamaskowanych, jest dozwolone tylko wtedy, gdy istnieje „uzasadnienie”, by sądzić, że jest to konieczne do celów, o których mowa w art. 6 ust. 2 lit. b) dyrektywy PNR, oraz uzyskano zgodę organu sądowego lub innego organu krajowego właściwego na mocy prawa krajowego do ustalenia, czy warunki ujawnienia zostały spełnione. Wreszcie, ust. 4 tego artykułu przewiduje, że po upływie pięcioletniego okresu, o którym mowa w ust. 1, dane PNR zostają usunięte w sposób trwały.

236. Z powyższego wynika, że dyrektywa PNR sama określa system przechowywania danych PNR, w tym długość okresu ich przechowywania, ustalając go na pięć lat²²⁸, w związku z czym państwa członkowskie co do zasady nie dysponują w tym względzie żadnymi uprawnieniami dyskrecjonalnymi, co zostało zresztą potwierdzone przez Komisję. W tych okolicznościach, jak już miałem okazję zauważyć, ósmie pytanie prejudycjalne, choć sformułowane jako pytanie dotyczące wykładni, wymaga w rzeczywistości, aby Trybunał wypowiedział się w przedmiocie zgodności tego systemu z kartą.

237. Zasadą ogólną w dziedzinie ochrony danych osobowych jest to, że dane te nie powinny być przechowywane w formie umożliwiającej bezpośrednią lub pośrednią identyfikację osoby, której dane dotyczą, przez okres dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane²²⁹. Ponadto z utrwalonego orzecznictwa wynika, że akt przewidujący

²²⁷ Definicja ta jest zawarta w motywie 25 dyrektywy PNR.

²²⁸ Sformułowanie zawarte w motywie 37 dyrektywy PNR, zgodnie z którym „zatrzymanie danych PNR w JIP przez okres nieprzekraczający pięciu lat, po upływie którego dane powinny zostać usunięte” (wyróżnienie własne), nie pozwala moim zdaniem na zakwestionowanie jasnego brzmienia art. 12 ust. 1 tej dyrektywy.

²²⁹ Zobacz, w odniesieniu do przetwarzania danych osobowych do celów wykrywania, zapobiegania przestępczości, prowadzenia postępowań przygotowawczych i ścigania przestępstw, art. 4 lit. e) i motyw 26 dyrektywy policyjnej. W sensie bardziej ogólnym zob. art. 5 ust. 1 lit. e) RODO oraz art. 5 ust. 4 lit. e) zmodernizowanej konwencji nr 108.

przechowywanie danych osobowych powinien w szczególności zawsze spełniać obiektywne kryteria ustanawiające związek między danymi osobowymi podlegającymi zatrzymaniu a zamierzonym celem²³⁰.

238. W opinii 1/15 Trybunał uznał w odniesieniu do danych zgromadzonych przy wjeździe do Kanady, że konieczny związek między danymi PNR a celem przewidywanej umowy PNR Kanada–UE istnieje w odniesieniu do wszystkich pasażerów lotniczych, dopóki przebywają oni na terytorium tego państwa trzeciego²³¹. Natomiast w odniesieniu do pasażerów lotniczych, którzy opuścili Kanadę i w odniesieniu do których nie zidentyfikowano zagrożeń w zakresie terroryzmu lub poważnych przestępstw międzynarodowych w chwili ich przybycia do tego państwa i aż do jego opuszczenia, Trybunał uznał, że taki związek, chociażby pośredni, uzasadniający przechowywanie ich danych PNR, nie istnieje²³². Trybunał uznał jednak, że przechowywanie tych danych może być dopuszczalne „w zakresie, w jakim w poszczególnych wypadkach zostaną zidentyfikowane elementy pozwalające na uznanie, że określone pasażerowie lotniczy mogliby – nawet po opuszczeniu Kanady – stanowić zagrożenie w rozumieniu zwalczania terroryzmu i poważnych przestępstw międzynarodowych”²³³.

239. Zasady ustanowione przez Trybunał w opinii 1/15 oznaczają po ich przeniesieniu na grunt dyrektywy PNR, że dane PNR lotów pozaunijnych zgromadzone przy wjeździe do Unii oraz dane PNR lotów wewnątrzunijnych zebrane przy wjeździe do danego państwa członkowskiego mogą być przechowywane, po ich wstępnej analizie w rozumieniu art. 6 ust. 2 lit. a) dyrektywy PNR, jedynie tak długo, jak długo pasażerowie ci przebywają na terytorium Unii lub tego państwa członkowskiego. Co się tyczy danych PNR lotów pozaunijnych zgromadzonych przy wyjeździe z Unii oraz danych PNR lotów wewnątrzunijnych zgromadzonych przy wyjeździe z danego państwa członkowskiego, dane te mogą co do zasady być przechowywane, po dokonaniu wspomnianej wstępnej oceny, wyłącznie w odniesieniu do pasażerów, w przypadku których obiektywne elementy pozwalają na wykazanie istnienia zagrożenia w zakresie zwalczania terroryzmu i poważnej przestępczości²³⁴.

240. Rządy i instytucje, które przedstawiły uwagi przed Trybunałem, ogólnie rzecz biorąc, sprzeciwiają się przeniesieniu na grunt niniejszej sprawy zasad ustanowionych w opinii 1/15 w dziedzinie przechowywania danych PNR. W tym względzie nie jest oczywiście wykluczone, że Trybunał zastosował kryterium związane z pobytem zainteresowanej osoby na terytorium Kanady ze względu na to, że orzekł w kwestii przechowywania danych osobowych na terytorium państwa trzeciego. Jest również możliwe, że stosowanie takiego kryterium w kontekście dyrektywy PNR mogłoby w konkretnych przypadkach prowadzić do tego, że ingerencja w prawa do poszanowania życia prywatnego i do ochrony danych osobowych byłaby potencjalnie dalej idąca w przypadku niektórych kategorii osób, w szczególności osób mających stałe miejsce zamieszkania w Unii i przemieszczających się w jej obrębie lub powracających do Unii po pobycie za granicą. Wreszcie, prawdą jest, jak podkreśliły niektóre państwa członkowskie i Rada, że wspomniane kryterium mogłoby okazać się trudne do zastosowania w praktyce, przynajmniej w odniesieniu do lotów wewnątrzunijnych.

²³⁰ Zobacz wyroki: Schrems I, pkt 93; Tele2 Sverige, pkt 110; opinia 1/15, pkt 191; a także wyrok La Quadrature du Net, pkt 133.

²³¹ Zobacz opinia 1/15, pkt 197.

²³² Zobacz opinia 1/15, pkt 205.

²³³ Zobacz opinia 1/15, pkt 207.

²³⁴ Chodzi tu o analogiczne zastosowanie pkt 187 i nast. opinii 1/15, ponieważ opinia ta odnosiła się wyłącznie do danych PNR zebranych przy wjeździe na terytorium Kanady.

241. Niemniej jednak, nawet gdyby odrzucić kryterium, którym Trybunał posłużył się w opinii 1/15, to przechowywanie całości danych PNR wszystkich pasażerów lotniczych, niezależnie od wyniku wstępnej oceny, o której mowa w art. 6 ust. 2 lit. a) dyrektywy PNR, i zupełnie niezależnie od ryzyka terroryzmu lub poważnej przestępczości określonego na podstawie obiektywnych i możliwych do zweryfikowania kryteriów, jest sprzeczne z utrwalonym orzecznictwem Trybunału przypomnianym w pkt 237 niniejszej opinii, które Trybunał zastosował w rzeczonej opinii. O ile zaś rozważania przedstawione w pkt 201–203 niniejszej opinii w ramach analizy czwartego pytania prejudycjalnego pozwalają moim zdaniem uzasadnić uogólnione i niezróżnicowane przekazywanie danych PNR oraz ich automatyczne przetwarzanie w ramach oceny wstępnej przewidzianej w art. 6 ust. 2 lit. a) dyrektywy PNR, o tyle stoję na stanowisku, że nie pozwalają one same w sobie na uzasadnienie uogólnionego i niezróżnicowanego zatrzymania tych danych również po przeprowadzeniu takiej oceny.

242. Pragnę ponadto zauważyć, że ten sam pięcioletni okres przechowywania ma zastosowanie zarówno w odniesieniu do walki z terroryzmem, jak i do walki z poważną przestępczością, a w ramach tego ostatniego celu – bez wyjątku do wszystkich przestępstw wymienionych w załączniku II. Tymczasem, jak wynika z rozważań przedstawionych w pkt 121 niniejszej opinii, wykaz ten jest szczególnie szeroki i obejmuje przestępstwa różnego rodzaju i wagi. W tym względzie należy zauważyć, że uzasadnienie proponowane praktycznie przez wszystkie państwa członkowskie i instytucje, które przedstawiły uwagi w niniejszym postępowaniu, oparte na długości i złożoności dochodzeń, zostało konkretnie przywołane jedynie w odniesieniu do przestępstw terrorystycznych i niektórych przestępstw o wybitnie transgranicznym charakterze, takich jak handel ludźmi lub handel środkami odurzającymi, a także, mówiąc bardziej ogólnie, w odniesieniu do niektórych form przestępczości zorganizowanej. Przypominam ponadto, że w opinii 1/15 podobne uzasadnienie Trybunał przyjął jedynie w odniesieniu do przechowywania danych PNR pasażerów lotniczych, co do których istnieje obiektywne ryzyko w zakresie zwalczania terroryzmu lub poważnych przestępstw międzynarodowych, w przypadku których zatrzymanie danych przez pięć lat uznano za niewykraczające poza to, co jest absolutnie konieczne²³⁵. Stwierdzono natomiast, że nie może ono usprawiedliwiać „trwałego przechowywania danych PNR wszystkich pasażerów lotniczych [...] do celów ewentualnego dostępu do rzeczonych danych niezależnie od jakiegokolwiek związku ze zwalczani[em] terroryzmu i poważnych przestępstw międzynarodowych”²³⁶.

