Zbiór Orzeczeń

OPINIA RZECZNIKA GENERALNEGO
YVES'A BOTA
przedstawiona w dniu 23 września 2015 r.[1]

Sprawa C-362/14

Maximillian Schrems
przeciwko
Data Protection Commissioner

[wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez High Court (Irlandia)]

Odesłanie prejudycjalne — Dane osobowe — Ochrona osób fizycznych w zakresie przetwarzania tych danych — Karta praw podstawowych Unii Europejskiej — Artykuły 7, 8 i 47 — Dyrektywa 95/46/WE — Artykuł 25 — Decyzja 2000/520/WE — Przekazywanie danych osobowych do Stanów Zjednoczonych — Ocena, czy stopień ochrony jest odpowiedni — Skarga osoby fizycznej, której dane zostały przekazane do państwa trzeciego — Krajowy organ nadzorczy — Uprawnienia

I – **Wprowadzenie**

1. Jak stwierdziła Komisja Europejska w swoim komunikacie z dnia 27 listopada 2013 r.[2], „[p]rzekazywanie danych osobowych jest ważnym i niezbędnym elementem stosunków transatlantyckich. Stanowi ono nieodłączną część transatlantyckiej wymiany handlowej, w szczególności jeżeli chodzi o nowe rozwijające się przedsiębiorstwa cyfrowe prowadzące działalność w takich dziedzinach, jak media społecznościowe lub chmura obliczeniowa, z czym wiąże się duża ilość danych przekazywanych z Unii Europejskiej do Stanów Zjednoczonych"[3].

2. Wymiana handlowa jest przedmiotem decyzji Komisji 2000/520/WE z **dnia 26 lipca 2000 r., przyjętej na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach bezpiecznej przystani oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA**[4]. Decyzja ta stanowi podstawę prawną dla przekazywania danych osobowych z Unii do tych przedsiębiorstw z siedzibą w Stanach Zjednoczonych, które przyjęły zasady dotyczące bezpiecznego transferu danych osobowych (zasady bezpiecznej przystani).

3. Omawiana decyzja ma obecnie sprostać wyzwaniu umożliwienia przepływu danych pomiędzy Unią a Stanami Zjednoczonymi przy jednoczesnym zapewnieniu wysokiego stopnia ochrony tych danych, jak wymaga tego prawo Unii.

1 — Język oryginału: francuski.

2 — **Komunikat Komisji do Parlamentu Europejskiego i Rady „Odbudowa zaufania do przepływów danych między Unią Europejską a Stanami Zjednoczonymi"** [COM(2013) 846 final].

3 — Strona 2.

4 — Dz.U. L 215, s. 7; sprostowanie Dz.U. 2001, L 115, s. 14.

4. Pewne ujawnione niedawno informacje wykazały bowiem istnienie amerykańskich programów gromadzenia informacji na znaczną skalę. Informacje te postawiły pod znakiem zapytania poszanowanie prawa Unii przy przekazywaniu danych osobowych do przedsiębiorstw z siedzibą w Stanach Zjednoczonych oraz ujawniły słabe punkty systemu bezpiecznej przystani.

5. W niniejszym wniosku o wydanie orzeczenia w trybie prejudycjalnym zwrócono się do Trybunału o wyjaśnienia co do tego, jakie stanowisko mają zająć krajowe organy nadzorcze i Komisja wobec napotykanych nieprawidłowości w stosowaniu decyzji 2000/520.

6. Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych [5] przewiduje w rozdziale IV zasady dotyczące przekazywania danych osobowych do państw trzecich.

7. W rozdziale tym, w art. 25 ust. 1 tej dyrektywy, zawarta została zasada, zgodnie z którą przekazywanie do państwa trzeciego danych osobowych poddawanych przetwarzaniu lub przeznaczonych do przetwarzania po ich przekazaniu może nastąpić tylko wówczas gdy, dane państwo trzecie zapewni odpowiedni stopień ochrony tych danych.

8. I odwrotnie, jak wskazał prawodawca unijny w motywie 57 tej dyrektywy, jeśli państwo trzecie nie zapewnia odpowiedniego stopnia ochrony, należy zakazać przekazywania danych osobowych do tego państwa.

9. Zgodnie z art. 25 ust. 2 dyrektywy 95/46 „[o]dpowiedni stopień ochrony danych zapewnianej przez państwo trzecie należy oceniać w świetle wszystkich okoliczności dotyczących operacji przekazania danych lub zbioru takich operacji; szczególną uwagę zwracać się będzie na charakter danych, cel i czas trwania proponowanych operacji przetwarzania danych, kraj pochodzenia i kraj ostatecznego przeznaczenia, przepisy prawa, zarówno ogólne jak i branżowe, obowiązujące w państwie trzecim oraz przepisy zawodowe i środki bezpieczeństwa stosowane w tym państwie”.

10. Na mocy art. 25 ust. 6 tej dyrektywy Komisja może stwierdzić, że państwo trzecie zapewnia, ze względu na swoje wewnętrzne ustawodawstwo lub zobowiązania międzynarodowe, odpowiedni stopień ochrony danych osobowych. Jeśli Komisja przyjmie taką decyzję, dane osobowe mogą być przekazywane do danego państwa trzeciego.

11. W wykonaniu tego przepisu Komisja przyjęła decyzję 2000/520. Z art. 1 ust. 1 tej decyzji wynika, że „zasady ochrony prywatności w ramach »bezpiecznej przystani«”, wprowadzane w życie zgodnie z wytycznymi zawartymi w „najczęściej zadawanych pytaniach” [6], są uważane za zapewniające odpowiedni poziom ochrony danych osobowych przekazywanych z Unii do przedsiębiorstw mających siedzibę w Stanach Zjednoczonych.

12. W konsekwencji decyzja 2000/520 upoważnia do przekazywania danych osobowych z państw członkowskich do tych przedsiębiorstw mających siedzibę w Stanach Zjednoczonych, które zobowiązały się do przestrzegania zasad bezpiecznej przystani.

13. Decyzja 2000/520 przewiduje w załączniku I szereg zasad, do przestrzegania których przedsiębiorstwa mogą dobrowolnie się zobowiązać, wraz z ograniczeniami i ze szczególnym systemem kontroli. Ilość przedsiębiorstw, które przyjęły ten tzw. kodeks postępowania, przekroczyła w 2013 r. 3200.

5 — Dz.U. L 281, s. 31. Dyrektywa zmieniona rozporządzeniem (WE) nr 1882/2003 Parlamentu Europejskiego i Rady z dnia 29 września 2003 r. (Dz.U. L 284, s. 1) (zwana dalej „dyrektywą 95/46”).

6 — Najczęściej zadawane pytania, zwane dalej „NZP”.

14. System bezpiecznej przystani opiera się na rozwiązaniu łączącym samocertyfikację i samoocenę dokonywaną przez przedsiębiorstwa prywatne z interwencją władz publicznych.

15. Zasady bezpiecznej przystani zostały opracowane „w konsultacji z kręgami przemysłowymi i publicznością w celu ułatwienia handlu między Stanami Zjednoczonymi a Unią Europejską […]. Są one przeznaczone do wyłącznego użytku przez amerykańskie organizacje otrzymujące dane osobowe z Unii […], w celu zakwalifikowania ich jako »bezpiecznej przystani« i domniemania »adekwatności [odpowiedniego stopnia ochrony]«, jakie ta przystań stwarza” [7].

16. Wymienione w załączniku I do decyzji 2000/520 zasady bezpiecznej przystani przewidują w szczególności:

— obowiązek informowania, zgodnie z którym „[o]rganizacja musi poinformować osoby o celach, w jakich zbiera i wykorzystuje informacje o nich, o sposobie kontaktowania się z organizacją w celu zasięgnięcia informacji albo złożenia skargi, o rodzajach stron trzecich, którym ujawnia te informacje, oraz o możliwościach wyboru i środkach ograniczenia korzystania i ujawnienia tych informacji, oferowanych przez organizację tym osobom. Ogłoszenie to musi być sformułowane […] z chwilą, gdy osoby fizyczne są po raz pierwszy proszone o dostarczenie organizacji informacji osobowych lub też w jak [najkrótszym możliwym terminie], ale w każdym przypadku przed użyciem przez organizację takich informacji w celu innym niż ten, w którym były one pierwotnie zbierane albo przetwarzane przez organizację przekazującą lub zanim ujawni je po raz pierwszy stronie trzeciej” [8];

— obowiązek umożliwienia przez organizację zainteresowanym osobom dokonania wyboru, czy dane ich dotyczące mogą zostać ujawnione osobie trzeciej lub wykorzystane w celu niezgodnym z celem (celami), dla którego (których) były pierwotnie zbierane, lub na które osoba fizyczna wyraziła później zgodę. W przypadku informacji wrażliwych „muszą one mieć możliwość twierdzącego lub wyraźnego wyboru (wyrażenie zgody), jeżeli informacje mają być ujawnione stronie trzeciej lub mają być użyte w celu innym niż cele, dla których były pierwotnie zbierane, lub do których wykorzystania zainteresowana osoba później upoważniła poprzez wykorzystanie możliwości wyrażenia zgody” [9];

— zasady dotyczące dalszego przekazywania danych. Tak więc, „[w] celu ujawnienia informacji stronie trzeciej, organizacje muszą stosować zasady ogłoszenia i wyboru” [10];

— w zakresie bezpieczeństwa danych obowiązek „[o]rganizacji tworząc[ych], przechowując[ych], używając[ych] albo rozpowszechniając[ych] informacje osobowe […] podejmowa[nia] rozsądn[ych] środk[ów] ostrożności w celu ich ochrony przed utratą, niewłaściwym wykorzystaniem oraz nieuprawnionym dostępem, ujawnieniem, zmianą i zniszczeniem” [11];

— jeśli chodzi o integralność danych, obowiązek organizacji „podj[ęcia] […] właściw[ych] krok[ów], aby zapewnić wiarygodność dla celów, jakim mają służyć, dokładność, kompletność i aktualność” [12];

— że osoba, której dane organizacja przechowuje, musi co do zasady „mieć dostęp do [tych danych] i mieć możliwość poprawiania, zmieniania lub usuwania takich informacji, gdy są one nieprawidłowe” [13];

7 — Akapit drugi załącznika I do decyzji 2000/520.

8 — Zobacz załącznik I, „Ogłoszenie”.

9 — Zobacz załącznik I, „Wybór”.

10 — Zobacz załącznik I, „Dalsze przekazywanie danych”.

11 — Zobacz załącznik I, „Bezpieczeństwo”.

12 — Zobacz załącznik I, „Integralność danych”.

13 — Zobacz załącznik I, „Dostęp”.

— obowiązek wprowadzenia „procedur[…] postępowania zapewniając[ych] przestrzeganie zasad [bezpiecznej przystani], prawo odwoływania się osób, których dane dotyczą, które wskutek nieprzestrzegania zasad zostały poszkodowane, oraz konsekwencje wynikające dla organizacji z powodu nieprzestrzegania zasad [do przestrzegania których się zobowiązały]” [14].

17. Amerykańska organizacja zamierzająca zobowiązać się do przestrzegania zasad bezpiecznej przystani musi przewidzieć w swojej polityce ochrony prywatności, że ujawnia publicznie fakt zobowiązania się do przestrzegania tych zasad i rzeczywistego ich przestrzegania oraz do samocertyfikacji poprzez poinformowanie Departamentu Handlu Stanów Zjednoczonych, że przestrzega ona tych zasad [15].

18. Organizacje mogą przestrzegać zasad bezpiecznej przystani na wiele sposobów. Mogą one na przykład „przystąpi[ć] do programu samoregulacji ochrony prywatności [zarządzanego przez sektor prywatny], który przestrzega zasad” lub „zakwalifikować [się] poprzez rozwój swych własnych polityk samoregulacji przestrzegania ochrony prywatności pod warunkiem, że będą one zgodne z zasadami […]. Ponadto, organizacje podlegające ustawowemu, wykonawczemu, administracyjnemu lub innemu zbiorowi praw (lub przepisów) chroniącemu skutecznie prywatność osób fizycznych mogą się także kwalifikować do korzystania z przywilejów »bezpiecznej przystani«” [16].

19. Istnieje szereg mechanizmów, łączących prywatny arbitraż i kontrolę organów publicznych, służących weryfikacji poszanowania zasad bezpiecznej przystani. Kontrola może zatem zostać zapewniona poprzez system pozasądowego rozwiązywania sporów przez niezależną osobę trzecią. Co więcej, przedsiębiorstwa mogą podjąć współpracę z grupą Unii ds. ochrony danych. Wreszcie Federal Trade Commission (Federalna Komisja Handlu, zwana dalej „FTC”) na podstawie uprawnień przyznanych jej na mocy sekcji 5 Federal Trade Commission Act (ustawy o Federalnej Komisji Handlu) oraz Department of Transportation (ministerstwo transportu) na podstawie uprawnień przyznanych mu na mocy sekcji 41712 United States Code (kodeksu Stanów Zjednoczonych), zawartej w jego tytule 49, są właściwe do rozpatrywania skarg.

20. Zgodnie z akapitem czwartym załącznika I do decyzji 2000/520 przyjęcie zasad bezpiecznej przystani może być ograniczone w szczególności przez „wymaga[nia] bezpieczeństwa narodowego, interesu publicznego albo przestrzegania prawa [Stanów Zjednoczonych]” oraz przez „ustaw[ę], rozporządzenie[…] rządu albo [orzeczenie sądu], ustanawiając[e] sprzeczne obowiązki albo udzielając[e] wyraźnego upoważnienia, pod warunkiem że działając na mocy tego upoważnienia organizacja potrafi wykazać, że nieprzestrzeganie przez nią zasad jest ograniczone do zakresu koniecznego do zaspokojenia nadrzędnych uzasadnionych interesów wspieranych przez to upoważnienie” [17].

21. Ponadto możliwość wstrzymania przepływu danych przez właściwe organy państw członkowskich poddana jest licznym warunkom przewidzianym w art. 3 ust. 1 decyzji 2000/520.

22. Niniejszy wniosek o wydanie orzeczenia w trybie prejudycjalnym prowadzi do rozważenia znaczenia decyzji 2000/520 w świetle art. 7, 8 i 47 Karty praw podstawowych Unii Europejskiej (zwanej dalej „kartą”), a także art. 25 ust. 6 i art. 28 dyrektywy 95/46. Wniosek ten został przedstawiony w ramach sporu pomiędzy Maximillianem Schremsem a Data Protection Commissioner (komisarzem ds. ochrony danych, zwanym dalej „komisarzem”) dotyczącego odmowy przez komisarza rozpatrzenia skargi wniesionej przez M. Schremsa z tego powodu, że Facebook Ireland Ltd (zwana dalej „Facebook Ireland” lub „spółką Facebook Ireland”) przechowuje dane osobowe swoich użytkowników na serwerach znajdujących się w Stanach Zjednoczonych.

14 — Zobacz załącznik I, „Zapewnianie prawu skuteczności”.

15 — Artykuł 1 ust. 2 i 3 decyzji 2000/520. Zobacz także załącznik II, NZP 6.

16 — Akapit trzeci załącznika I.

17 — Zobacz także załącznik IV tytuł B.

23. Maximillian Schrems jest obywatelem austriackim mieszkającym w Austrii. Jest on użytkownikiem serwisu społecznościowego Facebook od 2008 r.

24. Od wszystkich użytkowników sieci Facebook mieszkających na terytorium Unii wymagane jest zawarcie umowy ze spółką Facebook Ireland, będącą spółką zależną spółki dominującej Facebook Inc., mającej siedzibę w Stanach Zjednoczonych (zwanej dalej „Facebook USA" lub „spółką Facebook USA"). Dane użytkowników spółki Facebook Ireland mieszkających na terytorium Unii są, w całości lub częściowo, przekazywane na serwery spółki Facebook USA, znajdujące się na terytorium Stanów Zjednoczonych, gdzie dane te są przechowywane.

25. W dniu 25 czerwca 2013 r. M. Schrems złożył skargę do komisarza, podnosząc w istocie, że prawo i praktyka Stanów Zjednoczonych nie zapewniają rzeczywistej ochrony danych przechowywanych na terytorium Stanów Zjednoczonych przed nadzorem państwa. Wynika to jakoby z ujawnianych przez E. Snowdena od maja 2013 r. informacji na temat działalności amerykańskich służb wywiadowczych, a w szczególności działalności National Security Agency (agencji bezpieczeństwa narodowego, zwanej dalej „NSA").

26. Z informacji tych wynika w szczególności, że NSA wprowadziła program o nazwie „PRISM", w ramach którego agencja ta uzyskała swobodny dostęp do masowych danych przechowywanych na serwerach znajdujących się w Stanach Zjednoczonych, posiadanych lub kontrolowanych przez szereg spółek działających w dziedzinie Internetu i technologii, takich jak Facebook USA.

27. Komisarz ocenił, że nie miał obowiązku rozpatrzenia tej skargi, ponieważ była ona pozbawiona podstawy prawnej. Uznał, że nie ma dowodów na to, iż NSA uzyskała dostęp do danych M. Schremsa. Ponadto skargę należało jego zdaniem odrzucić ze względu na decyzję 2000/520, w której Komisja stwierdziła, że Stany Zjednoczone zapewniają w ramach systemu bezpiecznej przystani odpowiedni stopień ochrony przekazywanych danych osobowych. Wszelkie kwestie dotyczące odpowiedniego stopnia ochrony tych danych w Stanach Zjednoczonych należy rozpatrywać zgodnie z tą decyzją, co uniemożliwiało zbadanie problemu podniesionego w skardze.

