Sammlung der Rechtsprechung

SCHLUSSANTRÄGE DES GENERALANWALTS
YVES BOT
vom 23. September 2015 [1]

Rechtssache C-362/14

Maximillian Schrems
gegen
Data Protection Commissioner

(Vorabentscheidungsersuchen des High Court [Irland])

„Vorlage zur Vorabentscheidung — Personenbezogene Daten — Schutz natürlicher Personen bei der Verarbeitung dieser Daten — Charta der Grundrechte der Europäischen Union — Art. 7, 8 und 47 — Richtlinie 95/46/EG — Art. 25 — Entscheidung 2000/520/EG — Übermittlung personenbezogener Daten in die Vereinigten Staaten — Beurteilung der Angemessenheit des Schutzniveaus — Beschwerde einer natürlichen Person, deren Daten in ein Drittland übermittelt wurden — Nationale Kontrollstelle — Befugnisse“

I – **Einleitung**

1. Wie die Europäische Kommission in ihrer Mitteilung vom 27. November 2013 [2] festgestellt hat, stellt „[d]ie Übermittlung personenbezogener Daten … einen wichtigen und notwendigen Aspekt der transatlantischen Beziehungen dar. Sie ist integraler Bestandteil der transatlantischen Handelsbeziehungen, auch für neu entstehende digitale Geschäftsbereiche wie soziale Medien oder Cloud-Computing, für die große Datenmengen von der EU in die USA fließen.“ [3]

2. Die Handelsbeziehungen sind Gegenstand der Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA [4]. Diese Entscheidung liefert eine Rechtsgrundlage für die Übermittlung personenbezogener Daten von der Union an Unternehmen mit Sitz in den Vereinigten Staaten, die den Grundsätzen des sicheren Hafens beitreten.

3. Die genannte Entscheidung ist heute mit der Herausforderung konfrontiert, Datenübermittlungen zwischen der Union und den Vereinigten Staaten zu erlauben und zugleich ein hohes Schutzniveau dieser Daten zu gewährleisten, wie es das Unionsrecht verlangt.

1 — Originalsprache: Französisch.

2 — Mitteilung der Kommission an das Europäische Parlament und den Rat mit dem Titel „Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA“ (COM[2013] 846 final).

3 — S. 2.

4 — ABl. L 215, S. 7, berichtigt im ABl. 2001, L 115, S. 14.

4. Eine Reihe von Enthüllungen haben nämlich unlängst die Existenz groß angelegter amerikanischer Datensammlungsprogramme ans Licht gebracht. Diese Enthüllungen haben zu Bedenken wegen der Einhaltung der Normen des Unionsrechts bei Übermittlungen personenbezogener Daten an Unternehmen mit Sitz in den Vereinigten Staaten und wegen der Schwächen der Safe-Harbor-Regelung geführt.

5. Mit dem vorliegenden Vorabentscheidungsersuchen wird der Gerichtshof um Klarstellung ersucht, welche Haltung die nationalen Kontrollstellen und die Kommission einnehmen müssen, wenn sie mit Funktionsstörungen bei der Anwendung der Entscheidung 2000/520 konfrontiert sind.

6. Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr [5] sieht in ihrem Kapitel IV Vorschriften über die Übermittlung personenbezogener Daten in Drittländer vor.

7. Im Mittelpunkt dieses Kapitels steht der in Art. 25 Abs. 1 der Richtlinie aufgestellte Grundsatz, wonach die Übermittlung personenbezogener Daten, die Gegenstand einer Verarbeitung sind oder nach der Übermittlung verarbeitet werden sollen, in ein Drittland nur zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau für solche Daten gewährleistet.

8. Zum umgekehrten Fall führt der Unionsgesetzgeber im 57. Erwägungsgrund der Richtlinie aus, dass die Übermittlung personenbezogener Daten in ein Drittland, das kein angemessenes Schutzniveau bietet, zu untersagen ist.

9. Art. 25 Abs. 2 der Richtlinie 95/46 lautet: „Die Angemessenheit des Schutzniveaus, das ein Drittland bietet, wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen; insbesondere werden die Art der Daten, die Zweckbestimmung sowie die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen sowie die dort geltenden Standesregeln und Sicherheitsmaßnahmen berücksichtigt."

10. Gemäß Art. 25 Abs. 6 der Richtlinie kann die Kommission feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet. Sobald die Kommission eine Entscheidung in diesem Sinne erlässt, ist die Übermittlung personenbezogener Daten in das betreffende Drittland zulässig.

11. In Durchführung dieser Bestimmung erließ die Kommission die Entscheidung 2000/520. Nach deren Art. 1 Abs. 1 wird davon ausgegangen, dass die „Grundsätze des ‚sicheren Hafens' zum Datenschutz", die gemäß den in den „Häufig gestellten Fragen" [6] enthaltenen Leitlinien umgesetzt werden, ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die von der Union an in den Vereinigten Staaten niedergelassene Unternehmen übermittelt werden.

12. Die Entscheidung 2000/520 erlaubt daher die Übermittlung personenbezogener Daten aus den Mitgliedstaaten an Unternehmen mit Sitz in den Vereinigten Staaten, die sich zur Einhaltung der Grundsätze des sicheren Hafens verpflichtet haben.