243. Niewątpliwie – jak podkreślają Rada, Parlament i Komisja, a także wszystkie rządy, które przedstawiły uwagi w przedmiocie ósmego pytania prejudycjalnego – dyrektywa PNR przewiduje określone gwarancje zarówno w odniesieniu do przechowywania danych PNR, które po upływie początkowego sześciomiesięcznego terminu są częściowo maskowane, jak i w odniesieniu do ich wykorzystania w okresie zatrzymania, które uzależnione jest od spełnienia rygorystycznych warunków. Po pierwsze jednak, pragnę zauważyć, że z jednej strony projekt umowy PNR Kanada–UE również przewidywał system depersonalizacji danych PNR poprzez maskowanie²³⁷, lecz z drugiej strony, chociaż taka depersonalizacja, jak podkreśla w szczególności komitet doradczy konwencji nr 108²³⁸, może zmniejszyć ryzyko związane z przedłużonym okresem przechowywania danych, jak na przykład ryzyko nadużycia dostępu, to jednak dane zamaskowane nadal umożliwiają identyfikację osób i zachowują charakter danych osobowych,

²³⁵ Zobacz opinia 1/15, pkt 209.

²³⁶ Zobacz opinia 1/15, pkt 205.

²³⁷ Projekt umowy PNR Kanada–UE przewidywał maskowanie nazwisk wszystkich pasażerów po upływie 30 dni od ich otrzymania przez Kanadę i maskowanie innych informacji wyraźnie wymienionych po upływie dwóch lat od otrzymania, zob. art. 16 pkt 3 projektu umowy PNR Kanada–UE analizowanego przez Trybunał oraz opinia 1/15, pkt 30.

²³⁸ Zobacz opinia z dnia 19 sierpnia 2016 r., s. 9.

których przechowywanie powinno być również ograniczone w czasie, aby uniemożliwić prowadzenie uogólnionego nadzoru w sposób trwały. W tym względzie pragnę zauważyć, że pięcioletni okres przechowywania powoduje, iż znaczna liczba pasażerów, w szczególności pasażerów przemieszczających się na terytorium Unii, będzie praktycznie zawsze znajdować się w kartotece. Po drugie, co się tyczy ograniczeń w wykorzystywaniu danych, pragnę zauważyć, że przechowywanie danych osobowych i dostęp do takich danych stanowią odrębne ingerencje w prawa podstawowe do poszanowania życia prywatnego i do ochrony danych osobowych, które wymagają niezależnych uzasadnień. O ile istnienie daleko idących gwarancji w zakresie dostępu do przechowywanych danych pozwala całościowo ocenić wpływ środka nadzoru na wspomniane prawa podstawowe, o tyle gwarancje te nie pozwalają na wyeliminowanie ingerencji związanych z długotrwałym przechowywaniem w sposób uogólniony.

244. Jeśli chodzi o argument Komisji, zgodnie z którym przechowywanie danych PNR wszystkich pasażerów lotniczych jest konieczne, aby umożliwić JIP wykonanie zadania wskazanego w art. 6 ust. 2 lit. c) dyrektywy PNR, polegającego na aktualizacji lub tworzeniu nowych kryteriów stosowanych przy sprawdzaniach dokonywanych na podstawie ust. 3 lit. b) tego samego artykułu, pragnę zauważyć, że chociaż precyzja tych kryteriów zależy w części od ich porównania z zachowaniami „normalnymi”, to jednak muszę stwierdzić, iż należy je opracowywać na podstawie zachowań „przestępczych”. Taki argument, który zresztą podniosła jedynie ograniczona liczba państw członkowskich, moim zdaniem nie może mieć decydującego znaczenia, które, jak się wydaje, przypisuje mu Komisja, i sam w sobie uzasadniać uogólnione przechowywanie danych PNR wszystkich pasażerów lotniczych w formie nieanonimowej.

245. Biorąc pod uwagę powyższe rozważania, w celu zapewnienia wykładni art. 12 ust. 1 dyrektywy PNR, która byłaby zgodna z art. 7, 8 i art. 52 ust. 1 karty, przepis ten należy moim zdaniem interpretować w ten sposób, że przechowywanie danych PNR, dostarczonych do JIP przez przewoźników lotniczych, w bazie danych przez okres pięciu lat od ich przekazania do JIP państwa członkowskiego, na którego terytorium znajduje się punkt przylotu lub odlotu, jest dozwolone, po przeprowadzeniu wstępnej oceny na podstawie art. 6 ust. 2 lit. a) tejże dyrektywy, jedynie w zakresie, w jakim na podstawie obiektywnych kryteriów wykazano związek między tymi danymi a walką z terroryzmem lub poważną przestępczością. Uogólnione i nieodróżnicowane przechowywanie danych PNR w formie niezdepersonalizowanej może być uzasadnione, w drodze analogii do rozwiązań przyjętych przez Trybunał w tym samym orzecznictwie, jedynie w obliczu poważnego zagrożenia dla bezpieczeństwa państw członkowskich, które okaże się rzeczywiste i aktualne lub przewidywalne, związanego na przykład z działalnością terrorystyczną, i pod warunkiem, że okres przechowywania danych jest ograniczony do tego, co absolutnie konieczne.

246. Granice środka polegającego na przechowywaniu, o którym mowa w art. 12 ust. 1 dyrektywy PNR, można określić na przykład na podstawie oceny zagrożeń lub na podstawie doświadczenia zdobytego przez właściwe organy krajowe, pozwalającego na uwzględnienie konkretnych połączeń lotniczych, określonych schematów podróży, agencji, przy pomocy których dokonywane są rezerwacje, lub też kategorii osób lub danych obszarów geograficznych, zidentyfikowanych na podstawie elementów obiektywnych i niedyskryminacyjnych, w zgodzie z rozstrzygnięciami Trybunału w orzecznictwie dotyczącym przechowywania metadanych komunikatów elektronicznych²³⁹. Ponadto, analogicznie do opinii 1/15, należy przyjąć, że konieczny związek między danymi PNR a celem zamierzonym przez dyrektywę PNR istnieje tak

²³⁹ Zobacz w szczególności wyrok La Quadrature du Net, pkt 148, 149.

długo, jak długo pasażerowie lotniczy znajdują się w Unii (lub w danym państwie członkowskim) lub odbywają podróż wyjazdową. To samo dotyczy danych pasażerów, które doprowadziły do zweryfikowanego wyniku pozytywnego.

247. Na zakończenie analizy ósmego pytania prejudycjalnego pragnę poświęcić kilka uwag zasadom regulującym dostęp do danych PNR i ich wykorzystywanie po przeprowadzeniu wstępnej oceny, o której mowa w art. 6 ust. 2 lit. a) dyrektywy PNR, a przed ich depersonalizacją po upływie początkowego sześciomiesięcznego okresu przechowywania danych przewidzianego w art. 12 ust. 2 dyrektywy PNR.

248. Z lektury art. 6 ust. 2 lit. b) w związku z art. 12 ust. 3 dyrektywy PNR wynika, że w tym początkowym okresie niezdepersonalizowane dane PNR lub rezultat ich przetwarzania mogą zostać ujawnione właściwym organom zgodnie z pierwszym z tych przepisów, bez zachowania warunków określonych w lit. a) i b) drugiego z tych przepisów²⁴⁰. Artykuł 6 ust. 2 lit. b) dyrektywy PNR stanowi bowiem jedynie, że wnioski właściwych organów o ich przetwarzanie i ujawnienie muszą być „należycie uzasadnione” i „oparte na wystarczających podstawach”.