28. Komisarz odrzucił skargę na podstawie następującego ustawodawstwa krajowego.

29. Artykuł 10 ust. 1 Data Protection Act 1988 (ustawy z 1988 r. o ochronie danych), zmienionej Data Protection (Amendment) Act 2003 (ustawą z 2003 r. o ochronie danych) (zwanej dalej „ustawą o ochronie danych") przyznaje komisarzowi uprawnienie do rozpatrywania skarg oraz stanowi:

„a) Komisarz może zbadać lub zlecić zbadanie, czy przepisy niniejszej ustawy były, są lub mogą być naruszane w odniesieniu do danej osoby, w przypadku gdy osoba ta wniesie do niego skargę o naruszenie jednego z tych przepisów lub gdy komisarz uważa, że takie naruszenie może występować.

b) Kiedy osoba wnosi skargę do komisarza na podstawie lit. a) niniejszego ustępu, komisarz:

(i) rozpatruje skargę lub zleca jej rozpatrzenie, chyba że jest ona bezcelowa lub wynika ze złej wiary, oraz,

(ii) jeśli nie może uzyskać w rozsądnym terminie od zainteresowanych stron polubownego rozwiązania w przedmiocie skargi, powiadamia na piśmie skarżącego o decyzji podjętej w sprawie tej skargi, wskazując, że jeśli decyzja ta jest dla niego niekorzystna, skarżący może ją zaskarżyć do sądu na podstawie art. 26 niniejszej ustawy, w terminie 21 dni od dnia doręczenia powiadomienia".

30. W niniejszej sprawie komisarz stwierdził, że skarga M. Schremsa była „bezcelowa lub wynikała ze złej wiary" w tym znaczeniu, że była skazana na niepowodzenie ze względu na brak podstawy prawnej. Z tego powodu odmówił on rozpatrzenia tej skargi.

31. Artykuł 11 ustawy o ochronie danych reguluje przekazywanie danych osobowych poza terytorium krajowe. Artykuł 11 ust. 2 lit. a) tej ustawy przewiduje:

„Jeśli w ramach każdej procedury regulowanej niniejszą ustawą podniesiona zostaje kwestia:

(i) ustalenia, czy państwo lub terytorium położone poza Europejskim Obszarem Gospodarczym [(EOG)], do którego mają zostać przekazane dane osobowe, zapewnia odpowiedni stopień ochrony określony w ust. 1 niniejszego artykułu, oraz jeśli

(ii) Unia dokonała ustaleń w odniesieniu do rodzaju przekazania, o który chodzi,

to kwestia ta zostanie rozwiązana w zgodzie z tymi ustaleniami".

32. Artykuł 11 ust. 2 lit. b) ustawy o ochronie danych osobowych definiuje pojęcie ustaleń Unii w następujący sposób:

„W lit. a) niniejszego ustępu »ustalenia Unii« oznaczają ustalenia, jakie Komisja […] poczyniła na potrzeby art. 25 ust. 4 lub 6 dyrektywy [95/46], w ramach postępowania przewidzianego w art. 31 ust. 2 [tej dyrektywy], dla określenia, czy państwo lub terytorium położone poza [EOG] zapewniają odpowiedni stopień ochrony określony w ust. 1 niniejszego artykułu".

33. Komisarz zauważył, że decyzja 2000/520 stanowiła „ustalenia Unii" w rozumieniu art. 11 ust. 2 lit. a) ustawy o ochronie danych, tak więc na mocy tej ustawy każdą kwestię dotyczącą odpowiedniego stopnia ochrony danych w państwie trzecim, do którego te dane są przekazywane, należy rozpatrywać w zgodzie z tymi ustaleniami. Z uwagi na fakt, że istotą skargi wniesionej przez skarżącego była właśnie ta kwestia – a mianowicie że dane osobowe przekazywane były do państwa trzeciego, które w praktyce nie zapewnia odpowiedniego stopnia ochrony – komisarz przyjął, że owa kwestia nie podlega rozstrzygnięciu ze względu na charakter oraz na samo istnienie decyzji 2000/520.

34. Maximillian Schrems wniósł do High Court (wysokiego trybunału) skargę na decyzję komisarza odrzucającą jego skargę. Po zbadaniu dowodów przedstawionych w postępowaniu głównym sąd ten stwierdził, że nadzór elektroniczny i przechwytywanie danych osobowych służą realizacji koniecznych i niezbędnych celów interesu publicznego, mianowicie utrzymania bezpieczeństwa publicznego i zapobiegania ciężkim przestępstwom. High Court wskazał w tym względzie, że nadzór i przechwytywanie danych osobowych przekazywanych z Unii do Stanów Zjednoczonych służą realizacji uzasadnionych celów związanych ze zwalczaniem terroryzmu.

35. Według tego samego sądu informacje ujawnione przez E. Snowdena wskazują jednak na istotne przekroczenie uprawnień ze strony NSA i innych podobnych organów. O ile Foreign Intelligence Surveillance Court (sąd ds. nadzoru wywiadu, zwany dalej „FISC"), działający w ramach Foreign Intelligence Surveillance Act of 1978 (ustawy z 1978 r. o nadzorze nad obcymi służbami wywiadowczymi) [18], sprawuje nadzór, o tyle postępowanie przed nim jest tajne i niekontradyktoryjne. Co więcej, decyzje dotyczące dostępu do danych osobowych nie tylko podejmowane są na podstawie prawa amerykańskiego, ale też obywatele Unii nie mają żadnego skutecznego prawa do bycia wysłuchanym w przedmiocie nadzoru nad ich danymi i przechwytywania tych danych.

18 — Zobacz sekcja 702 tej ustawy, zmienionej Foreign Intelligence Surveillance Act of 2008 (ustawą z 2008 r. o nadzorze nad obcymi służbami wywiadowczymi). To w wykonaniu tej sekcji NSA utrzymuje bazę danych znaną jako „PRISM" (zob. Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection z dnia 27 listopada 2013 r.).

36. Z obszernych dokumentów towarzyszących oświadczeniom złożonym pod przysięgą w postępowaniu głównym jasno wynika, że prawdziwość znacznej części informacji ujawnionych przez E. Snowdena nie jest kwestionowana. High Court uznał w związku z tym, że po przekazaniu danych osobowych do Stanów Zjednoczonych NSA, a także inne amerykańskie agencje bezpieczeństwa, takie jak Federal Bureau of Investigation (Federalne Biuro Śledcze), mogą uzyskać dostęp do tych danych w ramach masowego i niezróżnicowanego nadzorowania oraz przechwytywania.

37. High Court stwierdził, że w prawie irlandzkim znaczenie konstytucyjnych praw do życia prywatnego i nienaruszalności mieszkania wymaga, aby wszelka ingerencja w te prawa była zgodna z wymogami przewidzianymi w ustawie i proporcjonalna. Masowy i niezróżnicowany dostęp do danych osobowych nie odpowiada w żaden sposób wymogowi proporcjonalności i należy go uważać za niezgodny z irlandzką konstytucją[19].

38. High Court wskazał, iż dla uznania przechwytywania wiadomości elektronicznych za konstytucyjne należy wykazać, że takie przechwytywanie wiadomości i kontrola określonych osób lub grup następują na podstawie obiektywnych przesłanek w interesie zapewniania bezpieczeństwa narodowego i zwalczania przestępczości oraz że istnieją odpowiednie i możliwe do zweryfikowania gwarancje.

39. High Court wskazał zatem, że gdyby niniejsza sprawa miała zostać rozstrzygnięta wyłącznie na podstawie prawa irlandzkiego, powstałby znaczny problem w odniesieniu do tego, czy Stany Zjednoczone „zapewniają odpowiedni stopień ochrony życia prywatnego oraz wolności i praw podstawowych" w rozumieniu art. 11 ust. 1 ustawy o ochronie danych. Wynika z tego, że na podstawie prawa irlandzkiego, a w szczególności jego wymogów konstytucyjnych, komisarz nie mógł odrzucić skargi M. Schremsa, lecz miał obowiązek zbadać tę kwestię.

40. W każdym razie High Court stwierdził, że tocząca się przed nim sprawa dotyczy stosowania prawa Unii w rozumieniu art. 51 ust. 1 karty, a więc zgodność z prawem decyzji komisarza należy oceniać z punktu widzenia prawa Unii.

41. Problem, z którym zetknął się komisarz, został wyjaśniony przez High Court w następujący sposób. Zgodnie z art. 11 ust. 2 lit. a) ustawy o ochronie danych komisarz musi rozpatrzyć kwestię odpowiedniego stopnia ochrony w państwie trzecim „zgodnie z" ustaleniami Unii dokonanymi przez Komisję na podstawie art. 25 ust. 6 dyrektywy 95/46. Wynika z tego, że komisarz nie może odstąpić od tych ustaleń. Skoro Komisja stwierdziła w swojej decyzji 2000/520, że Stany Zjednoczone gwarantują odpowiedni stopień ochrony w zakresie przetwarzania danych przez spółki, które zobowiązały się do przestrzegania zasad bezpiecznej przystani, komisarz zobowiązany jest siłą rzeczy do odrzucenia skargi podważającej nieodpowiedni stopień takiej ochrony.

42. Stwierdzając, że komisarz wykazał się skrupulatnym przestrzeganiem przepisów dyrektywy 95/46 i decyzji 2000/520, High Court wskazał, że M. Schrems podważa w rzeczywistości w większej mierze warunki samego systemu bezpiecznej przystani jako takiego niż sposób, w jaki komisarz go zastosował, i jednocześnie podkreślił, iż M. Schrems nie podważył bezpośrednio ważności dyrektywy 95/46 ani decyzji 2000/520.

43. Zdaniem High Court zasadniczą kwestią jest zatem to, czy z punktu widzenia prawa Unii i przy uwzględnieniu w szczególności późniejszego wejścia w życie art. 7 i 8 karty komisarz jest bezwzględnie związany ustaleniami Komisji wyrażonymi w decyzji 2000/520 dotyczącej odpowiedniego charakteru prawa i praktyki w dziedzinie ochrony danych osobowych w Stanach Zjednoczonych.

19 — High Court odniósł się w szczególności do poszanowania godności ludzkiej i do wolności jednostki (preambuła), do osobistej niezależności (art. 40 ust. 3 pkt 1 i 2), do nienaruszalności mieszkania (art. 40 ust. 5) i do ochrony życia rodzinnego (art. 41).

44. High Court wyjaśnił ponadto, że wniesiona do niego skarga nie zawiera żadnego zarzutu dotyczącego działań spółek Facebook Ireland i Facebook USA jako takich. Artykuł 3 ust. 1 lit. b) decyzji 2000/520, upoważniający właściwe organy krajowe do nakazania przedsiębiorstwu wstrzymania przepływu danych do państwa trzeciego, znajduje zdaniem tego sądu zastosowanie wyłącznie w okolicznościach, w których skarga skierowana jest przeciwko działaniom zainteresowanego przedsiębiorstwa, co nie ma miejsca w niniejszym przypadku.

45. High Court podkreślił zatem, że w rzeczywistości podważane jest nie tyle zachowanie spółki Facebook USA jako takie, ile raczej okoliczność, że Komisja uznała, iż prawo i praktyka w dziedzinie ochrony danych w Stanach Zjednoczonych gwarantują odpowiednią ochronę, podczas gdy informacje ujawnione przez E. Snowdena wskazują wyraźnie, że amerykańskie organy mogą uzyskać masowy i niezróżnicowany dostęp do danych osobowych osób zamieszkałych na terytorium Unii [20].

46. W tej kwestii High Court twierdzi, że trudno jest sobie wyobrazić, w jaki sposób decyzja 2000/520 mogłaby w praktyce spełnić wymogi art. 7 i 8 karty, zwłaszcza biorąc pod uwagę zasady sformułowane przez Trybunał w jego wyroku Digital Rights Ireland i in. [21]. W szczególności gwarancja przewidziana w art. 7 karty i wynikająca z głównych wartości wspólnych dla tradycji państw członkowskich zostałaby zagrożona, gdyby organy publiczne mogły uzyskać przypadkowy i powszechny dostęp do wiadomości elektronicznych bez konieczności przedstawienia obiektywnego uzasadnienia opartego na względach bezpieczeństwa narodowego lub zapobiegania przestępczości, związanych w szczególny sposób z zainteresowanymi jednostkami, i bez odpowiednich i wiarygodnych gwarancji. Skoro M. Schrems sugeruje w swojej skardze, że decyzja 2000/520 mogłaby in abstracto być niezgodna z art. 7 i 8 karty, Trybunał mógłby uznać, że dyrektywę 95/46, w szczególności jej art. 25 ust. 6, a także decyzję 2000/520 można zinterpretować w ten sposób, iż upoważniają one organy krajowe do przeprowadzenia własnych dochodzeń w celu ustalenia, czy przekazywanie danych osobowych do państwa trzeciego spełnia wymogi wynikające z art. 7 i 8 karty.

47. W tych okolicznościach High Court postanowił zawiesić postępowanie i zwrócić się do Trybunału z następującymi pytaniami prejudycjalnymi:

„Czy jeżeli w trakcie rozpatrywania skargi skierowanej do urzędnika dane osobowe przekazywane są do innego państwa trzeciego (w tym przypadku do Stanów Zjednoczonych Ameryki), którego obowiązujące przepisy i praktyka prawna nie gwarantują w ocenie skarżącego adekwatnej [odpowiedniego stopnia] ochrony osoby, której owe dane dotyczą, urzędnik ten jest – uwzględniając art. 7, 8 i 47 karty i niezależnie od [bez uszczerbku dla] przepisu art. 25 ust. 6 dyrektywy 95/46 – bezwzględnie związany odmiennymi ustaleniami Unii zawartymi w decyzji Komisji 2000/520?

Ewentualnie, czy urzędnik ten może, czy też musi zbadać tę sprawę indywidualnie w świetle nowych okoliczności faktycznych zaistniałych w międzyczasie, po dacie publikacji decyzji Komisji?”.

II – **Moja analiza**

48. Dwa pytania sformułowane przez High Court zmierzają do uzyskania od Trybunału wyjaśnień co do uprawnień, którymi dysponują krajowe organy nadzorcze przy rozpatrywaniu skargi dotyczącej przekazywania danych osobowych do przedsiębiorstwa z siedzibą w państwie trzecim, w przypadku gdy na poparcie tej skargi podnosi się, że owo państwo trzecie nie gwarantuje odpowiedniego stopnia ochrony przekazywanych danych, mimo iż Komisja na podstawie art. 25 ust. 6 dyrektywy 95/46 przyjęła decyzję uznającą, że wspomniane państwo trzecie zapewnia odpowiedni stopień ochrony.

20 — High Court wskazał w tym względzie, że główny zarzut podniesiony przed tym sądem przez M. Schremsa polegał na stwierdzeniu, iż biorąc pod uwagę informacje ujawnione niedawno przez E. Snowdena oraz okoliczność, że dane osobowe zostały udostępnione służbom wywiadowczym Stanów Zjednoczonych na szeroką skalę, komisarz nie mógł skutecznie uznać, iż w tym państwie trzecim zapewnia się odpowiedni stopień ochrony tych danych.

21 — Wyrok C-293/12 i C-594/12, EU:C:2014:238, pkt 65–69.

49. Pragnę zauważyć, że skarga wniesiona przez M. Schremsa do komisarza ma podwójny wymiar. Zmierza ona do podważenia przekazywania danych przez Facebook Ireland do spółki Facebook USA. Maximillian Schrems żąda zaprzestania tego przekazywania, ponieważ według niego Stany Zjednoczone nie zapewniają odpowiedniego stopnia ochrony danych osobowych przekazywanych w ramach systemu bezpiecznej przystani. Ściślej rzecz biorąc, zarzuca on temu państwu trzeciemu wprowadzenie programu PRISM upoważniającego NSA do uzyskania swobodnego dostępu do danych masowych przechowywanych na serwerach znajdujących się w Stanach Zjednoczonych. Skarga dotyczy zatem w szczególny sposób przekazywania danych osobowych przez Facebook Ireland do spółki Facebook USA, podważając jednocześnie w sposób bardziej ogólny stopień ochrony zapewniany tym danym w ramach systemu bezpiecznej przystani.

50. Komisarz uznał, że samo istnienie decyzji Komisji stwierdzającej, iż Stany Zjednoczone zapewniają w ramach systemu bezpiecznej przystani odpowiedni stopień ochrony, uniemożliwia mu rozpoznanie tej skargi.

51. Należy zatem przeanalizować łącznie te dwa pytania, zmierzające w istocie do ustalenia, czy art. 28 dyrektywy 95/46 w związku z art. 7 i 8 karty należy interpretować w ten sposób, że istnienie decyzji przyjętej przez Komisję na podstawie art. 25 ust. 6 tej dyrektywy uniemożliwia krajowym organom nadzorczym rozpatrzenie skargi zarzucającej państwu trzeciemu niezapewnienie odpowiedniego stopnia ochrony przekazywanym danym osobowym, a w razie potrzeby – zawieszenie przekazywania tych danych.