249. Zgodnie z utrwalonym orzecznictwem przypomnianym przez Trybunał w opinii 1/15 uregulowanie Unii nie może ograniczać się do stawiania wymogu, by dostęp organu do legalnie przechowywanych danych osobowych odpowiadał jednemu z celów tego uregulowania, lecz powinno również określać materialne i formalne przesłanki regulujące takie wykorzystywanie²⁴¹, w szczególności w tym celu, by chronić rzeczne dane przed ryzykiem nadużyć²⁴². W opinii tej Trybunał orzekł, że wykorzystanie danych PNR po ich sprawdzeniu w momencie przybycia pasażerów lotniczych do Kanady i podczas ich pobytu w tym państwie powinno opierać się na nowych okolicznościach uzasadniających takie wykorzystanie²⁴³, uściślając, że „jeżeli istnieją obiektywne elementy pozwalające na uznanie, że dane PNR jednego lub większej liczby pasażerów lotniczych mogłyby rzeczywiście przyczynić się do realizacji celu polegającego na zwalczaniu przestępstw terrorystycznych i poważnych przestępstw międzynarodowych, wykorzystanie tych danych nie wykracza poza granice tego, co ściśle konieczne”²⁴⁴. Odsyłając przez analogię do pkt 120 wyroku *Tele2 Sverige*, Trybunał orzekł, że w celu zagwarantowania w praktyce pełnego przestrzegania warunków „kluczowe jest, by wykorzystywanie podczas pobytu pasażerów lotniczych w Kanadzie zatrzymanych danych PNR było co do zasady, z wyjątkiem nagłych, należycie uzasadnionych wypadków, uzależnione od uprzedniej kontroli dokonywanej bądź przez sąd, bądź przez niezależny organ administracyjny, oraz by rozstrzygnięcie tego sądu lub tego organu było wydawane w następstwie uzasadnionego wniosku właściwych organów złożonego w szczególności w ramach postępowań mających na celu zapobieganie przestępstwom, ich wykrywanie lub ściganie”²⁴⁵. Trybunał uzależnił zatem możliwość wykorzystania danych PNR przechowywanych po ich sprawdzeniu w związku z podróżą lotniczą od spełnienia podwójnego warunku, jednocześnie materialnego – istnienia obiektywnych powodów uzasadniających takie wykorzystanie, i proceduralnego – kontroli ze strony sądu lub niezależnego organu administracyjnego. Przyjęta przez Trybunał wykładnia, zgoła nie „kontekstowa”, stanowi zastosowanie w dziedzinie danych PNR orzecznictwa wynikającego w szczególności z wyroków *Digital Rights* i *Tele2 Sverige*.

²⁴⁰ To samo dotyczy wniosków JIP innych państw członkowskich o ujawnienie danych PNR na podstawie art. 9 ust. 2 dyrektywy PNR.

²⁴¹ Zobacz opinia 1/15, pkt 192 i przytoczone tam orzecznictwo. Ostatnio zob. wyrok *Privacy international*, pkt 77; analogicznie wyrok Prokuratuur, pkt 49 i przytoczone tam orzecznictwo.

²⁴² Zobacz opinia 1/15, pkt 200.

²⁴³ Zobacz opinia 1/15, pkt 200.

²⁴⁴ Zobacz opinia 1/15, pkt 201.

²⁴⁵ Zobacz opinia 1/15, pkt 202.

250. System ustanowiony przez dyrektywę PNR, który w ciągu pierwszych sześciu miesięcy przechowywania danych PNR po dokonaniu wstępnej oceny, o której mowa w art. 6 ust. 2 lit. a) tej dyrektywy, zezwala na potencjalnie wielokrotne ujawnianie i przetwarzanie danych PNR bez odpowiednich gwarancji proceduralnych oraz wystarczająco jasnych i precyzyjnych przepisów materialnych określających przedmiot i zasady różnych ingerencji, nie spełnia zaś wymogów określonych przez Trybunał w opinii 1/15. Nie wydaje się również odpowiadać wymogowi wykorzystywania danych PNR w sposób ograniczony do tego, co absolutnie konieczne.

251. Proponuję zatem, aby Trybunał dokonał wykładni art. 6 ust. 2 lit. b) dyrektywy PNR w ten sposób, że przetwarzanie danych na podstawie tego przepisu, które następuje w początkowym sześciomiesięcznym okresie przewidzianym w art. 12 ust. 2 tej dyrektywy, spełnia wymogi określone przez Trybunał w opinii 1/15.

252. Jeśli chodzi o pierwszą przesłankę, o charakterze materialnym, od której Trybunał uzależnił możliwość późniejszego wykorzystywania danych PNR, jestem zdania, że pojęcia „uzasadnienia” w rozumieniu art. 12 ust. 3 lit. a) dyrektywy PNR oraz „wystarczających podstaw” w rozumieniu art. 6 ust. 2 lit. b) tej dyrektywy można bez trudu interpretować w ten sposób, że wnioski właściwych organów, o których mowa w tych przepisach, powinny wskazywać „obiektywne elementy pozwalające na uznanie, że dane PNR jednego lub większej liczby pasażerów lotniczych mogłyby rzeczywiście przyczynić się do realizacji celu polegającego na zwalczaniu przestępstw terrorystycznych i poważnych przestępstw [...]”²⁴⁶.

253. Co się tyczy drugiej przesłanki, o charakterze proceduralnym, moim zdaniem należy interpretować art. 6 ust. 2 lit. b) dyrektywy PNR w związku z jej art. 12 ust. 3 i w świetle art. 7, 8 i art. 52 ust. 1 karty w ten sposób, że wymóg uprzedniej zgody ze strony organu sądowego lub niezależnego organu administracyjnego przewidziany w art. 12 ust. 3 lit. b) tej dyrektywy ma zastosowanie do każdej operacji przetwarzania danych PNR na podstawie wspomnianego art. 6 ust. 2 lit. b).

4. Wnioski w przedmiocie pytań prejudycjalnych drugiego, trzeciego, czwartego, szóstego i ósmego

254. Na podstawie całości powyższych rozważań proponuję, aby Trybunał stwierdził nieważność pkt 12 załącznika I w zakresie, w jakim wśród kategorii danych PNR, które przewoźnicy lotniczy są zobowiązani przekazywać do JIP zgodnie z art. 8 dyrektywy PNR, uwzględnia on „uwagi ogólne”, i stwierdził, że analiza pytań prejudycjalnych drugiego, trzeciego, czwartego, szóstego i ósmego nie wykazała innych elementów mogących mieć wpływ na ważność tej dyrektywy, z zastrzeżeniem przyjęcia wykładni przepisów tej dyrektywy postulowanej w pkt 153, 160, 161–164, 219, 228, 239 i 251 niniejszej opinii.

255. W świetle proponowanej przeze mnie odpowiedzi na pytania prejudycjalne dotyczące ważności dyrektywy PNR nie ma potrzeby uwzględnienia złożonego między innymi przez Radę wniosku o utrzymanie w mocy skutków dyrektywy PNR, na wypadek gdyby Trybunał postanowił w całościowo lub częściowo stwierdzić nieważność całej dyrektywy PNR, abstrahując od wszelkich innych rozważań.

²⁴⁶ Zobacz podobnie opinia 1/15, pkt 201.

C. W przedmiocie piątego pytania prejudycjalnego

256. W piątym pytaniu prejudycjalnym sąd odsyłający zwraca się w istocie do Trybunału o wyjaśnienie, czy art. 6 dyrektywy PNR w związku z art. 7, 8 i art. 52 ust. 1 karty należy interpretować w ten sposób, że stoi on na przeszkodzie ustawodawstwu krajowemu, które za cel przetwarzania danych PNR uznaje monitorowanie działalności wywiadowczej służb wywiadowczych i bezpieczeństwa. Z postanowienia odsyłającego wynika, że działalność ta to działalność prowadzona przez służbę bezpieczeństwa państwa oraz główną służbę wywiadowczą i bezpieczeństwa w ramach zadań związanych z ochroną bezpieczeństwa narodowego.

257. Jak wskazałem w pkt 113 i 114 niniejszej opinii, ograniczenie celów przetwarzania danych osobowych jest podstawową gwarancją, która musi być zachowana, aby ingerencje w prawa podstawowe ustanowione w art. 7 i 8 karty nie wykraczały poza to, co jest konieczne i proporcjonalne w rozumieniu orzecznictwa Trybunału. Wyjaśniłem już również w odniesieniu do ingerencji w te prawa podstawowe, przewidzianych w dyrektywie PNR, że prawodawca Unii miał obowiązek ustanowienia jasnych i precyzyjnych reguł dotyczących zakresu i stosowania środków będących źródłem tego rodzaju ingerencji w celu poszanowania zasad legalności i proporcjonalności, zapisanych w szczególności w art. 52 ust. 1 karty.

258. Tymczasem art. 1 ust. 2 dyrektywy PNR wyjaśnia, że dane PNR zebrane zgodnie z ową dyrektywą „mogą być przetwarzane wyłącznie w celach zapobiegania przestępstwom terrorystycznym i poważnej przestępczości oraz ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, jak przewidziano w art. 6 ust. 2 lit. a), b) i c)” tej dyrektywy. Zgodnie z tym przepisem JIP przetwarzają dane PNR wyłącznie w celu dokonania wstępnej oceny pasażerów lotniczych [art. 6 ust. 2 lit. a)], odpowiadania na indywidualne wnioski właściwych organów [art. 6 ust. 2 lit. b)] oraz aktualizacji lub tworzenia nowych kryteriów stosowanych przy ocenach przeprowadzanych na podstawie art. 6 ust. 3 lit. b) [art. 6 ust. 2 lit. a)]. W odniesieniu do tych trzech przypadków wyraźnie przypomniano cele wskazane w art. 1 ust. 2 dyrektywy PNR w dziedzinie zwalczania terroryzmu i poważnej przestępczości.

259. Ponadto art. 7 ust. 4 tej dyrektywy uściśla, że nie tylko przetwarzanie danych PNR przewidziane w jej art. 6, lecz również dalsze przetwarzanie tych danych oraz wyniki tego przetwarzania przez właściwe organy państw członkowskich muszą być ograniczone „wyłącznie do określonych celów, jakimi są zapobieganie przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywanie, prowadzenie postępowań przygotowawczych w ich sprawie lub ich ściganie”.

260. Wyczerpujący charakter określenia celów realizowanych przez dyrektywę PNR jasno wynika z brzmienia jej art. 1 ust. 2 i znajduje potwierdzenie, poza wskazanymi już art. 6 ust. 2 i art. 7 ust. 4 tej dyrektywy, w szeregu artykułów i motywów tej dyrektywy, które systematycznie wiążą poszczególne etapy procesu dostępu, przetwarzania, przechowywania i udostępniania danych PNR tylko z tymi konkretnymi celami²⁴⁷.

²⁴⁷ Zobacz w szczególności art. 4, art. 7 ust. 1 i 2, art. 9 ust. 2, art. 10 ust. 2, art. 12 ust. 4 dyrektywy PNR; zob. między innymi motywy 6, 9, 10, 11, 15, 23, 25, 35 i 38 tej dyrektywy. Przypominam ponadto, że projekt dyrektywy PNR stanowił w motywie 28, iż „[n]iniejsza dyrektywa nie wpływa na możliwość ustanowienia przez państwa członkowskie, w swoim prawie krajowym, systemu gromadzenia danych PNR i zarządzania tymi danymi do celów innych niż te określone w niniejszej dyrektywie [...]”. W ostatecznym tekście dyrektywy PNR wyjaśnienia tego jednak nie powtórzono.

261. Zarówno z brzmienia art. 1 ust. 2 dyrektywy PNR, jak i z jego wykładni w świetle zasad legalności i proporcjonalności, które nakazują ograniczenie w sposób wyczerpujący celów środków będących źródłem ingerencji w prawa podstawowe do poszanowania życia prywatnego i ochrony danych osobowych, wynika, że wszelkie rozszerzenia celów przetwarzania danych PNR poza cele bezpieczeństwa wyraźnie wymienione w tym przepisie są sprzeczne z dyrektywą PNR.

262. Ów zakaz rozszerzania celów realizowanych przez dyrektywę odnosi się moim zdaniem w szczególności do działalności służb bezpieczeństwa i wywiadowczych państw członkowskich, w tym ze względu na brak przejrzystości charakteryzujący ich modus operandi. W tej kwestii zgadzam się z Komisją, że służby te nie powinny co do zasady mieć bezpośredniego dostępu do danych PNR. W tym kontekście uważam, że godna ubolewania jest już sama okoliczność, iż członkami krajowych JIP mogą być, jak ma to miejsce w przypadku belgijskiego JIP, oddelegowani funkcjonariusze służb bezpieczeństwa²⁴⁸.

263. Na podstawie powyższych rozważań na piąte pytanie prejudycjalne należy moim zdaniem odpowiedzieć, że dyrektywę PNR, a w szczególności jej art. 1 ust. 2 i art. 6, należy interpretować w ten sposób, że stoi ona na przeszkodzie ustawodawstwu krajowemu, które dopuszcza monitorowanie określonej działalności służb wywiadowczych i bezpieczeństwa jako cel przetwarzania danych PNR, w zakresie, w jakim w ramach takiego celu krajowa JIP jest zobowiązana do przetwarzania tych danych, przekazywania ich oraz wyniku ich przetwarzania rzeczonym służbom do celów innych niż cele wyczerpująco wskazane w art. 1 ust. 2 tej dyrektywy, czego ustalenie należy do sądu krajowego.

D. W przedmiocie siódmego pytania prejudycjalnego

264. W pytaniu siódmym sąd odsyłający dąży w istocie do ustalenia, czy art. 12 ust. 3 lit. b) dyrektywy PNR należy interpretować w ten sposób, że JIP stanowi „właściwy organ krajowy” w rozumieniu tego przepisu, który może zezwolić na ujawnienie pełnych danych PNR po upływie początkowego sześciomiesięcznego okresu od przekazania tych danych.

265. Przypominam, że art. 12 ust. 2 dyrektywy PNR przewiduje, iż po upływie okresu sześciomiesięcznego dane PNR są depersonalizowane przez maskowanie pewnych danych, które mogłyby posłużyć do bezpośredniej identyfikacji pasażera, którego dane dotyczą. Po upływie tego okresu ujawnienie takich pełnych danych jest dozwolone wyłącznie na warunkach przewidzianych w art. 12 ust. 3, a w szczególności gdy na ich ujawnienie uzyskano wcześniej zgodę „organu sądowego” [art. 12 ust. 3 lit. b) ppkt (i)] lub „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” [art. 12 ust. 3 lit. b) ppkt (ii)].

266. Większość rządów, które przedstawiły uwagi na piśmie w niniejszym postępowaniu, nie wypowiedziała się w przedmiocie siódmego pytania prejudycjalnego. Rząd czeski uważa, podobnie jak Komisja, że art. 12 ust. 3 dyrektywy PNR nie należy interpretować w ten sposób, że

²⁴⁸ Możliwość taką dopuszcza jednak art. 4 ust. 3 dyrektywy PNR, zgodnie z którym „[p]racownicy JIP mogą być oddelegowani z właściwych organów”, przynajmniej w zakresie, w jakim służby wywiadowcze i bezpieczeństwa danego państwa członkowskiego można uznać za właściwe organy w rozumieniu art. 7 ust. 2 tej dyrektywy.

JIP może stanowić „właściwy organ krajowy”. Natomiast rządy francuski, belgijski²⁴⁹, irlandzki, hiszpański i cypryjski takiej wykładni się sprzeciwiają. Uważają zasadniczo, że żaden przepis dyrektywy PNR ani prawa Unii nie stoi na przeszkodzie włączeniu JIP do grona właściwych organów krajowych w rozumieniu art. 12 ust. 2 lit. b) ppkt (ii) wspomnianej dyrektywy, a JIP ze względu na swój charakter jest organem wystarczająco niezależnym, aby wydawać zgody na przetwarzanie danych PNR.

267. Ze swej strony pragnę zauważyć, po pierwsze, że z brzmienia art. 12 ust. 3 lit. b) dyrektywy PNR, a w szczególności z użycia spójnika „lub” łączącego dwa przypadki w ppkt (i) i (ii) tego przepisu, wynika, że prawodawca Unii zamierzał umieścić na tej samej płaszczyźnie kontrolę sprawowaną przez organ krajowy, o którym mowa w ppkt (ii), oraz kontrolę sprawowaną przez organ sądowy, o którym mowa w ppkt (i). Stąd wniosek, że wspomniany organ krajowy powinien cechować się takim poziomem niezależności i bezstronności, aby sprawowaną przez niego kontrolę można było uznać za alternatywę porównywalną z kontrolą, której może dokonać organ sądowy²⁵⁰.

268. Po drugie, z prac przygotowawczych nad dyrektywą PNR wynika, że prawodawca Unii z jednej strony nie przyjął wniosku Komisji o powierzenie dyrektorowi JIP zadania w postaci udzielania zgody na ujawnienie pełnych danych PNR²⁵¹, a z drugiej strony wydłużył do sześciu miesięcy pierwotny okres zatrzymania tych danych zaproponowany przez tę instytucję, który wynosił 30 dni. To właśnie w tym kontekście, który charakteryzuje poszukiwanie równowagi między okresem zatrzymania przed depersonalizacją danych PNR a warunkami, jakim podlega ich demaskowanie po upływie tego okresu, należy widzieć decyzję prawodawcy Unii o uzależnieniu pełnego dostępu do danych PNR od spełnienia bardziej rygorystycznych wymogów proceduralnych w porównaniu z warunkami początkowo przewidzianymi przez Komisję oraz o powierzeniu niezależnemu organowi zadania sprawdzenia, czy warunki ujawnienia zostały spełnione.

269. Po trzecie, jak słusznie zauważyła Komisja, z systematyki dyrektywy PNR wynika, że ratio legis procedury uzyskiwania zgody, przewidzianej w art. 12 ust. 3 dyrektywy PNR, polega na powierzeniu bezstronnemu podmiotowi trzeciemu zadania polegającego na dokonaniu w każdym konkretnym przypadku wyważenia praw zainteresowanych osób z celem tej dyrektywy polegającym na ściganiu karnym.

270. Po czwarte, z orzecznictwa Trybunału wynika, że podmiot odpowiedzialny za przeprowadzenie uprzedniej kontroli wymaganej w celu wydania zgody właściwym organom krajowym na dostęp do danych osobowych, które są przechowywane zgodnie z prawem, powinien dysponować wszelkimi uprawnieniami i gwarancjami niezbędnymi do pogodzenia poszczególnych wchodzących w grę interesów i praw. Trybunał wyjaśnił również, że podmiot ów musi posiadać status pozwalający mu działać przy wykonywaniu swoich obowiązków w sposób obiektywny i bezstronny i w tym celu powinien pozostawać poza jakimkolwiek wpływem

²⁴⁹ Odnosząc się do wątpliwości wyrażonych przez rząd belgijski w kwestii właściwości Trybunału do udzielenia odpowiedzi na siódme pytanie prejudycjalne należy zauważyć, że zgodnie z brzmieniem tego pytania sąd odsyłający zwraca się do Trybunału o dokonanie wykładni art. 12 ust. 3 dyrektywy PNR, a nie w przedmiocie zgodności ustawodawstwa krajowego z tym przepisem. W każdym razie z utrwalonego orzecznictwa wynika, że Trybunał może dostarczyć sądowi krajowemu wskazówek pozwalających im na dokonanie oceny takiej zgodności (zob. w szczególności wyrok z dnia 7 września 2016 r., ANODE, C-121/15, EU:C:2016:637, pkt 54 i przytoczone tam orzecznictwo).