52. Artykuł 7 karty gwarantuje prawo do poszanowania życia prywatnego, zaś art. 8 karty wyraźnie przewiduje prawo do ochrony danych osobowych. Ustępy 2 i 3 tego drugiego przepisu przewidują, że dane te muszą być przetwarzane rzetelnie, w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą, że każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania oraz że przestrzeganie tych zasad podlega kontroli niezależnego organu.

A – *W przedmiocie uprawnień krajowych organów nadzorczych w przypadku decyzji Komisji dotyczącej odpowiedniego stopnia ochrony*

53. Jak wskazał M. Schrems w swoich uwagach, dla skargi w postępowaniu głównym centralną kwestią jest przekazywanie danych osobowych przez Facebook Ireland do spółki Facebook USA w świetle powszechnego dostępu NSA i innych amerykańskich agencji bezpieczeństwa do danych przechowywanych przez Facebook USA na podstawie uprawnień, jakie przyznaje im amerykańskie ustawodawstwo.

54. Rozpatrując skargę zmierzającą do podważenia twierdzenia, zgodnie z którym państwo trzecie zapewnia odpowiedni stopień ochrony przekazywanych danych, krajowy organ nadzorczy posiada zdaniem M. Schremsa uprawnienie do zawieszenia przekazywania danych przez przedsiębiorstwo wymienione w tej skardze, jeśli dysponuje dowodami popierającymi zasadność zarzutów zawartych w tej skardze.

55. Biorąc pod uwagę zobowiązanie komisarza do ochrony praw podstawowych M. Schremsa, ten ostatni utrzymuje, że komisarz ma obowiązek nie tylko rozpatrzenia skargi, ale także, w razie jej uwzględnienia, skorzystania z uprawnienia do zawieszenia przepływu danych pomiędzy spółką Facebook Ireland a spółką Facebook USA.

56. Tymczasem komisarz odrzucił skargę na podstawie przepisów ustawy o ochronie danych, które to przepisy wymieniają jego uprawnienia. Rozstrzygnięcie to zostało oparte na przekonaniu komisarza, że był on związany decyzją Komisji 2000/520.

57. Wynika z tego, że głównym problemem w niniejszej sprawie jest kwestia, czy zawarta w decyzji 2000/520 ocena Komisji dotycząca odpowiedniego stopnia ochrony jest bezwzględnie wiążąca dla krajowego organu ochrony danych i uniemożliwia rozpoznanie zarzutów zmierzających do podważenia tych ustaleń. Pytania prejudycjalne dotyczą więc zakresu uprawnień dochodzeniowych krajowych organów ochrony danych w przypadku przyjęcia przez Komisję decyzji w sprawie odpowiedniego stopnia ochrony.

58. Według Komisji należy uwzględnić związek pomiędzy jej uprawnieniami a uprawnieniami krajowych organów ochrony danych. Uprawnienia tych ostatnich nakierowane są na stosowanie ustawodawstwa w tej dziedzinie w indywidualnych przypadkach, podczas gdy ponowne ogólne zbadanie stosowania decyzji 2000/520, włącznie z każdą decyzją zawierającą jej zawieszenie lub uchylenie, należy do uprawnień Komisji.

59. Komisja podnosi, że M. Schrems nie zdołał przedstawić szczególnych argumentów wskazujących na to, iż narażony jest on na bezpośrednie ryzyko poniesienia poważnej szkody z powodu przekazywania danych pomiędzy spółkami Facebook Ireland i Facebook USA. Przeciwnie, wyrażone przez M. Schremsa obawy w kwestii programów nadzoru wprowadzonych w życie przez amerykańskie agencje bezpieczeństwa narodowego – ze względu na ich abstrakcyjny i ogólny charakter – pokrywają się z tymi, które skłoniły Komisję do podjęcia ponownego badania decyzji 2000/520.

60. Według Komisji krajowe organy nadzorcze wkraczałyby w przysługujące jej uprawnienia do renegocjacji warunków tej decyzji ze Stanami Zjednoczonymi lub, w razie potrzeby, zawieszenia jej, gdyby podejmowały działania na podstawie skarg wyrażających jedynie strukturalne i abstrakcyjne zastrzeżenia.

61. Nie podzielam opinii Komisji. Moim zdaniem istnienie decyzji przyjętej przez Komisję na podstawie art. 25 ust. 6 dyrektywy 95/46 nie niweczy ani nawet nie ogranicza uprawnień przysługujących krajowym organom nadzorczym na podstawie art. 28 tej dyrektywy. Wbrew temu, co twierdzi Komisja, krajowe organy nadzorcze rozpoznające skargę indywidualną mają moim zdaniem możliwość, na mocy ich uprawnień do rozpoznawania skarg i ich niezależności, wyrobienia sobie własnej opinii co do ogólnego poziomu ochrony zapewnianego przez państwo trzecie oraz wyciągnięcia z tego konsekwencji przy wydawaniu indywidualnej decyzji.

62. Z utrwalonego orzecznictwa Trybunału wynika, że dla potrzeb wykładni przepisów prawa Unii należy brać pod uwagę nie tylko ich brzmienie, ale także kontekst ich występowania i cel uregulowań, w skład których one wchodzą [22].

63. Z motywu 62 dyrektywy 95/46 wynika, że „[u]tworzenie w państwach członkowskich organów nadzorczych, wykonujących swoje funkcje w sposób całkowicie niezależny jest zasadniczym elementem ochrony osób fizycznych w zakresie przetwarzania danych osobowych".

64. Zgodnie z art. 28 ust. 1 akapit pierwszy tej dyrektywy „[k]ażde państwo członkowskie zapewni, że jeden lub więcej organów władzy publicznej będzie odpowiedzialnych za kontrolę stosowania na jego terytorium przepisów przyjętych przez państwa członkowskie na mocy niniejszej dyrektywy". Artykuł 28 ust. 1 akapit drugi omawianej dyrektywy stanowi, że „[o]rgany te postępują w sposób całkowicie niezależny przy wykonywaniu powierzonych im funkcji".

22 — Zobacz w szczególności wyrok Koushkaki, C-84/12, EU:C:2013:862, pkt 34 i przytoczone tam orzecznictwo.

65. Artykuł 28 ust. 3 dyrektywy 95/46 wymienia uprawnienia przysługujące każdemu organowi nadzorczemu, mianowicie uprawienia dochodzeniowe, skuteczne uprawnienia interwencyjne umożliwiające mu w szczególności nakładanie czasowego lub ostatecznego zakazu przetwarzania danych, a także prawo pozywania w przypadku naruszenia krajowych przepisów przyjętych zgodnie z tą dyrektywą lub powiadomienia organów sądowych o takim naruszeniu.

66. Co więcej, zgodnie z art. 28 ust. 4 akapit pierwszy dyrektywy 95/46 „[k]ażdy organ nadzorczy rozpatruje skargi zgłaszane [składane] przez dowolną osobę […] odnośnie do ochrony jej praw i wolności w zakresie przetwarzania danych osobowych". Artykuł 28 ust. 4 akapit drugi tej dyrektywy przewiduje, że „[k]ażdy organ nadzorczy w szczególności rozpatruje skargi dotyczące kontroli legalności przetwarzania danych, zgłaszane przez dowolną osobę, kiedy mają zastosowanie krajowe przepisy przyjęte zgodnie z art. 13 [rzeczonej] dyrektywy". Pragnę wyjaśnić, że ten ostatni przepis upoważnia państwa członkowskie do przyjęcia środków ustawodawczych w celu ograniczenia zakresu praw i obowiązków przewidzianych w dyrektywie 95/46, kiedy ograniczenie takie stanowi środek konieczny dla zapewnienia w szczególności bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego, a także dla prewencji, dochodzenia, wykrywania i ścigania przestępstw.

67. Jak już wskazał Trybunał, wymóg kontrolowania przez niezależny organ przestrzegania przepisów prawa Unii dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych wynika również z prawa pierwotnego Unii, a w szczególności z art. 8 ust. 3 karty i z art. 16 ust. 2 TFUE [23]. Przypomniał on także, że „[u]stanowienie w państwach członkowskich organów nadzorczych stanowi istotny element ochrony osób w związku z przetwarzaniem danych osobowych" [24].

68. Trybunał orzekł również, iż „wykładni art. 28 ust. 1 akapit drugi dyrektywy 95/46 należy dokonywać w ten sposób, że organy nadzorcze właściwe w zakresie [kontrolowania] przetwarzania danych osobowych powinny cechować się niezależnością pozwalającą im na wykonywanie ich zadań bez wpływu z zewnątrz. Ta niezależność wyklucza w szczególności jakiekolwiek nakazy i jakikolwiek inny wpływ z zewnątrz – bez względu na jego formę oraz na to, czy jest bezpośredni, czy pośredni – który mógłby zaważyć na decyzjach tych organów i podważyć w ten sposób wykonywanie przez nie ich zadań polegających na ustaleniu słusznej równowagi pomiędzy ochroną prawa do poszanowania życia prywatnego a swobodą przepływu danych osobowych" [25].

69. Trybunał wyjaśnił także, że „[z]agwarantowanie niezależności krajowych organów [nadzorczych] ma na celu zapewnienie skuteczności i pewności kontroli przestrzegania przepisów w zakresie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych" [26]. Ta gwarancja niezależności została przyjęta „celem wzmocnienia ochrony osób i instytucji, których dotyczą [te] decyzje [tych krajowych organów nadzorczych]" [27].

70. Jak to wynika między innymi z motywu 10 i z art. 1 dyrektywy 95/46, dyrektywa ta ma na celu zagwarantowanie w Unii „wyższego poziomu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych" [28]. Zdaniem Trybunału „[o]rgany [nadzorcze] przewidziane w art. 28 dyrektywy 95/46 są zatem strażnikami tych podstawowych praw i wolności" [29].

23 — Zobacz wyroki: Komisja/Austria, C-614/10, EU:C:2012:631, pkt 36; Komisja/Węgry, C-288/12, EU:C:2014:237, pkt 47.

24 — Zobacz w szczególności wyrok Komisja/Węgry, C-288/12, EU:C:2014:237, pkt 48 i przytoczone tam orzecznictwo. Zobacz także, podobnie, wyrok Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 68 i przytoczone tam orzecznictwo.

25 — Zobacz w szczególności wyrok Komisja/Węgry, C-288/12, EU:C:2014:237, pkt 51 i przytoczone tam orzecznictwo.

26 — Wyrok Komisja/Niemcy, C-518/07, EU:C:2010:125, pkt 25.

27 — Ibidem.

28 — Ibidem, pkt 22 i przytoczone tam orzecznictwo.

29 — Ibidem, pkt 23. Zobacz także, podobnie, wyroki: Komisja/Austria, C-614/10, EU:C:2012:631, pkt 52; Komisja/Węgry, C-288/12, EU:C:2014:237, pkt 53.

71. Biorąc pod uwagę istotną rolę krajowych organów nadzorczych w zakresie ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych, ich uprawnienia interwencyjne powinny pozostać nieograniczone, nawet jeśli Komisja przyjęła decyzję na podstawie art. 25 ust. 6 dyrektywy 95/46.

72. Pragnę zauważyć w tym względzie, że nic nie wskazuje na to, iż systemy przekazywania danych osobowych do państw trzecich wyłączone są z przedmiotowego zakresu stosowania art. 8 ust. 3 karty, który podnosi do najwyższego poziomu w hierarchii norm prawa Unii znaczenie kontroli sprawowanej przez niezależne organy w dziedzinie poszanowania zasad dotyczących ochrony danych osobowych.

73. Gdyby krajowe organy nadzorcze były bezwzględnie związane decyzjami przyjętymi przez Komisję, ograniczyłoby to w nieunikniony sposób ich pełną niezależność. Krajowe organy nadzorcze – zgodnie z ich rolą strażników praw podstawowych – powinny dysponować możliwością całkowicie niezależnego rozpoznania wniesionych do nich skarg w nadrzędnym interesie ochrony jednostek w zakresie przetwarzania danych osobowych.

74. Ponadto, jak słusznie podniosły na rozprawie rząd belgijski i Parlament Europejski, nie ma żadnego hierarchicznego związku pomiędzy rozdziałem IV dyrektywy 95/46, dotyczącym przekazywania danych osobowych do państw trzecich, a jej rozdziałem VI, który poświęcony jest w szczególności roli krajowych organów nadzorczych. Żaden element tego rozdziału VI nie wskazuje na to, że przepisy dotyczące krajowych organów nadzorczych są w jakikolwiek sposób podporządkowane odrębnym przepisom dotyczącym przekazywania danych, przewidzianym w rozdziale IV dyrektywy 95/46.

75. Przeciwnie, z art. 25 ust. 1 tej dyrektywy, zamieszczonego w jej rozdziale IV, wyraźnie wynika, że upoważnienie do przekazywania danych osobowych do państwa trzeciego zapewniającego odpowiedni stopień ochrony jest skuteczne jedynie z zastrzeżeniem poszanowania przepisów krajowych wydanych w zastosowaniu innych przepisów wspomnianej dyrektywy.

76. Pragnę przypomnieć w tym względzie, że na mocy tego przepisu państwa członkowskie zapewniają w swoim krajowym ustawodawstwie, iż przekazywanie do państwa trzeciego danych osobowych poddawanych przetwarzaniu lub przeznaczonych do przetwarzania po ich przekazaniu może nastąpić tylko wówczas, gdy, z zastrzeżeniem przestrzegania krajowych przepisów przyjętych na podstawie innych przepisów dyrektywy 95/46, dane państwo trzecie zapewnia odpowiedni stopień ochrony.

77. Zgodnie z art. 28 ust. 1 tej dyrektywy krajowe organy nadzorcze są odpowiedzialne za kontrolę stosowania na terytorium każdego państwa członkowskiego przepisów przyjętych przez państwa członkowskie na mocy tej dyrektywy.

78. Łączne odczytanie tych dwóch przepisów pozwala uznać, że reguła przewidziana w art. 25 ust. 1 dyrektywy 95/46, zgodnie z którą przekazywanie danych osobowych może nastąpić tylko wówczas, gdy państwo trzecie będące odbiorcą tych danych zapewnia im odpowiedni stopień ochrony, stanowi jedną z reguł, których stosowanie kontrolują krajowe organy nadzorcze.

79. Zgodnie z art. 8 ust. 3 karty uprawnienia krajowych organów nadzorczych do całkowicie niezależnego rozpatrywania skarg na podstawie art. 28 dyrektywy 95/46 należy interpretować szeroko. Uprawnienia te nie mogą zatem być ograniczone przez uprawnienia przyznane Komisji przez prawodawcę Unii na podstawie art. 25 ust. 6 tej dyrektywy w celu ustalenia odpowiedniego stopnia ochrony zapewnionego w państwie trzecim.

80. Krajowe organy nadzorcze – z uwagi na ich istotną rolę w zakresie ochrony danych osobowych – powinny być uprawnione do rozpatrywania skarg obejmujących elementy mogące podważyć stopień ochrony zapewniony przez państwo trzecie, także wówczas, gdy Komisja ustaliła w decyzji przyjętej na podstawie art. 25 ust. 6 dyrektywy 95/46, że dane państwo trzecie zapewnia odpowiedni stopień ochrony.

81. Jeśli krajowy organ nadzorczy po przeprowadzeniu badania uzna, że podważane przekazywanie danych narusza ochronę, z jakiej powinni korzystać obywatele Unii w zakresie przetwarzania dotyczących ich danych, może on zawiesić to sporne przekazywanie danych, i to bez względu na ogólną ocenę dokonaną przez Komisję w jej decyzji.

82. Bezsporne jest bowiem, zgodnie z art. 25 ust. 2 dyrektywy 95/46, że odpowiedni charakter stopnia ochrony zapewniany w państwie trzecim ocenia się na podstawie wszystkich okoliczności faktycznych i prawnych. Jeśli jedna z tych okoliczności ulega zmianie i wydaje się, że może podważyć odpowiedni charakter stopnia ochrony zapewnionego przez państwo trzecie, krajowy organ nadzorczy rozpatrujący skargę powinien mieć możliwość wyciągnięcia z tego konsekwencji w odniesieniu do spornego przekazywania danych.

83. Oczywiście, jak wskazała Irlandia, komisarz, podobnie jak inne organy państwa, jest związany decyzją 2000/520. Z art. 288 akapit czwarty TFUE wynika bowiem, że decyzja przyjęta przez instytucję Unii wiąże w całości. W konsekwencji decyzja 2000/520 jest wiążąca dla państw członkowskich, do których jest skierowana.

84. Pragnę wskazać w tym względzie, że sama decyzja 2000/520 przewiduje w art. 5, iż „[p]aństwa członkowskie podejmą wszelkie niezbędne środki w celu zapewnienia zgodności z [nią] najpóźniej do końca okresu 90 dni upływającego [w terminie 90 dni] od dnia jej notyfikowania państwom członkowskim”. Ponadto art. 6 tej decyzji potwierdza, że „skierowana jest [ona] do państw członkowskich”.

85. Niemniej jednak jestem zdania, że z punktu widzenia ww. przepisów dyrektywy 95/46 i karty wiążący charakter decyzji 2000/520 nie może wykluczyć rozpoznawania przez komisarza skarg podnoszących zarzut, że przekazywanie danych osobowych do Stanów Zjednoczonych w ramach tej decyzji nie oferuje wystarczających gwarancji ochrony wymaganych przez prawo Unii. Innymi słowy, taki wiążący charakter nie może spowodować, że każda skarga tego rodzaju zostanie bezwzględnie – a więc natychmiastowo i bez jakiegokolwiek badania jej zasadności – odrzucona.