²⁵⁰ Zobacz w tym względzie wyrok z dnia 5 listopada 2019 r., Komisja/Polska (Niezależność sądów powszechnych) (C-192/18, EU:C:2019:924, pkt 108–110).

²⁵¹ Artykuł 9 ust. 2 zdanie czwarte projektu dyrektywy PNR stanowił, że „[z]ezwolenie na dostęp do pełnych danych PNR uzyskuje jedynie dyrektor jednostki do spraw informacji o pasażerach [...]”.

z zewnątrz²⁵². W szczególności ze względu na wymóg niezależności, zwłaszcza w dziedzinie prawa karnego, organ odpowiedzialny za uprzednią kontrolę powinien mieć status strony trzeciej w stosunku do organu wnoszącego o udzielenie dostępu do danych, tak aby nie był zaangażowany w prowadzenie dochodzenia karnego, a także powinien zajmować neutralną pozycję wobec stron postępowania karnego²⁵³.

271. Należy zaś stwierdzić, że JIP nie daje wszystkich gwarancji niezawisłości i bezstronności, które powinien posiadać organ odpowiedzialny za uprzednią kontrolę przewidzianą w art. 12 ust. 3 dyrektywy PNR. JIP są bowiem bezpośrednio związane z organami właściwymi do zapobiegania przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania. Zgodnie z art. 4 ust. 1 dyrektywy PNR JIP sam jest takim organem lub jego działem. Ponadto ust. 3 tego artykułu przewiduje, że pracownicy JIP mogą być oddelegowani z właściwych organów. Tak jest w szczególności w przypadku belgijskiego JIP, w którego skład zgodnie z art. 14 ustawy PNR wchodzi między innymi delegowani członkowie służb policyjnych, głównej służby wywiadowczej i bezpieczeństwa oraz administracji generalnej cel i podatków akcyzowych.

272. Ogólnie rzecz biorąc, członkowie JIP niewątpliwie powinni oferować wszelkie gwarancje uczciwości, kompetencji, przejrzystości i niezależności, a państwa członkowskie powinny w razie potrzeby zapewnić przestrzeganie tych gwarancji w konkretnych przypadkach, biorąc pod uwagę więzi łączące ich z instytucjami macierzystymi, w szczególności w celu uniknięcia sytuacji, w której właściwe organy, w których strukturze członkowie ci się pierwotnie znajdowali, mają dostęp bezpośrednio do bazy danych PNR, a nie wyłącznie do wyników kwerend przeprowadzonych przez JIP. Niemniej jednak członkowie JIP, którzy zostali oddelegowani z właściwych organów w rozumieniu art. 7 ust. 2 dyrektywy PNR, w sposób nieunikniony utrzymują związki ze swoimi służbami macierzystymi w okresie oddelegowania i zachowują swój status, nawet jeśli podlegają funkcjonalnemu i hierarchicznemu zwierzchnictwu funkcjonariusza kierującego JIP.

273. Wniosek, zgodnie z którym JIP nie jest organem krajowym w rozumieniu art. 12 ust. 3 lit. b) ppkt (ii) dyrektywy PNR, potwierdza ponadto okoliczność, że zgodnie z tym przepisem inspektor ochrony danych odnośnej JIP powinien być „poinformowany” o wniosku o ujawnienie i przeprowadza „weryfikację ex post”. W przypadku bowiem, gdyby JIP był upoważniony, jako „inny organ krajowy”, do zatwierdzenia wniosku o ujawnienie danych na podstawie art. 12 ust. 3 dyrektywy PNR, inspektor ochrony danych, który jest między innymi zobowiązany, zgodnie z art. 5 ust. 1 tej dyrektywy, do stosowania odpowiednich gwarancji dotyczących przetwarzania danych PNR, byłby informowany o wniosku o udzielenie dostępu w chwili jego złożenia, a jego weryfikacja siłą rzeczy miałaby miejsce ex ante²⁵⁴.

274. W świetle powyższych rozważań proponuję, aby Trybunał odpowiedział na siódme pytanie prejudycjalne, że art. 12 ust. 3 lit. b) dyrektywy PNR należy interpretować w ten sposób, że JIP nie stanowi „innego właściwego organu krajowego” w rozumieniu tego przepisu.

²⁵² Wyrok Prokuratuur, pkt 52, 53.

²⁵³ Wyrok Prokuratuur, pkt 53, 54. Zobacz podobnie wyrok Big Brother Watch, §§ 349–352.

²⁵⁴ Artykuł 9 ust. 2 zdanie czwarte projektu dyrektywy PNR stanowił, że „[z]ezwolenie na dostęp do pełnych danych PNR uzyskuje jedynie dyrektor jednostki do spraw informacji o pasażerach”.

E. W przedmiocie dziewiątego pytania prejudycjalnego

275. W dziewiątym pytaniu prejudycjalnym sąd odsyłający zwraca się w istocie do Trybunału z pytaniem, po pierwsze, czy dyrektywa API jest zgodna z art. 3 ust. 2 TUE i z art. 45 karty w zakresie, w jakim ma ona zastosowanie do lotów wewnątrz Unii, a po drugie, czy dyrektywę tę w związku z art. 3 ust. 2 TUE i art. 45 karty należy interpretować w ten sposób, że stoi ona na przeszkodzie ustawodawstwu krajowemu, które w celu zwalczania nielegalnej imigracji i ulepszenia kontroli granicznych zezwala na system gromadzenia i przetwarzania danych pasażerów, co może powodować w sposób pośredni przywrócenie kontroli na granicach wewnętrznych.

276. Z postanowienia odsyłającego wynika, że to pytanie prejudycjalne związane jest z analizą drugiego zarzutu skargi, podniesionego przez LDH posiłkowo. Zarzut ten, dotyczący naruszenia art. 22 konstytucji belgijskiej w związku z art. 3 ust. 2 TUE i art. 45 karty, jest skierowany przeciwko art. 3 § 1, art. 8 § 2 i rozdziałowi 11, w szczególności art. 28–31 ustawy PNR. O ile pierwszy z tych artykułów określa w sposób ogólny przedmiot tej ustawy, uściślając, że ustawa ta „określa obowiązki przewoźników i operatorów turystycznych związane z przekazywaniem danych pasażerów udających się na terytorium kraju, przybywającym z niego lub przez nie przejeżdżającym”, o tyle jej art. 8 § 2 stanowi, iż „na warunkach przewidzianych w rozdziale 11 [ustawy], dane pasażerów są również przetwarzane w celu ulepszenia kontroli osób na granicach zewnętrznych oraz w celu zwalczania nielegalnej imigracji”. Zgodnie z art. 29 § 1 ustawy PNR do tych celów są przekazywane służbom policyjnym odpowiedzialnym za kontrolę graniczną oraz urzędowi ds. cudzoziemców jedynie „dane pasażerów”, o których mowa w art. 9 § 1 pkt 18 tej ustawy (a mianowicie dane API wymienione w pkt 18 dyrektywy PNR), dotyczące trzech kategorii pasażerów. Chodzi o „pasażerów, którzy zamierzają wjechać lub wjechali na terytorium przez granice zewnętrzne Belgii”, „pasażerów, którzy zamierzają opuścić terytorium lub opuścili terytorium przez granice zewnętrzne Belgii” oraz o „pasażerów, którzy planują przejazd, znajdują się lub przejechali przez międzynarodową strefę tranzytu położoną w Belgii”²⁵⁵. Z art. 29 § 3 ustawy PNR wynika, że rzeczne dane są przekazywane przez JIP służbom policyjnym odpowiedzialnym za kontrolę graniczną i urzędowi ds. cudzoziemców (Belgia) „niezwłocznie po ich zarejestrowaniu w bazie danych pasażerów” i są niszczone po upływie dwudziestu czterech godzin po ich przekazaniu. Zgodnie z tym przepisem po upływie tego terminu urząd ds. cudzoziemców może również zwrócić się do JIP z uzasadnionym wnioskiem o dostęp do tych samych danych, jeżeli jest to konieczne w ramach jego zadań ustawowych. W związku z tym ramy prawne, w które wpisuje się dziewiąte pytanie prejudycjalne, wykraczają poza cele dyrektywy PNR, zważywszy na cel przetwarzania danych, o którym mowa w art. 28 i 29 ustawy PNR, lecz wiążą się z celami dyrektywy API. Ponadto, jak wynika w szczególności z akt sprawy złożonych w sekretariacie Trybunału, drugi zarzut LDH opiera się na wykładni przepisów rozdziału 11 ustawy PNR, zgodnie z którą przepisy te mają zastosowanie również w przypadku przekraczania granic wewnętrznych Belgii.

277. Pierwsza część dziewiątego pytania prejudycjalnego opiera się na błędnym założeniu i moim zdaniem nie wymaga odpowiedzi ze strony Trybunału. Z art. 3 ust. 1 dyrektywy API w związku z jej art. 2 lit. b) i d) wynika bowiem jednoznacznie, że dyrektywa ta nakłada na przewoźników lotniczych obowiązek przesyłania danych API organom odpowiedzialnym za kontrolę osób na granicach zewnętrznych jedynie w odniesieniu do lotów, które wprowadzają pasażerów przez autoryzowane przejścia graniczne w celu przekraczania granic zewnętrznych państw członkowskich z państwami trzecimi. Podobnie, art. 6 ust. 1 tej dyrektywy przewiduje

²⁵⁵ Ustawa PNR, art. 29 ust. 1 i 2.

przetwarzanie jedynie danych API dotyczących tych lotów. Ponadto, o ile prawdą jest, że dyrektywa PNR przewiduje możliwość rozszerzenia przez państwa członkowskie obowiązku przekazywania zebranych danych API również na przewoźników lotniczych obsługujących loty wewnątrzunijne, o tyle rozszerzenie to należy rozumieć jako pozbawione wpływu na dyrektywę API²⁵⁶. W ramach dyrektywy PNR przekazane dane API będą przetwarzane tylko w ramach celów ścigania przewidzianych w tej dyrektywie. Natomiast motyw 34 dyrektywy PNR przewiduje, że nie narusza ona obecnych przepisów Unii o trybie prowadzenia kontroli granicznych ani przepisów Unii regulujących wjazd na terytorium Unii i wyjazd z tego terytorium, a art. 6 ust. 9 zdanie drugie tej dyrektywy stanowi, że jeżeli sprawdzenie na mocy ust. 2 tego artykułu jest dokonywane w odniesieniu do lotów wewnątrzunijnych pomiędzy państwami członkowskimi, do których stosuje się kodeks graniczny Schengen²⁵⁷, skutki takiego sprawdzenia nie naruszają tego rozporządzenia.

278. Przeformułowanie tej części dziewiątego pytania prejudycjalnego, jak sugeruje posiłkowo Komisja, w ten sposób, że dotyczy ona zgodności z postanowieniami traktatu i karty nie dyrektywy API, lecz dyrektywy PNR, a w szczególności jej art. 2, oznaczałoby nie tylko zmianę aktu prawnego, w odniesieniu do którego sąd odsyłający zwrócił się o ocenę ważności, lecz również wykraczałoby poza ramy prawne, w jakich to pytanie prejudycjalne się sytuje. Jak bowiem wyjaśniłem, przepisy rozdziału 11 ustawy PNR, przeciwko któremu skierowano drugi zarzut skargi, dokonują transpozycji dyrektywy API, a nie dyrektywy PNR.

279. Na wypadek gdyby Trybunał dokonał takiego przeformułowania, ograniczę się do kilku poniższych refleksji dotyczących w szczególności kwestii tego, czy wstępną ocenę – jaką państwa członkowskie mogą przeprowadzać na podstawie danych PNR pasażerów lotów wewnątrzunijnych, w ramach możliwości, którą dysponują zgodnie z art. 2 dyrektywy PNR – można uznać za równoważną „odprawie granicznej” w rozumieniu art. 23 lit. a) kodeksu granicznego Schengen²⁵⁸. Po pierwsze, chociaż wstępna ocena danych PNR nie odbywa się „na przejściu granicznym” ani w „chwili przekraczania granicy”, lecz wcześniej, jest ona jednak dokonywana „z powodu” mającego nastąpić przekroczenia granicy. Po drugie, zgodnie z art. 2 dyrektywy PNR państwa członkowskie są upoważnione do rozszerzenia wstępnej oceny danych PNR przewidzianej w art. 6 ust. 2 lit. a) dyrektywy PNR na pasażerów wszystkich lotów wewnątrz europejskich, niezależnie od zachowania osób, których dane dotyczą, i okoliczności wskazujących ewentualnie na ryzyko naruszenia bezpieczeństwa publicznego. Rzeczona wstępna ocena ma ponadto charakter systematyczny. Tymczasem nie wydaje się, aby jeden czy drugi z tych elementów odpowiadał warunkom, o których mowa w art. 23 lit. a) zdanie drugie ppkt (ii), (iii) i (iv) kodeksu granicznego Schengen²⁵⁹. Po trzecie, co się tyczy warunków, o których mowa w lit. a) zdanie drugie ppkt (i) i (iii) tego artykułu, zastanawiam się, czy ocena wstępna na podstawie art. 6 ust. 2 lit. a) dyrektywy PNR nie ma wspólnego celu, przynajmniej częściowo, z odprawą graniczną przeprowadzaną na podstawie art. 8 ust. 2 lit. b), art. 8 ust. 3 lit. a) ppkt (vi)

²⁵⁶ Zobacz motyw 10 dyrektywy PNR.

²⁵⁷ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/399 z dnia 9 marca 2016 r. w sprawie unijnego kodeksu zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen) (Dz.U. 2016, L 77, s. 1, zwany dalej „kodeksem granicznym Schengen”).

²⁵⁸ Artykuł 23 lit. a) kodeksu granicznego Schengen stanowi, że wykonywanie uprawnień policyjnych nie może być w szczególności uznawane za równoważne dokonywaniu odprawy granicznej, jeżeli środki policyjne: „(i) nie mają na celu kontroli granicznej; (ii) są oparte na informacjach i doświadczeniu policyjnym o charakterze ogólnym, dotyczących potencjalnych zagrożeń dla bezpieczeństwa publicznego i mają na celu w szczególności walkę z przestępczością transgraniczną; (iii) są opracowywane i stosowane w sposób zdecydowanie odróżniający je od rutynowej odprawy osób na granicach zewnętrznych; (iv) są przeprowadzane na podstawie kontroli wyrwykowej”.

²⁵⁹ Zobacz analogicznie wyrok z dnia 13 grudnia 2018 r., *Touring Tours und Travel i Sociedad de transportes* (C-412/17 i C-474/17, EU:C:2018:1005, pkt 61 i przytoczone tam orzecznictwo), a także postanowienie z dnia 4 czerwca 2020 r., *FU* (C-554/19, niepublikowane, EU:C:2020:439, pkt 49–56).

i art. 8 ust. 3 lit. g) ppkt (iii) kodeksu granicznego Schengen, zmienionego rozporządzeniem 2017/458, a przede wszystkim, czy różni się ona wyraźnie od tejże systematycznej odprawy pod kątem szczegółowych warunków jej przeprowadzania²⁶⁰. W tym względzie pragnę zauważyć, że art. 8 ust. 2e i art. 8 ust. 3 lit. ia) tego kodeksu uściślają, iż wspomnianych odpraw „można dokonywać z wyprzedzeniem, w oparciu o dane dotyczące pasażerów, otrzymane zgodnie z dyrektywą [API] lub zgodnie z innymi przepisami prawa Unii lub prawa krajowego”. Niemniej prawdą jest, że celem dyrektywy PNR nie jest „zapewnienie, że można zezwolić na wjazd osób na terytorium państwa członkowskiego lub na opuszczenie tego terytorium” lub „uniemożliwienie uniknięcia przez osoby odprawy granicznej”, które to elementy Trybunał uznał za cele „kontroli granicznej” zgodnie z kodeksem granicznym Schengen²⁶¹, ponieważ dyrektywa PNR służy wyłącznie ściganiu przestępstw. Ponadto art. 23 lit. a) zdanie drugie pkt (ii) wspomnianego kodeksu przewiduje wyraźnie, że wykonywanie uprawnień policyjnych nie może być uznawane za równoważne dokonywaniu odprawy granicznej, jeżeli kontrole te mają na celu w szczególności walkę z przestępczością transgraniczną²⁶². Wreszcie Trybunał powinien uwzględnić w swojej ocenie także okoliczność, podkreśloną w szczególności przez Komisję, że art. 2 dyrektywy PNR upoważnia państwa członkowskie jedynie do nałożenia na przewoźników lotniczych obowiązku przekazywania danych PNR, które zgromadzili w normalnym toku swojej działalności, a zatem nie przewiduje obowiązku analogicznego do obowiązku przewidzianego w dyrektywie API w odniesieniu do przekraczania granic zewnętrznych.

280. Co się tyczy drugiej części dziewiątego pytania prejudycjalnego, uważam, podobnie jak Komisja, że należy ją rozumieć w ten sposób, iż odnosi się ona do przekraczania granic wewnętrznych i zmierza do uzyskania od Trybunału wyjaśnień umożliwiających sądowi odsyłającemu ocenę zgodności przepisów rozdziału 11 ustawy PNR ze zniesieniem kontroli na granicach wewnętrznych państw członkowskich w strefie Schengen.

281. W tym względzie, biorąc pod uwagę niewielką ilość informacji, którymi dysponuje Trybunał, mogę jedynie stwierdzić, że przepisy rozdziału 11 ustawy PNR mogą być zgodne z prawem Unii, a w szczególności z art. 67 ust. 2 TFUE, tylko jeżeli są interpretowane w ten sposób, że dotyczą wyłącznie przekazywania i przetwarzania danych API pasażerów przekraczających granice zewnętrzne Belgii z państwami trzecimi.