86. Ponadto pragnę dodać, że z systematyki art. 25 dyrektywy 95/46 wynika, iż ustalenia dotyczące tego, czy państwo trzecie zapewnia odpowiedni stopień ochrony, mogą zostać dokonane albo przez państwa członkowskie, albo przez Komisję. Są to zatem kompetencje dzielone.

87. Z art. 25 ust. 6 tej dyrektywy wynika, że jeśli Komisja ustali, iż państwo trzecie zapewnia odpowiedni stopień ochrony w rozumieniu art. 25 ust. 2 tej dyrektywy, to państwa członkowskie powinny przyjąć środki niezbędne dla podporządkowania się decyzji Komisji.

88. Skoro taka decyzja wywiera skutek w postaci upoważnienia do przekazywania danych osobowych do państwa trzeciego, które zdaniem Komisji zapewnia odpowiedni stopień ochrony, państwa członkowskie powinny zatem co do zasady umożliwiać takie przekazywanie danych przez przedsiębiorstwa z siedzibą na ich terytorium.

89. Artykuł 25 dyrektywy 95/46 nie przyznaje jednak Komisji uprawnień wyłącznych w dziedzinie ustalania odpowiedniego stopnia ochrony przekazywanych danych osobowych. Systematyka tego przepisu świadczy o tym, że państwa członkowskie również grają rolę w tym zakresie. Decyzja Komisji odgrywa oczywiście ważną rolę w ujednolicaniu warunków prawidłowego przekazywania danych w ramach państw członkowskich. Tym niemniej owo ujednolicanie może trwać jedynie do chwili podważenia tych ustaleń.

90. Argument dotyczący konieczności ujednolicenia warunków przekazywania danych osobowych do państwa trzeciego ograniczony jest moim zdaniem poprzez sytuację taką jak rozpatrywana w postępowaniu głównym, w której Komisja nie tylko zostaje poinformowana o krytyce wobec jej ustaleń, ale także sama wysuwa taką krytykę i prowadzi negocjacje w celu poprawy sytuacji.

91. Ocena odpowiedniego stopnia ochrony zapewnionego przez państwo trzecie może również być przedmiotem współpracy pomiędzy państwami członkowskimi a Komisją. W art. 25 ust. 3 dyrektywy 95/46 przewidziano w tym względzie, że „[p]aństwa członkowskie i Komisja będą informować się wzajemnie o przypadkach, kiedy uznają, że państwo trzecie nie zapewnia odpowiedniego stopnia ochrony w znaczeniu ust. 2". Jak zauważa Parlament, oznacza to, że państwa członkowskie i Komisja mają grać równorzędną rolę przy identyfikowaniu przypadków, w których państwo trzecie nie zapewnia odpowiedniego stopnia ochrony.

92. Przedmiotem decyzji dotyczącej odpowiedniego stopnia ochrony jest upoważnienie do przekazywania danych osobowych do danego państwa trzeciego. Nie oznacza to wcale, że organy nadzorcze nie mogą już rozpatrywać skarg obywateli Unii zmierzających do uzyskania ochrony ich danych osobowych. Pragnę w tym względzie zauważyć, że art. 28 ust. 4 akapit pierwszy dyrektywy 95/46, zgodnie z którym „[k]ażdy organ nadzorczy rozpatruje skargi zgłaszane [składane] przez dowolną osobę […] odnośnie do ochrony jej praw i wolności w zakresie przetwarzania danych osobowych", nie przewiduje wyjątków od tej zasady w przypadku istnienia decyzji przyjętej przez Komisję w zastosowaniu art. 25 ust. 6 tej dyrektywy.

93. Jakkolwiek zatem decyzja przyjęta przez Komisję w zastosowaniu uprawnień wykonawczych przyznanych jej przez ten ostatni przepis wywiera skutek w postaci umożliwienia przekazywania danych osobowych do państwa trzeciego, to jednak decyzja taka nie może skutkować pozbawieniem państw członkowskich, a w szczególności ich krajowych organów nadzorczych, wszelkich uprawnień, ani nawet ich ograniczeniem, kiedy spotykają się one z zarzutem naruszenia praw podstawowych.

94. Krajowy organ nadzorczy powinien móc samodzielnie wykonywać uprawnienia przewidziane w art. 28 ust. 3 dyrektywy 95/46, w tym uprawnienie wprowadzenia zakazu, czasowego lub ostatecznego, przetwarzania danych osobowych. Jakkolwiek dokonane w tym przepisie wyliczenie uprawnień nie przewiduje wyraźnie uprawnień dotyczących przekazywania danych z państwa członkowskiego do państwa trzeciego, przekazywanie takie powinno moim zdaniem być uważane za stanowiące przetwarzanie danych [30]. Jak wynika z brzmienia tego przepisu, wyliczenie to nie jest ponadto wyczerpujące. W każdym razie organy nadzorcze, z uwagi na istotną rolę, jaką grają one w systemie wprowadzonym przez dyrektywę 95/46, powinny być uprawnione do zawieszenia przekazywania danych w przypadku ustalonego naruszenia lub ryzyka naruszenia praw podstawowych.

95. Pragnę dodać, że pozbawienie krajowych organów nadzorczych uprawnień dochodzeniowych w okolicznościach takich jak rozpatrywane w niniejszej sprawie byłoby sprzeczne nie tylko z zasadą niezależności, ale także z celem dyrektywy 95/46 wynikającym z jej art. 1 ust. 1.

96. Jak wskazał Trybunał, „[z] motywów 3, 8 i 10 dyrektywy 95/46 wynika, że zamiarem prawodawcy unijnego było ułatwienie swobodnego przepływu danych osobowych poprzez zbliżanie przepisów prawa państw członkowskich, przy poszanowaniu jednak praw podstawowych jednostki, w szczególności prawa do prywatności, i przy zapewnieniu jak najwyższego stopnia ochrony w Unii. Artykuł 1 tej dyrektywy przewiduje w ten sposób, że państwa członkowskie zobowiązują się chronić podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do prywatności w odniesieniu do przetwarzania danych osobowych" [31].

97. Przepisy dyrektywy 95/46 należy zatem interpretować zgodnie z jej celem, którym jest zagwarantowanie w Unii wysokiego poziomu ochrony podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do prywatności, w odniesieniu do przetwarzania danych osobowych.

30 — Zobacz opinia rzecznika generalnego P. Légera w sprawie Parlament/Rada i Komisja, C-317/04, EU:C:2005:710, pkt 92–95. Zobacz także wyrok Parlament/Rada i Komisja, C-317/04 i C-318/04, EU:C:2006:346, pkt 56.

31 — Zobacz w szczególności wyrok IPI, C-473/12, EU:C:2013:715, pkt 28 i przytoczone tam orzecznictwo.

98. Znaczenie tego celu i roli, jaką państwa członkowskie powinny odgrywać w jego osiąganiu, wskazuje na to, że kiedy szczególne okoliczności budzą poważne wątpliwości co do poszanowania praw podstawowych gwarantowanych przez kartę w przypadku przekazywania danych osobowych do państwa trzeciego, państwa członkowskie, a więc ich krajowe organy nadzorcze, nie mogą być w sposób bezwzględny związane przyjętą przez Komisję decyzją dotyczącą odpowiedniego stopnia ochrony.

99. Trybunał orzekł już, że „wykładnia przepisów dyrektywy 95/46 w zakresie, w jakim regulują one kwestię przetwarzania danych osobowych mogących naruszyć podstawowe wolności, a w szczególności prawo do prywatności, musi być bezwzględnie dokonywana z punktu widzenia praw podstawowych, które zgodnie z utrwalonym orzecznictwem stanowią część składową ogólnych zasad prawnych, których przestrzeganie zapewnia Trybunał i które zostały zawarte w karcie”[32].

100. Pragnę ponadto odnieść się do orzecznictwa, zgodnie z którym „na państwach członkowskich spoczywa nie tylko obowiązek wykładni swego prawa krajowego w zgodzie z prawem Unii, lecz również dbania o to, by nie opierać się na wykładni tekstu prawa wtórnego, która pozostawałaby w konflikcie z prawami podstawowymi, chronionymi przez porządek prawny Unii lub z innymi ogólnymi zasadami prawa Unii”[33].

101. Trybunał orzekł więc w wyroku N.S. i in.[34], że „stosowanie rozporządzenia [(WE)] nr 343/2003[35] w oparciu o niewzruszalne domniemanie, iż prawa podstawowe osoby ubiegającej się o azyl będą przestrzegane w państwie członkowskim, które zasadniczo jest właściwe do rozpatrzenia wniosku tej osoby, jest nie do pogodzenia z obowiązkiem państw członkowskich dotyczącym dokonywania wykładni i stosowania rozporządzenia nr 343/2003 w sposób zgodny z prawami podstawowymi”[36].

102. W tym względzie Trybunał przyznał, w kontekście statusu państw członkowskich jako bezpiecznych państw pochodzenia, jednych wobec drugich, w kwestiach prawnych i praktycznych związanych z prawem azylowym, że należy domniemywać, iż traktowanie osób ubiegających się o azyl w każdym państwie członkowskim jest zgodne z wymogami określonymi w karcie, w Konwencji dotyczącej statusu uchodźców, sporządzonej w Genewie dnia 28 lipca 1951 r.[37], a także w europejskiej Konwencji praw człowieka i podstawowych wolności, podpisanej w Rzymie dnia 4 listopada 1950 r.[38]. Tym niemniej Trybunał orzekł, iż „[n]ie można […] wykluczyć, że w praktyce wystąpią poważne trudności w funkcjonowaniu wspomnianego systemu w określonym państwie członkowskim i w związku z tym zaistnieje poważne niebezpieczeństwo, iż w razie transferu do tego państwa członkowskiego osoby ubiegające się o azyl będą traktowane w sposób, którego nie dałoby się pogodzić z ich prawami podstawowymi”[39].

32 — Zobacz w szczególności wyrok Google Spain i Google, C-131/12, EU:C:2014:317, pkt 68 i przytoczone tam orzecznictwo.

33 — Zobacz w szczególności wyrok N.S. i in., C-411/10 i C-493/10, EU:C:2011:865, pkt 77 i przytoczone tam orzecznictwo.

34 — Wyrok C-411/10 i C-493/10, EU:C:2011:865.

35 — **Rozporządzenie Rady z dnia 18 lutego 2003 r. ustanawiające kryteria i mechanizmy określania państwa członkowskiego właściwego dla rozpatrywania wniosku o azyl, wniesionego w jednym z państw członkowskich przez obywatela państwa trzeciego** (Dz.U. L 50, s. 1).

36 — Punkt 99 tego wyroku.

37 — *Recueil des traités des Nations unies*, t. 189, s. 150, nr 2545 (1954).

38 — Zobacz wyrok N.S. i in., C-411/10 i C-493/10, EU:C:2011:865, pkt 80.

39 — Ibidem, pkt 81.

103. W konsekwencji Trybunał orzekł, że „na państwach członkowskich, w tym na sądach krajowych, ciąży obowiązek niedokonania transferu osoby ubiegającej się o azyl do »odpowiedzialnego państwa członkowskiego« w rozumieniu rozporządzenia nr 343/2003, jeżeli nie mogą one pominąć faktu, iż systemowe nieprawidłowości w zakresie procedury azylowej i warunków przyjmowania osób ubiegających się o azyl w tym państwie członkowskim stanowią poważne i udowodnione powody, aby przypuszczać, że wnioskodawca zetknie się z rzeczywistym niebezpieczeństwem bycia poddanym nieludzkiemu lub poniżającemu traktowaniu w rozumieniu art. 4 karty” [40].

104. Wydaje się, że wnioski z wyroku N.S. i in. [41] można rozciągnąć na sytuację taką jak rozpatrywana w postępowaniu głównym. Wykładnię prawa wtórnego Unii, opierającą się na niewzruszalnym domniemaniu, że prawa podstawowe będą przestrzegane – przez państwo członkowskie, Komisję czy państwo trzecie – należy zatem uważać za niezgodną z obowiązkami państw członkowskich w zakresie wykładni i stosowania prawa wtórnego Unii w sposób zgodny z prawami podstawowymi. Artykuł 25 ust. 6 dyrektywy 95/46 nie narzuca więc takiego niewzruszalnego domniemania poszanowania praw podstawowych w odniesieniu do dokonanej przez Komisję oceny odpowiedniego stopnia ochrony zapewnionego przez państwo trzecie. Przeciwnie, leżące u podstaw tego przepisu domniemanie, że przekazywanie danych do państwa trzeciego odbywa się z poszanowaniem praw podstawowych, należy uważać za wzruszalne [42]. W konsekwencji omawianego przepisu nie należy interpretować w ten sposób, że podważa on gwarancje zawarte w szczególności w art. 28 ust. 3 dyrektywy 95/46 i art. 8 ust. 3 karty, zmierzające do ochrony i poszanowania prawa do ochrony danych osobowych.

105. Ze wspomnianego wyroku płynie zatem wniosek, że w przypadku systemowych nieprawidłowości stwierdzonych w państwie trzecim, do którego dane osobowe są przekazywane, państwa członkowskie powinny mieć możliwość podjęcia środków niezbędnych dla ochrony praw podstawowych gwarantowanych w art. 7 i 8 karty.

106. Co więcej, jak wskazał rząd włoski w swoich uwagach, przyjęcie przez Komisję decyzji dotyczącej odpowiedniego stopnia ochrony nie może skutkować obniżeniem poziomu ochrony obywateli Unii w zakresie przetwarzania danych, które ich dotyczą, kiedy dane te są przekazywane do państwa trzeciego, w porównaniu do poziomu ochrony, z jakiego osoby te korzystają, kiedy dane, które ich dotyczą, są przetwarzane w Unii. Krajowe organy nadzorcze powinny w konsekwencji mieć możliwość ingerowania i wykonywania swoich uprawnień w zakresie przekazywania danych do państw trzecich, będących przedmiotem decyzji dotyczącej odpowiedniego stopnia ochrony. W przeciwnym wypadku obywatele Unii korzystaliby ze słabszej ochrony niż wówczas, gdy ich dane są przetwarzane w Unii.

107. W ten sposób przyjęcie przez Komisję decyzji w zastosowaniu art. 25 ust. 6 dyrektywy 95/46 wywiera jedynie skutek w postaci zniesienia całkowitego zakazu przekazywania danych osobowych do państw trzecich zapewniających poziom ochrony porównywalny do poziomu zapewnionego w tej dyrektywie. Innymi słowy, nie chodzi o stworzenie szczególnego wyjątkowego systemu, który zapewnia obywatelom Unii słabszą ochronę niż system ogólny przewidziany w tej dyrektywie dla przetwarzania danych dokonywanego w Unii.

40 — Ibidem, pkt 94.

41 — Wyrok C-411/10 i C-493/10, EU:C:2011:865.

42 — Punkt 104 tego wyroku.

108. Rzeczywiście, Trybunał wskazał w pkt 63 wyroku Lindqvist [43], że „[r]ozdział IV dyrektywy 95/46, w którym zawarty jest art. 25, wprowadza szczególny system". Tym niemniej nie oznacza to moim zdaniem, że taki system może oferować słabszą ochronę. Przeciwnie, dla osiągnięcia celu ochrony danych, wyznaczonego w art. 1 ust. 1 dyrektywy 95/46, art. 25 tej dyrektywy nakłada na państwa członkowskie i Komisję szereg obowiązków [44] oraz wprowadza zasadę, zgodnie z którą kiedy państwo trzecie nie zapewnia odpowiedniego stopnia ochrony, przekazywanie danych osobowych do tego państwa powinno być zakazane [45].

109. W odniesieniu dokładniej do systemu bezpiecznej przystani Komisja dopuszcza ingerencję krajowych organów nadzorczych i zawieszenie przepływu danych jedynie w ramach wyznaczonych w art. 3 ust. 1 lit. b) decyzji 2000/520.

110. Zgodnie z motywem 8 tej decyzji „[d]la zachowania przejrzystości i w celu zagwarantowania właściwym władzom w państwach członkowskich możliwości zapewnienia ochrony osób fizycznych w zakresie przetwarzania ich danych osobowych, konieczne jest wyszczególnienie w niniejszej decyzji okoliczności wyjątkowych, w których zawieszenie określonych przekazów danych powinno [może] być usprawiedliwione, bez względu na to, czy stwierdzono ich właściwą ochronę".

111. W ramach niniejszej sprawy dyskutowane było bardziej szczegółowo stosowanie art. 3 ust. 1 lit. b) wspomnianej decyzji. Na mocy tego przepisu krajowe organy nadzorcze mogą zawiesić przepływ danych w przypadku, gdy „istnieje duże prawdopodobieństwo, że zasady są łamane; istnieje uzasadnione domniemanie, że mechanizm realizacji prawa, o którym mowa, nie podejmuje lub nie podejmie właściwych kroków w odpowiednim czasie w celu załatwienia spornej sprawy; dalszy przekaz tworzyłby bezpośrednie ryzyko wystąpienia poważnej szkody dla osób, których dane dotyczą; a właściwe władze [organy] państwa członkowskiego dołożyły należytych starań w tych okolicznościach w celu powiadomienia danej organizacji i umożliwienia udzielenia odpowiedzi".