282. Jeżeli Trybunał postanowi przeformułować drugą część dziewiątego pytania prejudycjalnego w ten sposób, że dotyczyć ona będzie wykładni dyrektywy PNR w powiązaniu z przepisami rozdziału 11 ustawy PNR, ograniczę się do stwierdzenia, że przetwarzanie danych API przewidziane w art. 28 i 29 tej ustawy jest elementem systemu ustanowionego przez ustawodawcę belgijskiego w celu transpozycji dyrektywy PNR. I tak, po pierwsze, danymi API, które są przedmiotem przetwarzania, są dane wymienione w pkt 12 załącznika I do tej dyrektywy, a nie tylko dane wskazane w wykazie zawartym w art. 3 ust. 2 dyrektywy API. Po drugie, zgodnie z art. 29 § 1 ustawy PNR dane te są przekazywane służbom policyjnym odpowiedzialnym za kontrolę graniczną i urzędowi ds. cudzoziemców przez JIP – która jest odpowiedzialna za gromadzenie i przetwarzanie danych PNR wyłącznie w ramach celów realizowanych przez dyrektywę PNR – a nie, jak przewiduje dyrektywa API, bezpośrednio przez przewoźników lotniczych. Ponadto przekazywane są również dane pasażerów, którzy zamierzają opuścić terytorium belgijskie lub je opuścili, a odbiorcami tych danych nie są jedynie organy prowadzące

²⁶⁰ W tym względzie pragnę zauważyć, że w pkt 188 opinii 1/15 Trybunał stwierdził, iż „identyfikacja za pomocą danych PNR pasażerów mogących stanowić zagrożenie dla bezpieczeństwa publicznego stanowi część kontroli granicznych”.

²⁶¹ Wyrok z dnia 13 grudnia 2018 r., Touring Tours und Travel i Sociedad de transportes (C-412/17 i C-474/17, EU:C:2018:1005, pkt 55 i przytoczone tam orzecznictwo).

²⁶² Zobacz podobnie w szczególności postanowienie z dnia 4 czerwca 2020 r., FU (C-554/19, niepublikowane, EU:C:2020:439, pkt 46).

kontrole graniczne, lecz również urząd ds. cudzoziemców odpowiedzialny za zarządzanie populacją imigrantów i zwalczanie nielegalnej imigracji. Po trzecie, wydaje się, że na podstawie art. 29 § 4 akapit drugi ustawy PNR urząd ds. cudzoziemców może kierować do JIP wnioski o dostęp do danych API nawet po zakończeniu ich przetwarzania w związku z przekroczeniem granic przez pasażerów, których dane dotyczą. W tym sensie urząd ten jest de facto traktowany jak właściwy organ na podstawie art. 7 dyrektywy PNR, mimo że nie ma charakteru takiego organu i nie widnieje w wykazie tych organów przekazanym Komisji przez Belgię. Takiego zaś pomieszczenia systemów przewidzianych w dyrektywie API i w dyrektywie PNR nie można moim zdaniem zaakceptować, ponieważ narusza ono zasadę ograniczenia celów zapisaną w art. 1 ust. 2 dyrektywy PNR²⁶³.

283. Na podstawie całości powyższych rozważań proponuję, aby Trybunał odpowiedział na dziewiąte pytanie prejudycjalne w ten sposób, że art. 3 ust. 1 dyrektywy API, na podstawie którego państwa członkowskie podejmują niezbędne kroki do ustanowienia zobowiązania dla przewoźników do przesyłania na wnioski organów odpowiedzialnych za przeprowadzanie kontroli osób na granicach zewnętrznych, przed końcem kontroli, informacji dotyczących pasażerów, o których mowa w ust. 2 tego artykułu, w związku z art. 2 lit. b) i d) tej dyrektywy, dotyczy tylko pasażerów wprowadzanych przez autoryzowane przejścia graniczne w celu przekraczania granic zewnętrznych państw członkowskich z państwami trzecimi. Przepisy krajowe, które jedynie w celu ulepszenia kontroli osób na granicach zewnętrznych oraz w celu zwalczania nielegalnej imigracji rozszerzają ów obowiązek na dane osób przekraczających granice wewnętrzne danego państwa członkowskiego samolotem lub innymi środkami transportu, są sprzeczne z art. 67 ust. 2 TFUE i art. 22 kodeksu granicznego Schengen.

F. W przedmiocie dziesiątego pytania prejudycjalnego

284. W dziesiątym pytaniu prejudycjalnym sąd odsyłający zwraca się w istocie do Trybunału o wyjaśnienie, czy w przypadku gdyby doszedł do wniosku, że ustawa PNR narusza art. 7, 8 i art. 52 ust. 1 karty, mógłby tymczasowo utrzymać w mocy skutki tej ustawy w celu uniknięcia braku pewności prawa i umożliwienia dalszego wykorzystywania wcześniej zgromadzonych i przechowywanych danych do celów określonych w ustawie.

285. Trybunał odpowiedział na pytanie o takiej samej treści w wyroku *La Quadrature du Net*, dotyczącym przechowywania metadanych komunikatów elektronicznych, ogłoszonym po złożeniu wniosku o wydanie orzeczenia w trybie prejudycjalnym w niniejszej sprawie. W wyroku tym Trybunał przypominał najpierw swoje orzecznictwo, zgodnie z którym do naruszenia pierwszeństwa i jednolitego stosowania prawa Unii doszłoby, gdyby sądy krajowe były uprawnione do przyznania, choćby tymczasowo, przepisom krajowym pierwszeństwa przed prawem Unii, z którym te przepisy są sprzeczne. Następnie przypominał, że w wyroku z dnia 29 lipca 2019 r. w sprawie *Inter-Environnement Wallonie i Bond Beter Leefmilieu Vlaanderen*²⁶⁴, w której rozważana była zgodność z prawem środków przyjętych z naruszeniem ustanowionego w prawie Unii obowiązku przeprowadzenia uprzedniej oceny oddziaływania przedsięwzięcia na środowisko i na teren chroniony, orzekł, iż sąd krajowy może wyjątkowo utrzymać w mocy skutki takich środków, w przypadku gdy prawo krajowe na to zezwala, jeżeli to utrzymanie w mocy jest uzasadnione nadrzędnymi względami związanymi z koniecznością uniknięcia rzeczywistego i poważnego zagrożenia polegającego na przerwaniu dostaw energii elektrycznej w danym

²⁶³ W dokumencie roboczym z 2020 r. dotyczącym dyrektywy API Komisja podkreśla również problematyczny charakter nakładania się systemów przetwarzania danych PNR i API na poziomie krajowym, zob. s. 20.

²⁶⁴ C-411/17, EU:C:2019:622, pkt 175, 176, 179, 181.

państwie członkowskim, przy czym wspomniane utrzymanie w mocy może obejmować jedynie okres ściśle niezbędny do usunięcia tej niezgodności z prawem. Trybunał doszedł jednak do wniosku, że w przeciwieństwie do pominięcia obowiązku proceduralnego takiego jak uprzednia ocena oddziaływania przedsięwzięcia w szczególnej dziedzinie ochrony środowiska, naruszenie praw podstawowych zapisanych w art. 7 i 8 karty nie może być przedmiotem konwalidacji w drodze procedury analogicznej do tej, o której mowa w ww. wyroku²⁶⁵. Takiej samej odpowiedzi należy moim zdaniem udzielić na dziesiąte pytanie prejudycjalne w niniejszym postępowaniu.

286. Ponieważ zarówno sąd odsyłający, jak i rząd belgijski, a także Komisja i Rada zastanawiają się nad kwestią tego, czy prawo Unii stoi na przeszkodzie wykorzystywaniu w ramach postępowania karnego informacji lub dowodów uzyskanych dzięki wykorzystaniu danych PNR zebranych, przetwarzanych lub zatrzymywanych w sposób niezgodny z prawem Unii, pragnę przypomnieć, że w pkt 222 wyroku *La Quadrature du Net* Trybunał wyjaśnił, iż w obecnym stanie prawa Unii wyłącznie do prawa krajowego należy, co do zasady, określenie przepisów dotyczących dopuszczalności i oceny, w ramach postępowania karnego wszczętego przeciwko osobom podejrzanym o popełnienie poważnych przestępstw, informacji i dowodów uzyskanych w wyniku takiego przechowywania danych sprzecznego z prawem Unii, z zastrzeżeniem poszanowania zasady równowagi i skuteczności. W odniesieniu do tej ostatniej Trybunał orzekł, że zasada ta nakłada na krajowy sąd karny obowiązek nieuwzględniania informacji i dowodów uzyskanych w drodze uogólnionego i nieodróżnionego zatrzymywania danych o ruchu i danych o lokalizacji niezgodnego z prawem Unii w ramach postępowania karnego wszczętego przeciwko osobom podejrzanym o popełnienie przestępstwa, jeżeli osoby te nie są w stanie skutecznie ustosunkować się do tych informacji i dowodów, należących do dziedziny niepodlegającej rozpoznaniu przez sąd i mogących mieć decydujący wpływ na ocenę okoliczności faktycznych. Zasady te można również zastosować *mutatis mutandis* do okoliczności postępowania głównego.