112. Omawiany przepis wprowadza szereg warunków poddawanych różnej wykładni przez strony w niniejszym postępowaniu [46]. Bez wchodzenia w szczegóły tych wykładni, wynika z niego, że warunki te w ścisły sposób wyznaczają uprawnienia krajowych organów nadzorczych do zawieszenia przepływu danych.

113. Przeciwnie do twierdzeń Komisji, art. 3 ust. 1 lit. b) decyzji 2000/520 należy interpretować zgodnie z celem ochrony danych osobowych, do którego zmierza dyrektywa 95/46, jak również w świetle art. 8 karty. Nakaz wykładni zgodnej z prawami podstawowymi przemawia za szeroką wykładnią tego przepisu.

114. Wynika z tego, że warunki przewidziane w art. 3 ust. 1 lit. b) decyzji 2000/520 nie mogą moim zdaniem uniemożliwić krajowym organom nadzorczym wykonywania w sposób całkowicie niezależny uprawnień, jakie przysługują im na mocy art. 28 ust. 3 dyrektywy 95/46.

43 — Wyrok C-101/01, EU:C:2003:596.

44 — Punkt 65.

45 — Punkt 64.

46 — Zdaniem M. Schremsa pierwszy warunek, zgodnie z którym „istnieje duże prawdopodobieństwo, że zasady są łamane", nie jest spełniony. Nie zarzucono bowiem, że spółka Facebook USA, jako dokonująca samocertyfikacji instytucja, do której dane są przekazywane, sama naruszyła zasady bezpiecznej przystani ze względu na masowy i niezróżnicowany dostęp do przechowywanych przez nią danych uzyskiwany przez amerykańskie władze. Zasady bezpiecznej przystani są bowiem wyraźnie ograniczone amerykańskim prawem, zdefiniowanym w akapicie czwartym załącznika I do decyzji 2000/520, odsyłającym do ustawy, rozporządzeń rządu albo orzeczeń sądowych.

115. Jak bowiem wskazały w istocie na rozprawie rządy belgijski i austriacki, wyjście awaryjne, jakie stanowi art. 3 ust. 1 lit. b) decyzji 2000/520, jest tak wąskie, że trudno jest z niego skorzystać w praktyce. Wymagane jest spełnienie kumulatywnych kryteriów i poprzeczka została zawieszona zbyt wysoko. Tymczasem w świetle art. 8 ust. 3 karty margines swobody krajowych organów nadzorczych dotyczący uprawnień przyznanych im w art. 28 ust. 3 tej dyrektywy nie może być tak ograniczony, że nie mogą one ich w ogóle wykonywać.

116. W tym względzie Parlament słusznie zauważył, że prawodawca Unii podjął decyzję co do tego, jakie uprawnienia powinny przysługiwać krajowym organom nadzorczym. Uprawnienia wykonawcze przyznane przez prawodawcę Unii Komisji w art. 25 ust. 6 dyrektywy 95/46 nie naruszają zatem uprawnień przyznanych przez tego samego prawodawcę krajowym organom nadzorczym w art. 28 ust. 3 tej dyrektywy. Innymi słowy, Komisja nie posiada kompetencji do ograniczenia uprawnień krajowych organów nadzorczych.

117. W konsekwencji dla zapewnienia właściwej ochrony praw podstawowych osób fizycznych w zakresie przetwarzania danych osobowych krajowe organy nadzorcze powinny mieć możliwość prowadzenia dochodzenia w przypadku zarzucanych naruszeń tych praw. Jeśli w wyniku takiego dochodzenia organy te uznają, że w państwie trzecim objętym decyzją dotyczącą odpowiedniego stopnia ochrony występują istotne okoliczności wskazujące na naruszenie prawa obywateli Unii do ochrony danych osobowych, które ich dotyczą, powinny one móc zawiesić przepływ danych do odbiorców z siedzibą w tym państwie trzecim.

118. Innymi słowy, krajowe organy nadzorcze powinny mieć możliwość prowadzenia dochodzenia i w razie potrzeby zawieszenia przekazywania danych, niezależnie od restrykcyjnych warunków określonych w art. 3 ust. 1 lit. b) decyzji 2000/520.

119. Co więcej, krajowe organy nadzorcze, na mocy swego prawa pozywania w przypadku naruszenia krajowych przepisów przyjętych zgodnie z dyrektywą 95/46 lub prawa do powiadomienia organów sądowych o takim naruszeniu, przewidzianych w art. 28 ust. 3 tej dyrektywy, powinny mieć możliwość – gdy są one w posiadaniu informacji dotyczących okoliczności wskazujących, że państwo trzecie nie zapewnia odpowiedniego stopnia ochrony – wniesienia sprawy do sądu krajowego, który z kolei może orzec, w razie potrzeby, o zwróceniu się do Trybunału z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym w celu oceny ważności wydanej przez Komisję decyzji dotyczącej odpowiedniego stopnia ochrony.

120. Ze wszystkich tych elementów wynika, że art. 28 dyrektywy 95/46 w związku z art. 7 i 8 karty należy interpretować w ten sposób, iż istnienie decyzji przyjętej przez Komisję na podstawie art. 25 ust. 6 tej dyrektywy nie skutkuje uniemożliwieniem krajowemu organowi nadzorczemu rozpoznania skargi, w której zarzuca się, że państwo trzecie nie zapewnia odpowiedniego stopnia ochrony danych osobowych, a w razie potrzeby, zawieszenia przekazywania tych danych.

121. Jakkolwiek High Court w swoim postanowieniu odsyłającym podkreśla, że M. Schrems nie podważył formalnie w swojej skardze ważności ani dyrektywy 95/46, ani decyzji 2000/520, to jednak z tego postanowienia odsyłającego wynika, że główna krytyka sformułowana przez M. Schremsa zmierza do podważenia ustaleń, zgodnie z którymi Stany Zjednoczone zapewniają w ramach systemu bezpiecznej przystani odpowiedni stopień ochrony przekazywanych danych osobowych.

122. Z uwag komisarza wynika również, że skarga M. Schremsa zmierza do bezpośredniego podważenia decyzji 2000/520. Wnosząc tę skargę, M. Schrems zamierzał podważyć warunki i funkcjonowanie systemu bezpiecznej przystani jako takiego ze względu na to, że masowy nadzór nad danymi osobowymi przekazywanymi do Stanów Zjednoczonych wskazuje, iż nie istnieje wiarygodna ochrona tych danych w prawie i praktyce obowiązujących w tym państwie trzecim.

123. Co więcej, sąd odsyłający sam zauważył, że gwarancja zawarta w art. 7 karty i wynikająca z głównych wartości wspólnych tradycjom konstytucyjnym państw członkowskich zostałaby zniweczona, gdyby uznano, że organy państwowe mogą uzyskiwać dostęp do wiadomości elektronicznych w sposób przypadkowy i powszechny, bez konieczności wskazania obiektywnego uzasadnienia w oparciu o względy bezpieczeństwa narodowego lub zapobiegania przestępczości w odniesieniu do osoby lub osób zainteresowanych czy zastosowania odpowiednich i możliwych do zweryfikowania zabezpieczeń [47]. Sąd odsyłający wyraził zatem pośrednio wątpliwości co do ważności decyzji 2000/520.

124. Ocena okoliczności, czy Stany Zjednoczone w ramach systemu bezpiecznej przystani gwarantują odpowiedni stopień ochrony przekazywanych danych osobowych, prowadzi zatem siłą rzeczy do rozważań co do ważności tej decyzji.

125. W tym względzie należy wskazać, że w ramach wprowadzonego w art. 267 TFUE mechanizmu współpracy pomiędzy Trybunałem a sądami krajowymi Trybunał, nawet jeśli wpłynie do niego wniosek o wydanie orzeczenia w trybie prejudycjalnym dotyczący jedynie wykładni prawa Unii, może w określonych okolicznościach uznać za konieczne zbadanie ważności przepisów prawa wtórnego.

126. W związku z tym Trybunał kilkakrotnie stwierdzał z urzędu nieważność aktu, gdy wniesiono do niego jedynie o jego wykładnię [48]. Orzekł także, iż „jeśli okaże się, że prawdziwym przedmiotem pytania zadanego przez sąd krajowy jest badanie raczej ważności niż wykładni aktu [unijnego], do Trybunału należy udzielenie temu sądowi bezpośrednio odpowiedzi, bez zobowiązywania go do powodującego opóźnienia formalizmu niezgodnego z naturą mechanizmów wprowadzonych w art. [267 TFUE]” [49]. Co więcej, Trybunał orzekł już, że wątpliwości wyrażone przez sąd odsyłający co do zgodności aktu prawa wtórnego z zasadami dotyczącymi ochrony praw podstawowych należy rozumieć jako podważenie ważności tego aktu z punktu widzenia prawa Unii [50].

127. Pragnę również przypomnieć, że z orzecznictwa Trybunału wynika, iż akty instytucji, organów i agencji Unii objęte są domniemaniem ważności, wobec czego wywołują one skutki prawne aż do czasu ich cofnięcia, stwierdzenia nieważności w wyniku skargi o stwierdzenie nieważności albo uznania za nieważne w następstwie wniosku o wydanie orzeczenia w trybie prejudycjalnym lub wskutek podniesienia zarzutu niezgodności z prawem. Jedynie Trybunał jest właściwy do stwierdzenia, że akt Unii jest nieważny, a celem tej kompetencji jest zapewnienie pewności prawa poprzez jednolite stosowanie prawa Unii. Decyzja wiąże w całości i jest bezpośrednio stosowana we wszystkich państwach członkowskich tak długo, jak długo nie została stwierdzona jej nieważność, nie została ona zmieniona albo nie została uchylona przez Komisję [51].

128. Uważam zatem, że Trybunał powinien przeprowadzić ocenę ważności decyzji 2000/520 w celu udzielenia sądowi odsyłającemu pełnej odpowiedzi i rozwiania wyrażonych w trakcie niniejszego postępowania wątpliwości co do ważności tej decyzji.

129. Uwzględniając powyższe, należy także wyjaśnić, że badanie ważności decyzji 2000/520 należy ograniczyć do zarzutów stanowiących przedmiot debaty w ramach niniejszego postępowania. Nie wszystkie aspekty dotyczące funkcjonowania systemu bezpiecznej przystani były bowiem dyskutowane w tych ramach, a więc podjęcie wyczerpującego badania niedociągnięć tego systemu nie wydaje mi się w tym miejscu możliwe.

47 — Punkt 24 postanowienia odsyłającego.

48 — Zobacz w szczególności wyroki: Strehl, 62/76, EU:C:1977:18, pkt 10–17; Roquette Frères, 145/79, EU:C:1980:234, pkt 6; a także Schutzverband der Spirituosen-Industrie, C-457/05, EU:C:2007:576, pkt 32–39.

49 — Wyrok Schwarze, 16/65, EU:C:1965:117, s. 1094.

50 — Zobacz wyrok Hauer, 44/79, EU:C:1979:290, pkt 16.

51 — Zobacz w szczególności wyrok CIVAD, C-533/10, EU:C:2012:347, pkt 39–41 i przytoczone tam orzecznictwo.

130. Natomiast ustalenie, czy powszechny i nieukierunkowany dostęp amerykańskich służb wywiadowczych do przekazywanych danych może wpłynąć na zgodność z prawem decyzji 2000/520, było przedmiotem debaty przed Trybunałem w ramach niniejszego postępowania. Ważność tej decyzji może zatem zostać zbadana pod tym kątem.

B – *W przedmiocie ważności decyzji 2000/520*

1. W przedmiocie okoliczności, jakie należy uwzględnić przy dokonywaniu oceny ważności decyzji 2000/520

131. Należy przypomnieć orzecznictwo, zgodnie z którym „w ramach skargi o stwierdzenie nieważności zgodność aktu z prawem ocenia się na podstawie okoliczności faktycznych i prawnych istniejących w chwili przyjęcia tego aktu, zaś ocena dokonana przez Komisję może zostać podważona tylko, jeśli okaże się ona oczywiście błędna w świetle okoliczności znanych jej w chwili przyjęcia spornego aktu”[52].

132. W swoim wyroku Gaz de France – Berliner Investissement[53] Trybunał przypomniał zasadę, zgodnie z którą „ocena ważności danego aktu, której przeprowadzenie należy do Trybunału w ramach odesłania prejudycjalnego, powinna zazwyczaj opierać się na sytuacji istniejącej w chwili przyjęcia tego aktu”[54]. Trybunał najwyraźniej przyznał jednak, że „ważność danego aktu mogłaby być oceniana na podstawie nowych elementów, które pojawiły się po jego przyjęciu”[55].

133. Naszkicowana w ten sposób przez Trybunał sytuacja wyjściowa wydaje mi się mieć szczególne znaczenie w ramach niniejszej sprawy.

134. Decyzje przyjmowane przez Komisję na podstawie art. 25 ust. 6 dyrektywy 95/46 mają bowiem szczególne cechy. Ich celem jest ocena odpowiedniego charakteru stopnia ochrony danych osobowych zapewnionego przez państwo trzecie. Chodzi więc o ocenę, która siłą rzeczy zmienia się w zależności od kontekstu faktycznego i prawnego panującego w tym państwie trzecim.

135. Uwzględniając okoliczność, że decyzja dotycząca odpowiedniego stopnia ochrony stanowi szczególny typ decyzji, reguła, zgodnie z którą ocena ważności tej decyzji może zostać przeprowadzona wyłącznie na podstawie okoliczności istniejących w chwili jej przyjęcia, powinna zostać w niniejszej sprawie zmodyfikowana. W przeciwnym razie reguła taka prowadziłaby do tego, że wiele lat po przyjęciu decyzji dotyczącej odpowiedniego stopnia ochrony ocena ważności, jakiej Trybunał ma dokonać, nie mogłaby uwzględniać późniejszych wydarzeń, i to nawet wówczas, gdy odesłanie prejudycjalne mające na celu ocenę ważności nie jest ograniczone w czasie, a jego złożenie może być właśnie konsekwencją późniejszych okoliczności wykazujących niedociągnięcia spornego aktu.

136. W niniejszej sprawie utrzymywanie w mocy decyzji 2000/520 od około 15 lat świadczy o dorozumianym potwierdzeniu przez Komisję dokonanej przez nią w 2000 r. oceny. Kiedy w ramach odesłania prejudycjalnego Trybunał ma zbadać ważność oceny utrzymywanej w czasie przez Komisję, jest więc nie tylko możliwe, ale też właściwe, aby mógł on skonfrontować tę ocenę z nowymi okolicznościami, które zaszły po przyjęciu decyzji dotyczącej właściwego stopnia ochrony.

52 — Zobacz w szczególności wyrok BVGD/Komisja, T-104/07 i T-339/08, EU:T:2013:366, pkt 291, odnoszący się do wyroku IECC/Komisja, C-449/98 P, EU:C:2001:275, pkt 87.

53 — Wyrok C-247/08, EU:C:2009:600.

54 — Punkt 49 i przytoczone tam orzecznictwo.

55 — Punkt 50 i przytoczone tam orzecznictwo. Zobacz podobnie K. Lenaerts, I. Maselis, K. Gutman, *EU Procedural Law*, Oxford University Press, 2014, którzy stwierdzają, że „in certain cases, the validity of the particular Union measure can be assessed by reference to new factors arising after that measure was adopted, depending on the determination of the Court” (pkt 10.16, s. 471).

137. Z uwagi na szczególny charakter decyzji dotyczącej odpowiedniego stopnia ochrony decyzja ta powinna stanowić przedmiot systematycznej ponownej oceny przeprowadzanej przez Komisję. Jeśli w wyniku nowych wydarzeń, które wystąpiły w międzyczasie, Komisja nie zmienia swojej decyzji, potwierdza ona siłą rzeczy, choć w sposób dorozumiany, pierwotnie dokonaną ocenę. Powtarza ona zatem swoje ustalenia, zgodnie z którymi dane państwo trzecie zapewnia odpowiedni stopień ochrony przekazywanych danych osobowych. Do Trybunału należy zbadanie, czy ustalenia te są wiarygodne pomimo okoliczności, które wystąpiły później.

138. Dla zapewnienia skutecznej kontroli sądowej tego typu decyzji badanie jej ważności powinno więc moim zdaniem zostać przeprowadzone z uwzględnieniem aktualnego kontekstu faktycznego i prawnego.

2. W przedmiocie pojęcia odpowiedniego stopnia ochrony

139. Artykuł 25 dyrektywy 95/46 opiera się w całości na zasadzie, zgodnie z którą przekazywanie danych osobowych do państwa trzeciego może nastąpić tylko pod warunkiem, że to państwo trzecie gwarantuje odpowiedni stopień ochrony tych danych. Celem tego przepisu jest więc zapewnienie ochrony przewidzianej w tej dyrektywie w przypadku przekazywania danych osobowych do państwa trzeciego. Należy w tym względzie przypomnieć, że wskazana dyrektywa zapewnia wysoki poziom ochrony obywatelom Unii w odniesieniu do przetwarzania danych osobowych, które ich dotyczą.

140. Biorąc pod uwagę istotną rolę, jaką gra ochrona danych osobowych z punktu widzenia prawa podstawowego do poszanowania życia prywatnego, taki wysoki poziom ochrony należy zatem zagwarantować także w przypadku przekazywania danych osobowych do państwa trzeciego.