IV. Wnioski

287. Na podstawie całości powyższych rozważań proponuję, aby na pytania prejudycjalne przedłożone przez *Cour constitutionnelle* (trybunał konstytucyjny, Belgia) Trybunał udzielił następującej odpowiedzi:

- 1) Artykuł 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 w sprawie ochrony danych), w związku z art. 2 ust. 2 lit. d) tego rozporządzenia, należy interpretować w ten sposób, że:
 - ma on zastosowanie do przepisów krajowych dokonujących 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, w zakresie, w jakim przepisy te regulują przetwarzanie danych PNR przez przewoźników lotniczych i przez inne podmioty gospodarcze, w tym przekazywanie danych PNR jednostkom do spraw informacji o pasażerach (JIP) wskazanym w art. 4 rzeczony dyrektywy, przewidziane w jej art. 8;

²⁶⁵ Zobacz wyrok *La Quadrature du Net*, pkt 217–219.

- nie ma on zastosowania do przepisów krajowych dokonujących transpozycji dyrektywy 2016/681 w zakresie, w jakim regulują one przetwarzanie danych do celów określonych w art. 1 ust. 2 tej dyrektywy przez właściwe organy krajowe, włączając w to JIP, oraz w odpowiednich przypadkach służby bezpieczeństwa i wywiadowcze zainteresowanego państwa członkowskiego;
 - ma on zastosowanie do przepisów krajowych dokonujących transpozycji dyrektywy Rady 2004/82/WE z dnia 29 kwietnia 2004 r. w sprawie zobowiązania przewoźników do przekazywania danych pasażerów i 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 w celu ulepszenia kontroli osób na granicach zewnętrznych oraz w celu zwalczania nielegalnej imigracji.
- 2) Punkt 12 załącznika I do dyrektywy 2016/681 jest nieważny w zakresie, w jakim wśród kategorii danych, które przewoźnicy lotniczy są zobowiązani przekazywać do JIP zgodnie z art. 8 tej dyrektywy, uwzględnia on „uwagi ogólne”.
 - 3) Analiza pytań drugiego, trzeciego, czwartego, szóstego i ósmego nie wykazała istnienia innych okoliczności, które mogłyby wpłynąć na ważność dyrektywy 2016/681.
 - 4) Punkt 12 załącznika I do dyrektywy 2016/681 w części, która nie została uznana za nieważną, należy interpretować w ten sposób, że obejmuje on jedynie informacje dotyczące małoletnich, które zostały w nim wyraźnie wymienione i które mają bezpośredni związek z lotem.
 - 5) Punkt 18 załącznika I do dyrektywy 2016/681 należy interpretować w ten sposób, że obejmuje on jedynie te uprzednie informacje o pasażerach, które są wyraźnie wymienione w tym punkcie oraz w art. 3 ust. 2 dyrektywy 2004/82, przy czym zostały one zebrane przez przewoźników lotniczych w normalnym toku ich działalności.
 - 6) Pojęcie „baz danych, które mają znaczenie” zapisane w art. 6 ust. 3 lit. a) dyrektywy 2016/681 należy interpretować w ten sposób, że obejmuje ono wyłącznie krajowe bazy danych zarządzane przez właściwe organy na podstawie art. 7 ust. 1 tej dyrektywy, jak również bazy danych Unii i międzynarodowe bezpośrednio wykorzystywane przez te organy w ramach wykonywania ich zadań. Rzeczne bazy danych powinny pozostawać w bezpośrednim i ścisłym związku z celami rzeczony dyrektywy polegającymi na zwalczaniu terroryzmu i poważnej przestępczości w tym znaczeniu, że zostały one opracowane do tych celów. W ramach transpozycji do prawa krajowego dyrektywy 2016/681 państwa członkowskie są zobowiązane do opublikowania wykazu tych baz danych i do jego aktualizowania.
 - 7) Artykuł 6 ust. 3 lit. b) dyrektywy 2016/681 należy interpretować w ten sposób, że stoi on na przeszkodzie stosowaniu w ramach zautomatyzowanego przetwarzania przewidzianego w tym przepisie systemów algorytmicznych mogących prowadzić bez interwencji człowieka do zmiany wcześniej ustalonych kryteriów będących podstawą przetwarzania, a które to systemy nie pozwalają na określenie w sposób jasny i przejrzysty powodów uzyskania wyniku pozytywnego w następstwie tego przetwarzania.

- 8) Wykładni art. 12 ust. 1 dyrektywy 2016/681, która byłaby zgodna z art. 7, 8 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej, należy dokonywać w ten sposób, że przechowywanie danych PNR, dostarczonych do JIP przez przewoźników lotniczych, w bazie danych przez okres pięciu lat od ich przekazania do JIP państwa członkowskiego, na którego terytorium znajduje się punkt przylotu lub odlotu, jest dozwolone, po przeprowadzeniu wstępnej oceny na podstawie art. 6 ust. 2 lit. a) tejże dyrektywy, jedynie w zakresie, w jakim na podstawie obiektywnych kryteriów wykazano związek między tymi danymi a walką z terroryzmem lub poważną przestępczością. Uogólnione i nieodróżnicowane przechowywanie tych danych PNR w formie niezdepersonalizowanej może być uzasadnione jedynie w obliczu poważnego zagrożenia dla bezpieczeństwa państw członkowskich, które okaże się rzeczywiste i aktualne lub przewidywalne, związanego na przykład z działalnością terrorystyczną, i pod warunkiem, że okres przechowywania danych jest ograniczony do tego, co absolutnie konieczne.
- 9) Artykuł 6 ust. 2 lit. b) dyrektywy 2016/681 należy interpretować w ten sposób, że ujawnianie danych PNR lub wyniku przetwarzania tych danych na podstawie owego przepisu, które następuje w początkowym sześciomiesięcznym okresie przewidzianym w art. 12 ust. 2 tej dyrektywy, powinno spełniać warunki określone w art. 12 ust. 3 lit. b) rzeczony dyrektywy.
- 10) Dyrektywę 2016/681, a w szczególności jej art. 1 ust. 2 i art. 6, należy interpretować w ten sposób, że stoi ona na przeszkodzie ustawodawstwu krajowemu, które dopuszcza monitorowanie określonej działalności służb wywiadowczych i bezpieczeństwa jako cel przetwarzania danych PNR, w zakresie, w jakim w ramach takiego celu krajowa JIP jest zobowiązana do przetwarzania tych danych, przekazywania ich oraz wyniku ich przetwarzania tym służbom do celów innych niż cele wyczerpująco wskazane w rzeczonym art. 1 ust. 2, czego ustalenie należy do sądu krajowego.
- 11) Artykuł 12 ust. 3 lit. b) dyrektywy 2016/681 należy interpretować w ten sposób, że JIP nie stanowi „innego właściwego organu krajowego” w rozumieniu tego przepisu.
- 12) Artykuł 3 ust. 1 dyrektywy 2004/82, na podstawie którego państwa członkowskie podejmują niezbędne kroki do ustanowienia zobowiązania dla przewoźników do przesyłania na wniosek organów odpowiedzialnych za przeprowadzanie kontroli osób na granicach zewnętrznych, przed końcem kontroli, informacji dotyczących pasażerów, o których mowa w ust. 2 tego artykułu, w związku z art. 2 lit. b) i d) tej dyrektywy, dotyczy tylko pasażerów wprowadzanych przez autoryzowane przejścia graniczne w celu przekraczania granic zewnętrznych państw członkowskich z państwami trzecimi. Przepisy krajowe, które jedynie w celu ulepszenia kontroli osób na granicach zewnętrznych oraz w celu zwalczania nielegalnej imigracji rozszerzają ów obowiązek na dane osób przekraczających granice wewnętrzne danego państwa członkowskiego samolotem lub innymi środkami transportu, są sprzeczne z art. 67 ust. 2 TFUE i art. 22 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/399 z dnia 9 marca 2016 r. w sprawie unijnego kodeksu zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen).
- 13) Sąd krajowy nie może zastosować przepisu prawa krajowego, który upoważnia go do ograniczenia w czasie skutków stwierdzenia niezgodności z prawem, którego ma on dokonać na mocy tego prawa w odniesieniu do ustawodawstwa krajowego nakładającego na przewoźników lotniczych, naziemnych i morskich oraz na operatorów turystycznych, w celu walki z terroryzmem i poważną przestępczością, obowiązek przekazywania danych PNR oraz przewidującego ogólne i nieodróżnicowane przetwarzanie i przechowywanie tych danych,

niezgodnie z art. 7, 8 i art. 52 ust. 1 karty praw podstawowych. Zgodnie z zasadą skuteczności krajowy sąd karny ma obowiązek nieuwzględniania informacji i dowodów uzyskanych na podstawie takich przepisów niezgodnych z prawem Unii w ramach postępowania karnego wszczętego przeciwko osobom podejrzanym o popełnienie aktów terroryzmu lub poważnej przestępczości, jeżeli osoby te nie są w stanie skutecznie ustosunkować się do tych informacji i dowodów, należących do dziedziny niepodlegającej rozpoznaniu przez sąd i mogących mieć decydujący wpływ na ocenę okoliczności faktycznych.