141. Z tego powodu jestem zdania, że Komisja może na podstawie art. 25 ust. 6 dyrektywy 95/46 stwierdzić, że państwo trzecie zapewnia odpowiedni stopień ochrony, tylko w sytuacji, gdy w wyniku oceny całego prawa i praktyki w danym państwie trzecim może ona ustalić, iż owo państwo trzecie zapewnia poziom ochrony zasadniczo równoważny poziomowi przewidzianemu przez tę dyrektywę, nawet jeśli sposoby tej ochrony mogą różnić się od sposobów ogólnie stosowanych w Unii.

142. Jakkolwiek angielski termin „adequate” może być rozumiany, z lingwistycznego punktu widzenia, jako określający poziom ochrony zaledwie satysfakcjonujący lub wystarczający, a więc może posiadać zakres semantyczny inny od francuskiego terminu „adéquat”, należy zauważyć, że jedynym kryterium, którym należy się kierować przy dokonywaniu wykładni tego terminu, jest cel osiągnięcia wysokiego poziomu ochrony praw podstawowych, jakiego wymaga dyrektywa 95/46.

143. Analiza poziomu ochrony zapewnionego w państwie trzecim powinna opierać się na dwóch podstawowych okolicznościach, mianowicie treści stosowanych reguł i środkach zapewnienia poszanowania tych reguł[56].

144. Moim zdaniem dla osiągnięcia poziomu ochrony zasadniczo równoważnego poziomowi obowiązującemu w Unii, systemowi bezpiecznej przystani, polegającemu w znacznej mierze na samocertyfikacji i samoocenie przedsiębiorstw dobrowolnie uczestniczących w tym systemie, powinny towarzyszyć odpowiednie gwarancje i wystarczający mechanizm kontroli. Przekazywanie danych osobowych do państw trzecich nie powinno zatem korzystać ze słabszej ochrony niż przetwarzanie danych dokonywane w Unii.

56 — Zobacz s. 5 dokumentu roboczego WP 12 Komisji, zatytułowanego „Przekazywanie danych osobowych do państw trzecich: stosowanie art. 25 i 26 dyrektywy dotyczącej ochrony danych”, przyjętego przez grupę ds. ochrony **osób fizycznych w zakresie przetwarzania danych osobowych w dniu** 24 lipca 1998 r.

145. W tym względzie pragnę na wstępie wskazać, że w Unii panuje przekonanie, iż mechanizm kontroli zewnętrznej w postaci niezależnego organu stanowi niezbędny element każdego systemu zmierzającego do zapewnienia poszanowania reguł dotyczących ochrony danych osobowych.

146. Co więcej, w celu zapewnienia skuteczności art. 25 ust. 1–3 dyrektywy 95/46 należy wziąć pod uwagę okoliczność, że odpowiedni charakter stopnia ochrony zapewnionego w państwie trzecim ma charakter ewolucyjny, a sytuacja może zmieniać się w czasie w zależności od szeregu czynników. Państwa członkowskie i Komisja powinny zatem nieustannie obserwować wszelkie zmiany okoliczności, które mogą uczynić niezbędnym dokonanie ponownej oceny odpowiedniego stopnia ochrony zapewnionego w państwie trzecim. Ocena odpowiedniego stopnia ochrony nie może być jedynie ograniczona do jednego momentu, a następnie utrzymywana w nieskończoność, niezależnie od wszelkiej zmiany okoliczności wskazującej na to, że w rzeczywistości zapewniany stopień ochrony nie jest już odpowiedni.

147. Obowiązek zapewnienia przez państwo trzecie odpowiedniego stopnia ochrony stanowi zatem obowiązek stały. Jakkolwiek ocena dokonywana jest w określonym momencie, to jednak utrzymanie w mocy decyzji dotyczącej odpowiedniego stopnia ochrony zakłada, że żadna występująca później okoliczność nie podważa pierwotnej oceny dokonanej przez Komisję.

148. Nie należy bowiem tracić z oczu okoliczności, że celem art. 25 dyrektywy 95/46 jest unikanie przekazywania danych osobowych do państw trzecich, które nie zapewniają odpowiedniego stopnia ochrony, z naruszeniem prawa podstawowego do ochrony danych osobowych gwarantowanego w art. 8 karty.

149. Należy podkreślić, że powierzone Komisji przez prawodawcę unijnego w art. 25 ust. 6 dyrektywy 95/46 uprawnienie do ustalenia, że państwo trzecie zapewnia odpowiedni stopień ochrony, jest wyraźnie uzależnione od wymogu, aby owo państwo trzecie zapewniało taki stopień ochrony w rozumieniu ust. 2 tego artykułu. Komisja powinna w konsekwencji dostosować swoją decyzję, jeśli nowe okoliczności mogą podważyć jej pierwotną ocenę.

3. Moja ocena

150. Pragnę przypomnieć, że na mocy art. 25 ust. 6 dyrektywy 95/46 „Komisja może stwierdzić, zgodnie z procedurą określoną w art. 31 ust. 2, że państwo trzecie zapewnia prawidłowy [odpowiedni] stopień ochrony w znaczeniu ust. 2 niniejszego artykułu, co wynika z jego prawa krajowego lub międzynarodowych zobowiązań, jakie państwo to przyjęło, szczególnie po zakończeniu negocjacji określonych w ust. 5, w zakresie ochrony życia prywatnego i podstawowych praw i wolności osób fizycznych”. Artykuł 25 ust. 6 tej dyrektywy w związku z jej art. 25 ust. 2 oznacza, że dla stwierdzenia, iż państwo trzecie zapewnia odpowiedni stopień ochrony, Komisja powinna dokonać oceny obowiązujących w państwie trzecim reguł prawnych, a także ich stosowania.

151. Jak wskazałem, utrzymanie przez Komisję jej decyzji 2000/520 pomimo wystąpienia nowych okoliczności faktycznych i prawnych należy uważać za zamiar potwierdzenia przez nią jej pierwotnej oceny.

152. Trybunał nie może wypowiadać się w ramach postępowania w trybie prejudycjalnym w przedmiocie oceny okoliczności faktycznych leżących u podstaw sporu, który skłonił sąd krajowy do wystąpienia z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym [57].

57 — Zobacz w szczególności wyrok Fallimento Traghetti del Mediterraneo, C-140/09, EU:C:2010:335, pkt 22 i przytoczone tam orzecznictwo.

153. Oprę się więc na okolicznościach faktycznych wskazanych przez sąd odsyłający w jego wniosku o wydanie orzeczenia w trybie prejudycjalnym, czyli okolicznościach, które na wstępie zostały w przeważającej mierze uznane za ustalone przez samą Komisję [58].

154. Okoliczności przedstawione przed Trybunałem dla podważenia przeprowadzonej przez Komisję oceny, zgodnie z którą system bezpiecznej przystani zapewnia odpowiedni stopień ochrony danych osobowych przekazywanych z Unii do Stanów Zjednoczonych, mogą zostać opisane w następujący sposób.

155. W swoim wniosku o wydanie orzeczenia w trybie prejudycjalnym sąd odsyłający opiera się na dwóch następujących ustaleniach faktycznych. Po pierwsze, do danych osobowych przekazywanych przez przedsiębiorstwa takie jak Facebook Ireland do ich spółki dominującej z siedzibą w Stanach Zjednoczonych mogą następnie uzyskać dostęp NSA i inne agencje federalne w trakcie prowadzonych przez nie masowych i nieukierunkowanych działań nadzorowania i przechwytywania. Wobec informacji ujawnionych przez E. Snowdena żaden inny realistyczny wniosek nie może bowiem obecnie zostać wyciągnięty z dostępnych dowodów [59]. Po drugie, obywatelom Unii nie przysługuje skuteczne prawo do bycia wysłuchanym w kwestii nadzorowania i przechwytywania danych, które ich dotyczą, przez NSA i inne amerykańskie agencje bezpieczeństwa [60].

156. Dokonane w ten sposób przez High Court ustalenia faktyczne znajdują więc potwierdzenie w ustaleniach dokonanych przez samą Komisję.

157. W swoim ww. komunikacie dotyczącym funkcjonowania zasad bezpiecznego transferu danych osobowych z punktu widzenia obywateli Unii i przedsiębiorstw z siedzibą w Unii Komisja podzieliła zatem pogląd, że w 2013 r. informacje dotyczące skali i zakresu amerykańskich programów nadzoru wzbudziły obawy dotyczące ciągłości ochrony danych osobowych przekazanych zgodnie z amerykańskim prawem w ramach systemu bezpiecznej przystani. Wskazała ona, że wydaje się, iż wszystkie przedsiębiorstwa, które biorą udział w programie PRISM i udzielają dostępu amerykańskim organom do danych przechowywanych i przetwarzanych w Stanach Zjednoczonych, dokonały poświadczenia zgodności w ramach systemu bezpiecznej przystani. W ten sposób system bezpiecznej przystani stał się jej zdaniem jednym z kanałów dostępu amerykańskich organów wywiadowczych do danych osobowych wstępnie przetworzonych w Unii [61].

158. Z tych okoliczności wynika, że prawo i praktyka Stanów Zjednoczonych pozwalają na gromadzenie na znaczną skalę danych osobowych obywateli Unii, które są przekazywane w ramach systemu bezpiecznej przystani, bez zapewnienia tym obywatelom skutecznej ochrony sądowej.

159. Te ustalenia faktyczne wykazują moim zdaniem, że decyzja 2000/520 nie przewiduje wystarczających gwarancji. Ze względu na ten brak gwarancji decyzja ta została wprowadzona w życie w sposób nieodpowiadający wymogom zawartym w karcie i w dyrektywie 95/46.

160. Tymczasem decyzja przyjęta przez Komisję na podstawie art. 25 ust. 6 dyrektywy 95/46 ma na celu stwierdzenie, że państwo trzecie „zapewnia" odpowiedni stopień ochrony. Czasownik „zapewnia" odmieniony w czasie teraźniejszym wskazuje, że decyzja taka, aby mogła zostać utrzymana w mocy, powinna dotyczyć państwa trzeciego, które utrzymuje po przyjęciu tej decyzji odpowiednie gwarancje ochrony.

58 — Zobacz komunikat Komisji wymieniony w przypisie 2 i k**omunikat Komisji do Parlamentu Europejskiego i Rady w sprawie funkcjonowania zasad bezpiecznego transferu danych osobowych z punktu widzenia obywateli UE i przedsiębiorstw z siedzibą w UE** [COM(2013) 847 final].

59 — Punkt 7 lit. c) postanowienia odsyłającego.

60 — Punkt 7 lit. b) postanowienia odsyłającego.

61 — Strona 19 tego komunikatu.

161. W rzeczywistości ujawnione informacje dotyczące działalności NSA, która wykorzystuje dane przekazywane w ramach systemu bezpiecznej przystani, uwidoczniły słabości podstawy prawnej, jaką stanowi decyzja 2000/520.

162. Niedociągnięcia ujawnione w trakcie niniejszego postępowania zawarte są dokładniej w akapicie czwartym załącznika I do tej decyzji.

163. Pragnę przypomnieć, że zgodnie z brzmieniem tego przepisu „[p]rzyjęcie zasad [bezpiecznej przystani] może być ograniczone: a) w zakresie niezbędnym do spełnienia wymagań bezpieczeństwa narodowego, interesu publicznego albo przestrzegania prawa; b) ustawą, rozporządzeniem rządu albo prawem precedensowym [orzeczeniem sądu], ustanawiającym sprzeczne obowiązki albo udzielającym wyraźnego upoważnienia, pod warunkiem że działając na mocy tego upoważnienia organizacja potrafi wykazać, że nieprzestrzeganie przez nią zasad jest ograniczone do zakresu koniecznego do zaspokojenia nadrzędnych uzasadnionych interesów wspieranych przez to upoważnienie".

164. Problem wynika w istocie z użytku, jaki amerykańskie organy robią z odstępstw przewidzianych w tym przepisie. Ze względu na ich zbyt ogólne sformułowanie, wprowadzenie tych odstępstw w życie przez te organy nie jest ograniczone do tego, co jest ściśle niezbędne.

165. Temu zbyt ogólnemu sformułowaniu towarzyszy okoliczność, że obywatele Unii nie dysponują odpowiednią drogą sądową przeciwko przetwarzaniu ich danych osobowych w celach innych niż te, dla których dane te zostały pierwotnie zgromadzone, a następnie przekazane do Stanów Zjednoczonych.

166. Przewidzianym w decyzji 2000/520 odstępstwom od stosowania zasad bezpiecznej przystani, w szczególności ze względów bezpieczeństwa narodowego, powinno było towarzyszyć wprowadzenie niezależnego mechanizmu kontroli umożliwiającego uniknięcie stwierdzonych naruszeń prawa do życia prywatnego.

167. W ten sposób ujawnione informacje dotyczące praktyk amerykańskich służb wywiadowczych w zakresie powszechnego nadzorowania danych przekazywanych w ramach bezpiecznej przystani uwidoczniły pewne niedociągnięcia decyzji 2000/520.

168. Zarzuty podnoszone w ramach niniejszej sprawy nie dotyczą naruszenia przez Facebook zasad bezpiecznej przystani. Jeśli certyfikowane przedsiębiorstwo, takie jak Facebook USA, umożliwia amerykańskim organom dostęp do danych przekazanych mu z państwa członkowskiego, można uznać, że robi to w celu przestrzegania amerykańskiego ustawodawstwa. Biorąc pod uwagę okoliczność, że taka sytuacja jest wyraźnie dopuszczona w decyzji 2000/520, ze względu na szerokie sformułowanie zawartych w niej odstępstw, w rzeczywistości w ramach niniejszej sprawy podniesiona zostaje kwestia zgodności takich odstępstw z prawem pierwotnym Unii.

169. Należy w tym względzie podkreślić, że z utrwalonego orzecznictwa Trybunału wynika, iż przestrzeganie praw człowieka stanowi przesłankę zgodności z prawem aktów unijnych oraz iż niedopuszczalne są w Unii środki, które są nie do pogodzenia z poszanowaniem tych praw [62].

170. Z orzecznictwa Trybunału wynika także, że przedstawianie do wiadomości osobom trzecim, publicznym lub prywatnym, zgromadzonych danych osobowych stanowi ingerencję w prawo do poszanowania życia prywatnego „bez względu na późniejsze wykorzystanie informacji w ten sposób podawanych do wiadomości" [63]. Ponadto w wyroku Digital Rights Ireland i in. [64] Trybunał potwierdził,

62 — Zobacz w szczególności wyrok Kadi i Al Barakaat International Foundation/Rada i Komisja, C-402/05 P i C-415/05 P, EU:C:2008:461, pkt 284 i przytoczone tam orzecznictwo.

63 — Wyrok Österreichischer Rundfunk i in., C-465/00, C-138/01 i C-139/01, EU:C:2003:294, pkt 74.

64 — Wyrok C-293/12 i C-594/12, EU:C:2014:238.

że okoliczność upoważnienia właściwych organów krajowych do uzyskania dostępu do takich danych stanowi dodatkową ingerencję w to prawo podstawowe [65]. Co więcej, wszelka forma przetwarzania danych osobowych objęta jest art. 8 karty i stanowi ingerencję w prawo do ochrony takich danych [66]. Dostęp, jaki uzyskują amerykańskie służby wywiadowcze do przekazywanych danych, stanowi zatem również ingerencję w prawo podstawowe do ochrony danych osobowych zagwarantowane w art. 8 karty, ponieważ dostęp taki stanowi przetwarzanie tych danych.

171. Jak Trybunał stwierdził w tym wyroku, ustalona w ten sposób ingerencja ma znaczny zakres i należy ją uważać za szczególnie poważną, biorąc pod uwagę znaczną liczbę zainteresowanych użytkowników i ilość przekazywanych danych. Okoliczności te, w połączeniu z tajnością dostępu uzyskiwanego przez organy amerykańskie do danych osobowych przekazywanych do przedsiębiorstw z siedzibą w Stanach Zjednoczonych, czynią tę ingerencję wyjątkowo poważną.

172. Dochodzi do tego okoliczność, że obywatele Unii, użytkownicy Facebooka, nie są informowani o tym, iż ich dane osobowe są powszechnie dostępne dla amerykańskich agencji bezpieczeństwa.

173. Należy również podkreślić okoliczność, że sąd odsyłający stwierdził, iż w Stanach Zjednoczonych obywatelom Unii nie przysługuje skuteczne prawo do bycia wysłuchanym w kwestii nadzorowania i przechwytywania danych, które ich dotyczą. Właściwy FISC prowadzi nadzór, ale postępowanie przed nim jest tajne i niekontradyktoryjne [67]. Jestem zdania, że stanowi to ingerencję w prawo obywateli Unii do skutecznej ochrony prawnej chronione przez art. 47 karty.

174. W ten sposób dochodzi do ingerencji w prawa podstawowe chronione w art. 7, 8 i 47 karty, na którą to ingerencję pozwalają odstępstwa od zasad bezpiecznej przystani zawarte w akapicie czwartym załącznika I do decyzji 2000/520.

175. Należy obecnie zbadać, czy ingerencja ta jest uzasadniona.

176. Zgodnie z art. 52 ust. 1 karty wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w karcie muszą zostać przewidziane ustawą i muszą szanować istotę tych praw i wolności. Z zastrzeżeniem zasady proporcjonalności, ograniczenia praw i wolności mogą zostać wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób.

177. Biorąc pod uwagę warunki postawione w ten sposób wobec dopuszczalności ograniczeń w wykonywaniu praw i wolności chronionych kartą, mam poważne wątpliwości co do tego, czy sporne w niniejszej sprawie ograniczenia mogą zostać uznane za zgodne z zasadniczą istotą art. 7 i 8 karty. Dostęp uzyskiwany przez amerykańskie służby wywiadowcze do przekazywanych danych wydaje się bowiem rozciągać na treść wiadomości elektronicznych, co naruszałoby zasadniczą istotę prawa podstawowego do poszanowania życia prywatnego i innych praw zawartych w art. 7 karty. Ponadto o ile szerokie sformułowanie ograniczeń przewidzianych w akapicie czwartym załącznika I do decyzji 2000/520 pozwala potencjalnie na odrzucenie stosowania ogółu zasad bezpiecznej przystani, o tyle można uznać, że ograniczenia te naruszają zasadniczą istotę prawa podstawowego do ochrony danych osobowych [68].

178. Jeśli chodzi o to, czy stwierdzona ingerencja odpowiada celowi interesu ogólnego, pragnę na wstępie przypomnieć, że zgodnie z akapitem czwartym lit. b) załącznika I do decyzji 2000/520 zobowiązanie się do przestrzegania zasad bezpiecznej przystani może być ograniczone „ustawą, rozporządzeniem rządu albo prawem precedensowym [orzeczeniem sądu], ustanawiającym sprzeczne

65 — Punkt 35.

66 — Punkt 36.

67 — Punkt 7 lit. b) postanowienia odsyłającego.

68 — Zobacz w tym względzie wyrok Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 39, 40.

obowiązki albo udzielającym wyraźnego upoważnienia, pod warunkiem że działając na mocy tego upoważnienia organizacja potrafi wykazać, że nieprzestrzeganie przez nią zasad jest ograniczone do zakresu koniecznego do zaspokojenia nadrzędnych uzasadnionych interesów wspieranych przez to upoważnienie".

179. Należy stwierdzić, że „uzasadnione interesy", o których mowa w tym przepisie, nie zostały doprecyzowane. Wynika z tego niepewność co do zakresu stosowania, potencjalnie wyjątkowo szerokiego, tego odstępstwa od stosowania zasad bezpiecznej przystani przez przystępujące przedsiębiorstwa.

180. Wyjaśnienia zawarte w tytule B załącznika IV do decyzji 2000/520, zatytułowanym „Wyraźne upoważnienia prawne", potwierdzają to wrażenie; w szczególności potwierdza je twierdzenie, zgodnie z którym „[n]ajwyraźniej w przypadkach, gdy prawo amerykańskie nakłada sprzeczny obowiązek na organizacje amerykańskie, czy to działające w ramach »bezpiecznej przystani« czy poza nią, muszą one przestrzegać tego prawa". Wskazano jednak ponadto, jeżeli chodzi o wyraźne upoważnienia, że „podczas gdy celem zasad »bezpiecznej przystani« jest zatarcie różnic między amerykańskimi a europejskimi systemami ochrony prywatności, ustawodawczym prerogatywom naszych wybranych ustawodawców należne jest poważanie".

181. Wynika z tego moim zdaniem, że owo odstępstwo jest sprzeczne z art. 7, 8 i art. 52 ust. 1 karty, ponieważ nie zmierza ono do realizacji celu interesu ogólnego zdefiniowanego w wystarczająco precyzyjny sposób.

182. W każdym razie łatwość i powszechność, z jaką sama decyzja 2000/520 w swoich załączniku I akapit czwarty lit. b) i załączniku IV tytuł B przewiduje, że można odstąpić od zasad bezpiecznej przystani w zastosowaniu prawa amerykańskiego, są nie do pogodzenia z warunkiem, zgodnie z którym odstępstwa od reguł dotyczących ochrony danych osobowych powinny być ograniczone do tego, co ściśle niezbędne. Jest wprawdzie mowa o warunku niezbędności, jednak poza tym, że wykazanie spełnienia tego warunku obciąża zainteresowane przedsiębiorstwo, nie widzę, w jaki sposób takie przedsiębiorstwo mogłoby się uchylić od obowiązku odstąpienia od zasad bezpiecznej przystani, który wynika z reguł prawa, jakie zobowiązane jest ono stosować.

183. Jestem zatem zdania, że należy stwierdzić nieważność decyzji 2000/520, ponieważ występowanie odstępstwa pozwalającego w tak powszechny i nieprecyzyjny sposób na niestosowanie zasad systemu bezpiecznej przystani samo w sobie uniemożliwia uznanie, że system ten zapewnia odpowiedni stopień ochrony danych osobowych, które są przekazywane z Unii do Stanów Zjednoczonych.

184. Obecnie, jeśli chodzi o pierwszą kategorię ograniczeń przewidzianych w akapicie czwartym lit. a) załącznika I do decyzji 2000/520 w zakresie niezbędnym do spełnienia wymagań bezpieczeństwa narodowego, interesu publicznego albo przestrzegania amerykańskiego prawa, tylko pierwszy z tych celów wydaje mi się wystarczająco precyzyjny, aby uważać go za uznany przez Unię cel interesu ogólnego w rozumieniu art. 52 ust. 1 karty.

185. Należy obecnie zbadać proporcjonalność stwierdzonej ingerencji.

186. 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 osiągnięcia" [69].

69 — Wyrok Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 46 i przytoczone tam orzecznictwo.

187. Co się tyczy sądowej kontroli przestrzegania tych wymogów „w przypadku, gdy dotyczy ona ingerencji w prawa podstawowe, zakres uprawnień dyskrecjonalnych prawodawcy Unii może okazać się ograniczony w zależności od kilku czynników, w tym między innymi obszaru, którego kontrola ta dotyczy, natury prawa gwarantowanego przez kartę, charakteru i wagi tej ingerencji oraz jej celu” [70].

188. Moim zdaniem decyzje, jakie Komisja przyjmuje na podstawie art. 25 ust. 6 dyrektywy 95/46, poddane są pełnej kontroli Trybunału w odniesieniu do proporcjonalności oceny dokonanej przez tę instytucję co do odpowiedniego stopnia ochrony zapewnionej w państwie trzecim, jaka wynika z „jego prawa krajowego lub międzynarodowych zobowiązań”.

189. Należy w tym względzie zauważyć, że w swoim wyroku Digital Rights Ireland i in. [71] Trybunał orzekł, iż „mając na uwadze, po pierwsze, znaczącą rolę, jaką odgrywa ochrona danych osobowych w świetle prawa podstawowego do poszanowania życia prywatnego oraz, po drugie, zakres i wagę ingerencji w to prawo, której źródłem jest [rozpatrywana] dyrektywa […], uprawnienia dyskrecjonalne prawodawcy Unii są ograniczone, skutkiem czego kontrola tych uprawnień musi mieć charakter ścisły” [72].

190. Taka ingerencja powinna być właściwa dla realizacji celu zamierzonego przez sporny akt Unii i niezbędna do osiągnięcia tego celu.

191. W tym względzie, „[c]o się tyczy prawa do poszanowania życia prywatnego, zgodnie z utrwalonym orzecznictwem [Trybunału] ochrona tego prawa podstawowego […] wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia ograniczały się do tego, co absolutnie [ściśle] konieczne” [73].

192. Przy sprawowaniu kontroli Trybunał bierze także pod uwagę, że „ochrona danych osobowych mająca swoje źródło w wyraźnie przewidzianym w art. 8 ust. 1 karty obowiązku jest szczególnie istotna z punktu widzenia prawa do poszanowania życia prywatnego ustanowionego w jej art. 7” [74].

193. Zdaniem Trybunału, który odnosi się w tym względzie do orzecznictwa Europejskiego Trybunału Praw Człowieka, „rozpatrywane uregulowania Unii muszą zawierać jasne i dokładne reguły dotyczące zakresu i sposobu stosowania rozpatrywanych środków, a także ustanawiać minimalne zabezpieczenia służące temu, aby osoby, których dane zostały zatrzymane, miały wystarczające gwarancje rzeczywistej ochrony ich danych osobowych przed ryzykiem nadużyć oraz ich bezprawnym udostępnianiem i wykorzystywaniem” [75]. Trybunał wskazał, iż „[k]onieczność zapewnienia takich gwarancji ma znaczenie tym większe, że […] dane osobowe przetwarzane są automatycznie, z czym wiąże się ryzyko bezprawnego uzyskania dostępu do nich” [76].

194. Moim zdaniem występuje analogia pomiędzy akapitem czwartym lit. a) załącznika I do decyzji 2000/520 a art. 13 ust. 1 dyrektywy 95/46. W pierwszym z tych przepisów wskazano, że przyjęcie zasad bezpiecznej przystani może zostać ograniczone przez „wymaga[nia] bezpieczeństwa narodowego, interesu publicznego albo przestrzegania [amerykańskiego] prawa”. W drugim przewidziano, że państwo członkowskie może przyjąć środki ustawodawcze w celu ograniczenia zakresu praw

70 — Ibidem, pkt 47 i przytoczone tam orzecznictwo.

71 — Wyrok C-293/12 i C-594/12, EU:C:2014:238.

72 — Punkt 48.

73 — Wyrok Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 52 i przytoczone tam orzecznictwo.

74 — Ibidem, pkt 53.

75 — Ibidem, pkt 54 i przytoczone tam orzecznictwo.

76 — Ibidem, pkt 55 i przytoczone tam orzecznictwo.

i obowiązków, przewidzianego w art. 6 ust. 1, art. 10, art. 11 ust. 1, art. 12 i 21 tej dyrektywy, kiedy ograniczenie takie stanowi środek konieczny dla zabezpieczenia w szczególności bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego, a także działań prewencyjnych, prowadzonych czynności dochodzeniowo-śledczych i prokuratorskich w sprawach karnych.

195. Jak Trybunał wskazał w swoim wyroku IPI [77], z brzmienia art. 13 ust. 1 dyrektywy 95/46 wynika, że państwa członkowskie mogą ustanowić przepisy przewidziane w tym przepisie wyłącznie wówczas, gdy są one konieczne. „Konieczny" charakter przepisów stanowi tym samym warunek uprawnień przyznanych państwom członkowskim na mocy tego przepisu [78]. W odniesieniu do przetwarzania danych osobowych w Unii ograniczenia przewidziane w art. 13 tej dyrektywy należy rozumieć jako ograniczone do tego, co jest ściśle niezbędne do osiągnięcia zamierzonego celu. Dotyczy to moim zdaniem także ograniczeń zasad bezpiecznej przystani przewidzianych w akapicie czwartym załącznika I do decyzji 2000/520.

196. Należy stwierdzić, że nie wszystkie wersje językowe wymieniają kryterium konieczności w brzmieniu akapitu pierwszego lit. a) załącznika I do decyzji 2000/520. Chodzi w szczególności o wersję w języku francuskim, która wskazuje, że „[l]'adhésion aux principes peut être limitée par […] les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis", podczas gdy przykładowo wersje w językach hiszpańskim, niemieckim i angielskim wskazują, że ograniczenia powinny być niezbędne dla osiągnięcia wyżej wymienionych celów.

197. W każdym razie okoliczności faktyczne przedstawione przez sąd odsyłający, a także przez Komisję w jej ww. komunikatach wskazują jasno, że w praktyce wprowadzenie w życie tych ograniczeń nie jest ograniczone do tego, co ściśle konieczne dla osiągnięcia wymienionych celów.

198. Pragnę w tym względzie zauważyć, że dostęp do przekazywanych danych osobowych, jaki uzyskują amerykańskie służby wywiadowcze, obejmuje generalnie wszystkie jednostki, środki łączności elektronicznej, a także wszystkie przekazywane dane, w tym treść wiadomości, przy czym nie przewidziano jakiegokolwiek zróżnicowania, ograniczenia lub wyjątku w zależności od zamierzonego celu interesu ogólnego [79].

199. Dostęp amerykańskich służb wywiadowczych do przekazywanych danych dotyczy bowiem w sposób zgeneralizowany wszystkich osób korzystających z usług łączności elektronicznej, nie jest przy tym wymagane, aby te zainteresowane osoby stwarzały zagrożenie dla bezpieczeństwa narodowego [80].

200. Takie powszechne i nieukierunkowane nadzorowanie jest nieproporcjonalne ze swojej natury i stanowi nieuzasadnioną ingerencję w prawa zagwarantowane w art. 7 i 8 karty.

201. Jak słusznie wskazał Parlament w swoich uwagach, skoro ani prawodawca Unii, ani państwa członkowskie nie mogą przyjąć przepisów ustawowych, które z naruszeniem karty przewidywałyby powszechne i nieukierunkowane nadzorowanie, wynika z tego siłą rzeczy, że a fortiori nie można w żadnym wypadku uznać, iż państwa trzecie zapewniają odpowiedni stopień ochrony danych osobowych obywateli Unii, jeśli ich uregulowania w rzeczywistości umożliwiają powszechne i nieukierunkowane nadzorowanie i przechwytywanie tego typu danych.

202. Należy ponadto podkreślić, że system bezpiecznej przystani taki jak zdefiniowany w decyzji 2000/520 nie zawiera gwarancji właściwych dla uniknięcia masowego i powszechnego dostępu do przekazywanych danych.

77 — Wyrok C-473/12, EU:C:2013:715.

78 — Punkt 32.

79 — Zobacz analogicznie wyrok Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 57 i przytoczone tam orzecznictwo.

80 — Ibidem, pkt 58, 59.

203. Pragnę w tym względzie zauważyć, że Trybunał podkreślił w swoim wyroku Digital Rights Ireland i in. [81] wagę przyjęcia „jasnych i precyzyjnych reguł określających zakres ingerencji w prawa podstawowe ustanowione w art. 7 i 8 karty” [82]. Zdaniem Trybunału „przepisy mają[…] zagwarantować to, że ingerencja ta nie będzie rzeczywiście wykraczać poza to, co ściśle niezbędne” [83]. Trybunał położył również w tym samym wyroku nacisk na konieczność ustanowienia „gwarancji takich jak te określone w art. 8 karty, pozwalających na zapewnienie skutecznej ochrony […] danych [osobowych] przed ryzykiem nadużyć oraz przed jakimkolwiek dostępem do nich i wykorzystywaniem w sposób niedozwolony” [84].

204. Należy stwierdzić, że mechanizmy prywatnego arbitrażu i FTC, ze względu na ich rolę ograniczoną do sporów handlowych, nie stanowią środka umożliwiającego zakwestionowanie dostępu amerykańskich służb wywiadowczych do danych osobowych przekazywanych z Unii.

205. Właściwość FTC obejmuje nieuczciwe bądź wprowadzające w błąd czyny i praktyki handlowe, a więc nie obejmuje gromadzenia i wykorzystania osobistych informacji do celów niehandlowych [85]. Ograniczony zakres właściwości FTC ogranicza prawo jednostek do ochrony ich danych osobowych. FTC zostało ustanowione nie dla zapewnienia, jak ma to miejsce w Unii w odniesieniu do krajowych organów nadzorczych, ochrony prawa jednostki do życia prywatnego, ale dla zagwarantowania handlu uczciwego i wiarygodnego dla konsumentów, co ogranicza w rzeczywistości jego kompetencje do ingerowania w sferę związaną z ochroną danych osobowych. FTC nie gra zatem roli porównywalnej do tej, jaką pełnią krajowe organy nadzorcze przewidziane w art. 28 dyrektywy 95/46.

206. Obywatele Unii, których dane zostały przekazane, mogą zwrócić się do instytucji wyspecjalizowanego arbitrażu ustanowionych w Stanach Zjednoczonych, takich jak TRUSTe i BBBOnline, w celu domagania się wyjaśnień co do tego, czy przedsiębiorstwo przetrzymujące ich dane osobowe narusza warunki systemu samocertyfikacji. Arbitraż prywatny zapewniony przez instytucje takie jak TRUSTe nie może rozpoznawać naruszeń prawa do ochrony danych osobowych, których to naruszeń dopuszczają się instytucje lub organy inne niż samocertyfikowane przedsiębiorstwa. Te instytucje arbitrażowe nie są właściwe do orzekania o zgodności z prawem działań amerykańskich agencji bezpieczeństwa.

207. Ani FTC, ani instytucje prywatnego arbitrażu nie są więc właściwe do kontrolowania możliwych naruszeń zasad ochrony danych osobowych popełnionych przez instytucje publiczne takie jak amerykańskie agencje bezpieczeństwa. Taka właściwość miałaby natomiast zasadnicze znaczenie dla pełnego zagwarantowania prawa do skutecznej ochrony tych danych. Komisja nie mogła zatem stwierdzić, przyjmując decyzję 2000/520 i utrzymując ją w mocy, że dla wszystkich danych osobowych przekazywanych do Stanów Zjednoczonych istniała odpowiednia ochrona prawa przyznanego w art. 8 ust. 3 karty, a więc że niezależny organ sprawuje skuteczną kontrolę nad przestrzeganiem wymogów ochrony i bezpieczeństwa tych danych.

208. W konsekwencji należy stwierdzić, że w ramach przewidzianego w decyzji 2000/520 systemu bezpiecznej przystani brak jest niezależnego organu, który mógłby kontrolować, czy wprowadzanie w życie odstępstw od zasad bezpiecznej przystani jest ograniczone do tego, co ściśle konieczne. Wykazałem, że taka kontrola przez niezależny organ stanowi z punktu widzenia prawa Unii niezbędny element poszanowania ochrony jednostek w odniesieniu do przetwarzania danych osobowych [86].

81 — Wyrok C-293/12 i C-594/12, EU:C:2014:238.

82 — Punkt 65.

83 — Ibidem.

84 — Ibidem, pkt 66.

85 — Zobacz w tym względzie załącznik II, NZP 11, do decyzji 2000/520, ppkt „Działanie Federalnej Komisji Handlu”, oraz załączniki III, V i VII do tej decyzji.

86 — Zobacz wyrok Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 68 i przytoczone tam orzecznictwo.

209. Należy w tym względzie podkreślić rolę, jaką w obowiązującym w Unii systemie ochrony danych osobowych grają krajowe organy nadzorcze w zakresie kontrolowania ograniczeń przewidzianych w art. 13 dyrektywy 95/46. Zgodnie z art. 28 ust. 4 akapit drugi tej dyrektywy „[k]ażdy organ nadzorczy w szczególności rozpatruje skargi dotyczące kontroli legalności przetwarzania danych, zgłaszane [składane] przez dowolną osobę, kiedy mają zastosowanie krajowe przepisy przyjęte zgodnie z art. 13 niniejszej dyrektywy". Analogicznie moim zdaniem wymienieniu ograniczeń stosowania zasad bezpiecznej przystani w akapicie czwartym załącznika I do decyzji 2000/520 powinno było towarzyszyć wprowadzenie mechanizmu kontroli zapewnionego przez niezależny organ wyspecjalizowany w dziedzinie ochrony danych osobowych.

210. Interwencja niezależnych organów nadzorczych znajduje się bowiem w centrum europejskiego systemu ochrony danych osobowych. Naturalnie zatem istnienie takich organów jest uważane z góry za jeden z niezbędnych warunków stwierdzenia odpowiedniego stopnia ochrony zapewnionego przez państwa trzecie. Chodzi o warunek umożliwiający niewprowadzenie zakazu przepływów danych z terytorium państw członkowskich na terytorium państw trzecich zgodnie z art. 25 dyrektywy 95/46 [87]. Jak wskazano w dokumencie z dyskusji przyjętym przez grupę roboczą ustanowioną w art. 29 tej dyrektywy, w Europie istnieje szeroki konsensus, zgodnie z którym „mechanizm »kontroli zewnętrznej« w postaci niezależnego organu stanowi niezbędny element każdego systemu zmierzającego do zapewnienia poszanowania reguł ochrony danych" [88].

211. Pragnę ponadto wskazać, że FISC nie zapewnia skutecznego środka prawnego obywatelom Unii, których dane osobowe są przekazywane do Stanów Zjednoczonych. Ochrona przed nadzorowaniem przez służby rządowe w ramach sekcji 702 ustawy z 1978 r. w sprawie nadzoru zagranicznego wywiadu ma bowiem zastosowanie wyłącznie do obywateli amerykańskich, a także do obcokrajowców mieszkających legalnie i na stałe w Stanach Zjednoczonych. Jak Komisja sama wskazała, kontrola amerykańskich programów gromadzenia informacji mogłaby ulec poprawie poprzez wzmocnienie roli FISC i wprowadzenie drogi prawnej dla jednostek. Mechanizmy te mogłyby ograniczyć dotyczące obywateli Unii przetwarzanie danych osobowych, które nie mają znaczenia dla ochrony bezpieczeństwa narodowego [89].

212. Co więcej, Komisja sama wskazała, że obywatele Unii nie mają żadnej możliwości uzyskania dostępu do danych, ich zmiany ani usunięcia. Nie istnieją również środki odwoławcze na drodze sądowej lub administracyjnej w związku z gromadzeniem i dalszym przetwarzaniem danych osobowych takich osób w ramach amerykańskich programów nadzoru [90].

213. Należy wreszcie wspomnieć, że amerykańskie przepisy dotyczące ochrony życia prywatnego mogą być stosowane w różny sposób wobec obywateli amerykańskich i obcokrajowców [91].

214. Z powyższych rozważań wynika, że decyzja 2000/520 nie zawiera jasnych i precyzyjnych reguł określających zakres ingerencji w prawa podstawowe ustanowione w art. 7 i 8 karty. W rezultacie należy stwierdzić, że decyzja ta i sposób, w jaki się ją stosuje, wyjątkowo szeroko i mocno ingerują w te prawa podstawowe, przy czym przepisy mające zagwarantować to, że ingerencja ta nie będzie rzeczywiście wykraczać poza to, co ściśle konieczne, nie regulują precyzyjnie tej kwestii.

87 — Zobacz Y. Poullet, L'autorité de contrôle: „vues" de Bruxelles, *Revue française d'administration publique*, nr 89, styczeń-marzec 1999 r., s. 69, w szczególności s. 71.

88 — Zobacz s. 7 dokumentu roboczego WP 12 Komisji, wymienionego w przypisie 56.

89 — Komunikat Komisji wymieniony w przypisie 2, s. 10, 11.

90 — Zobacz komunikat Komisji wymieniony w przypisie 58, pkt 7.2, s. 20.

91 — Zobacz w tej kwestii Ch. Kuner, Foreign Nationals and Data Protection Law: A Transatlantic Analysis, *Data Protection Anno 2014: How To Restore Trust?*, Intersentia, Cambridge 2014, s. 213, w szczególności s. 216 i nast.

215. Przyjmując decyzję 2000/520, a następnie utrzymując ją w mocy, Komisja przekroczyła zatem granice wyznaczone przez poszanowanie zasady proporcjonalności w odniesieniu do art. 7, 8 i art. 52 ust. 1 karty. Dochodzi do tego stwierdzenie nieuzasadnionej ingerencji w chronione przez art. 47 karty prawo obywateli Unii do skutecznego środka prawnego.

216. W konsekwencji należy stwierdzić nieważność tej decyzji, ponieważ ze względu na opisane powyżej naruszenia praw podstawowych nie można uznać, że wprowadzony przez nią system bezpiecznej przystani zapewnia odpowiedni stopień ochrony danych osobowych przekazywanych z Unii do Stanów Zjednoczonych w ramach tego systemu.

217. Wobec takiego stwierdzenia naruszeń praw podstawowych obywateli Unii moim zdaniem Komisja powinna była zawiesić stosowanie decyzji 2000/520.

218. Decyzja ta została przyjęta na czas nieokreślony. Tymczasem niniejsza sprawa pokazuje, że odpowiedni charakter stopnia ochrony zapewniany przez państwo trzecie może zmieniać się czasie w zależności od zmiany zarówno fizycznych, jak i prawnych okoliczności leżących u podstaw tej decyzji.

219. Pragnę zauważyć, że sama decyzja 2000/520 zawiera przepisy przewidujące możliwość dostosowania jej przez Komisję w zależności od okoliczności.

220. Jak więc wynika z motywu 9 tej decyzji, „[w] świetle doświadczenia oraz nowych rozwiązań dotyczących ochrony prywatności w okolicznościach, w których technika umożliwia coraz łatwiejsze przekazywanie i przetwarzanie danych osobowych, a także w świetle sprawozdań w sprawie wprowadzenia w życie sporządzonych przez zaangażowane władze wykonawcze, może zajść potrzeba dokonania przeglądu »bezpiecznej przystani« tworzonej przez zasady i NZP”.

221. Podobnie zgodnie z brzmieniem art. 3 ust. 4 omawianej decyzji, „[j]eżeli informacje zebrane zgodnie z ust. 1, 2 i 3 dostarczą dowodów, że jakikolwiek organ odpowiedzialny za zapewnienie przestrzegania zasad wdrożonych zgodnie z NZP w Stanach Zjednoczonych nie spełnia skutecznie swojej roli, Komisja informuje o tym Departament Handlu USA oraz, w razie potrzeby, przedstawia projekt środków […] w celu uchylenia albo zawieszenia niniejszej decyzji lub też ograniczenia jej zakresu”.

222. Ponadto zgodnie z art. 4 ust. 1 decyzji 2000/520 decyzja ta może „być dostosowywana w dowolnym czasie w świetle doświadczenia uzyskanego podczas wprowadzania jej w życie i/lub, jeżeli wymagania ustawodawstwa USA będą wyższe niż poziom bezpieczeństwa zapewniany przez zasady i NZP. W każdym przypadku, Komisja oceni wprowadzanie w życie niniejszej decyzji na podstawie dostępnych informacji trzy lata od jej notyfikowania państwom członkowskim i złoży sprawozdanie na temat wszelkich stosownych ustaleń komitetowi, ustanowionemu na podstawie art. 31 dyrektywy 95/46[…], łącznie z wszelkimi dowodami, które mogą wpływać na ocenę przepisów określonych w art. 1 niniejszej decyzji w odniesieniu do zapewniania przez nie właściwej ochrony w rozumieniu art. 25 dyrektywy 95/46[…]”. Zgodnie z art. 4 ust. 2 decyzji 2000/520 „Komisja, w miarę potrzeb, przedstawia projekt środków zgodnie z procedurą określoną w art. 31 dyrektywy 95/46[…]”.

223. Komisja stwierdziła w swoich uwagach, że istnieje „duże prawdopodobieństwo, iż przystąpienie do zasad bezpiecznej przystani zostało ograniczone w sposób, który nie odpowiada już ściśle określonym warunkom wyjątku przewidzianego w dziedzinie bezpieczeństwa narodowego” [92]. Zauważyła ona w tym względzie, że „[o]mawiane ujawnione informacje wykazują znaczny zakres niezróżnicowanego nadzoru na dużą skalę, niezgodny z kryterium konieczności przewidzianym w tym wyjątku, ani ogólniej

92 — Punkt 44.

z prawem do ochrony danych osobowych ustanowionym w art. 8 karty”[93]. Ponadto Komisja sama stwierdziła, że „[z]asięg tych programów nadzoru w połączeniu z nierównym traktowaniem obywateli U[nii] podaje w wątpliwość poziom ochrony zapewniony przez ustalenia w ramach programu »Bezpieczna przystań«”[94].

224. Co więcej, Komisja wyraźnie uznała na rozprawie, że w ramach decyzji 2000/520, w kształcie obecnie stosowanym, nie ma gwarancji, iż prawa obywateli Unii do ochrony danych, które ich dotyczą, będą zapewnione. Stwierdzenie to nie może jednak jej zdaniem pozbawić tej decyzji ważności. Jakkolwiek Komisja zgadza się ze stwierdzeniem, zgodnie z którym powinna ona podejmować działania w odpowiedzi na nowe okoliczności, to jednak uważa ona, że przyjęła właściwe i proporcjonalne środki, rozpoczynając negocjacje ze Stanami Zjednoczonymi w celu dokonania reformy systemu bezpiecznej przystani.

225. Nie podzielam tej opinii. W międzyczasie bowiem powinna istnieć możliwość zawieszenia – z inicjatywy krajowych organów nadzorczych lub w wyniku wniesionej do nich skarg – przekazywania danych osobowych do Stanów Zjednoczonych.

226. Poza tym jestem zdania, że wobec takich ustaleń Komisja powinna była zawiesić stosowanie decyzji 2000/520. Cel ochrony danych osobowych, do realizacji którego zmierzają dyrektywa 95/46 oraz art. 8 karty, nakłada bowiem obowiązki nie tylko na państwa członkowskie, ale także na instytucje Unii, jak wynika z art. 51 ust. 1 karty.

227. W swojej ocenie stopnia ochrony zapewnionego przez państwo trzecie Komisja powinna zbadać nie tylko ustawodawstwo wewnętrzne i zobowiązania międzynarodowe tego państwa trzeciego, ale także sposób, w jaki ochrona danych osobowych jest zapewniania w praktyce. Jeśli badanie praktyki wykaże nieprawidłowości, Komisja powinna zareagować i w razie potrzeby zawiesić lub dostosować bezzwłocznie swoją decyzję.

228. Jak wykazałem w moich rozważaniach powyżej, ciążący na państwach członkowskich obowiązek polega przede wszystkim na zapewnieniu, poprzez działanie ich krajowych organów nadzorczych, poszanowania zasad przewidzianych w dyrektywie 95/46.

229. Obowiązek ciążący na Komisji polega na zawieszeniu stosowania decyzji, którą przyjęła ona na podstawie art. 25 ust. 6 tej dyrektywy, w przypadku wykazanych niedociągnięć danego państwa trzeciego, w czasie gdy prowadzi ona negocjacje z tym państwem trzecim w celu zaradzenia tym niedociągnięciom.

230. Pragnę przypomnieć, że decyzja przyjęta przez Komisję na podstawie tego przepisu ma na celu stwierdzenie, iż państwo trzecie „zapewnia” odpowiedni stopień ochrony danych osobowych przekazywanych do tego państwa trzeciego. Czasownik „zapewnia” odmieniony w czasie teraźniejszym wskazuje, że aby utrzymanie takiej decyzji w mocy było możliwe, powinna ona dotyczyć państwa trzeciego, które po przyjęciu tej decyzji nadal gwarantuje taki odpowiedni stopień ochrony.

231. Zgodnie z motywem 57 dyrektywy 95/46 „należy zakazać przekazywania danych osobowych do państwa trzeciego, które nie zapewnia odpowiedniego stopnia ochrony”.

93 — Ibidem.

94 — Zobacz komunikat Komisji wymieniony w przypisie 2, s. 5.

232. Zgodnie z art. 25 ust. 4 tej dyrektywy, „[j]eżeli Komisja stwierdzi, na podstawie procedury przewidzianej w art. 31 ust. 2, że państwo trzecie nie zapewnia odpowiedniego stopnia ochrony w znaczeniu ust. 2 niniejszego artykułu, państwa członkowskie podejmą konieczne środki, aby nie dopuścić do przekazania jakichkolwiek danych tego samego rodzaju do wspomnianego państwa trzeciego". Ponadto art. 25 ust. 5 wspomnianej dyrektywy przewiduje, że „[w]e właściwym czasie Komisja przystąpi do negocjacji w celu zaradzenia sytuacji stwierdzonej na podstawie ust. 4".

233. Z tego ostatniego przepisu wynika, że w ramach systemu wprowadzonego przez art. 25 dyrektywy 95/46 negocjacje wszczęte z państwem trzecim mają na celu zaradzenie brakowi odpowiedniego stopnia ochrony stwierdzonemu zgodnie z procedurą przewidzianą w art. 31 ust. 2 tej dyrektywy. W rozważanym przypadku Komisja nie stwierdziła formalnie, zgodnie z tą procedurą, że system bezpiecznej przystani nie zapewnia już odpowiedniego stopnia ochrony. Pomimo to, jeśli Komisja zdecydowała o wszczęciu negocjacji ze Stanami Zjednoczonymi, to dlatego, że uprzednio uznała, iż poziom ochrony zapewniony przez to państwo trzecie nie był już odpowiedni.

234. Mimo że Komisja wiedziała o nieprawidłowościach w stosowaniu decyzji 2000/520, nie zawiesiła stosowania ani nie dostosowała tej decyzji, co prowadziło do dalszego naruszania praw podstawowych osób, których dane osobowe były i nadal są przekazywane w ramach systemu bezpiecznej przystani.

235. Trybunał orzekł już, choć rzeczywiście w innym kontekście, że Komisja zobowiązana jest dostosować regulację do nowych danych [95].

236. Taki brak działania ze strony Komisji, naruszający bezpośrednio prawa podstawowe chronione przez art. 7, 8 i 47 karty, stanowi moim zdaniem dodatkowe uzasadnienie stwierdzenia nieważności decyzji 2000/520 w ramach niniejszego odesłania prejudycjalnego [96].

III – **Wnioski**

237. Mając na względzie powyższe rozważania, proponuję, aby Trybunał udzielił następującej odpowiedzi na pytania prejudycjalne przedstawione przez High Court:

Artykuł 28 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych w związku z art. 7 i 8 Karty praw podstawowych Unii Europejskiej należy interpretować w ten sposób, że istnienie decyzji przyjętej przez Komisję Europejską na podstawie art. 25 ust. 6 dyrektywy 95/46 nie skutkuje uniemożliwieniem krajowemu organowi nadzorczemu rozpoznania skargi, w której zarzucono, że państwo trzecie nie zapewnia odpowiedniego stopnia ochrony przekazywanych danych osobowych, a w razie potrzeby – zawieszenia przekazywania tych danych.

Decyzja Komisji 2000/520/WE z dnia 26 lipca 2000 r., przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach „bezpiecznej przystani" oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA, jest nieważna.

95 — Zobacz podobnie wyrok Agrarproduktion Staebelow, C-504/04, EU:C:2006:30, pkt 40.

96 — Jakkolwiek Trybunał orzekł w wyroku T. Port, C-68/95, EU:C:1996:452, że „w traktacie nie przewidziano możliwości odesłania, poprzez które sąd krajowy zwracałby się do Trybunału o stwierdzenie w trybie prejudycjalnym bezczynności instytucji" (pkt 53), to jednak wydaje się, że zajął on wobec tej możliwości bardziej przychylne stanowisko w wyroku Ten Kate Holding Musselkanaal i in., C-511/03, EU:C:2005:625, pkt 29.