5 — ABl. L 281, S. 31, in der durch die Verordnung (EG) Nr. 1882/2003 des Europäischen Parlaments und des Rates vom 29. September 2003 (ABl. L 284, S. 1) geänderten Fassung (im Folgenden: Richtlinie 95/46).

6 — Frequently asked questions, im Folgenden: FAQ.

13. Die Entscheidung 2000/520 führt in ihrem Anhang I eine Reihe von Grundsätzen auf, denen sich die Unternehmen freiwillig unterwerfen können und die mit Grenzen und einem speziellen Kontrollsystem einhergehen. Die Zahl der Unternehmen, die sich diesem „Verhaltenskodex“ unterworfen haben, lag im Jahr 2013 bei mehr als 3 200.

14. Die Safe-Harbor-Regelung beruht auf einer Lösung in Form einer Kombination aus Selbstzertifizierung und Selbstbewertung durch Privatunternehmen einerseits und Eingriffen der öffentlichen Gewalt andererseits.

15. Die Grundsätze des sicheren Hafens wurden „in Absprache mit der Industrie und der breiten Öffentlichkeit entwickelt, um den Handel zwischen der … Union und den Vereinigten Staaten zu erleichtern. Sie sind ausschließlich für den Gebrauch durch US-Organisationen bestimmt, die personenbezogene Daten aus der … Union erhalten, um sich für den ‚sicheren Hafen‘ und die daraus erwachsende Vermutung der ‚Angemessenheit‘ des Datenschutzes zu qualifizieren.“ [7]

16. Die Grundsätze des sicheren Hafens in Anhang I der Entscheidung 2000/520 sehen u. a. vor:

— eine Informationspflicht, wonach die Organisation „Privatpersonen darüber informieren [muss], zu welchem Zweck sie die Daten über sie erhebt und verwendet, wie sie die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, an welche Kategorien von Dritten die Daten weitergegeben werden und welche Mittel und Wege sie den Privatpersonen zur Verfügung stellt, um die Verwendung und Weitergabe der Daten einzuschränken. Diese Angaben sind den Betroffenen … zu machen, wenn sie erstmalig gebeten werden, der Organisation personenbezogene Daten zu liefern, oder so bald wie möglich danach, auf jeden Fall aber bevor die Organisation die Daten zu anderen Zwecken verwendet als denen, für die sie von der übermittelnden Organisation ursprünglich erhoben oder verarbeitet wurden, oder bevor sie die Daten erstmalig an einen Dritten weitergibt“ [8];

— eine Verpflichtung für Organisationen, Privatpersonen die Möglichkeit zu geben, zu wählen, ob ihre Daten an Dritte weitergegeben oder für einen Zweck verwendet werden sollen, der mit dem ursprünglichen oder dem nachträglich von der betreffenden Person genehmigten Erhebungszweck unvereinbar ist. Bei sensiblen Daten benötigen die Organisationen „die ausdrückliche Zustimmung (‚opt in‘) der betroffenen Personen, wenn die Daten an Dritte weitergegeben oder für einen anderen als den ursprünglichen Erhebungszweck oder den Zweck verwendet werden sollen, dem die betroffene Person nachträglich durch Ausübung des Wahlrechts zugestimmt hat“ [9];

— Vorschriften über die Weitergabe von Daten. So darf eine Organisation „Daten nur dann an Dritte weitergeben, wenn sie die Grundsätze der Informationspflicht und der Wahlmöglichkeit anwendet“ [10];

— in Bezug auf die Datensicherheit eine Verpflichtung für „Organisationen, die personenbezogene Daten erstellen, verwalten, verwenden oder verbreiten, … angemessene Sicherheitsvorkehrungen [zu] treffen, um sie vor Verlust, Missbrauch und unbefugtem Zugriff, Weitergabe, Änderung und Zerstörung zu schützen“ [11];

7 — Anhang I Abs. 2 der Entscheidung 2000/520.

8 — Vgl. Anhang I unter „Informationspflicht“.

9 — Vgl. Anhang I unter „Wahlmöglichkeit“.

10 — Vgl. Anhang I unter „Weitergabe“.

11 — Vgl. Anhang I unter „Sicherheit“.

— in Bezug auf die Datenintegrität eine Verpflichtung für Organisationen, „[i]n dem … notwendigen Umfang … durch angemessene Maßnahmen [zu] gewährleisten, dass die Daten für den vorgesehenen Zweck hinreichend zuverlässig, genau, vollständig und aktuell sind“ [12];

— Privatpersonen müssen grundsätzlich „Zugang zu den … Daten haben, die eine Organisation über sie besitzt, und sie müssen die Möglichkeit haben, diese zu korrigieren, zu ändern oder zu löschen, wenn sie falsch sind“ [13];

— eine Verpflichtung zur Schaffung von „Mechanismen …, die die Einhaltung der Grundsätze des sicheren Hafens gewährleisten, Rechtsbehelfe für Betroffene vorsehen, bei deren Daten die Grundsätze nicht eingehalten wurden, sowie Sanktionen für die Organisation, die die Grundsätze nicht befolgt“ [14].

17. Eine amerikanische Organisation, die den Grundsätzen des sicheren Hafens beitreten will, ist verpflichtet, in ihrer Datenschutzpolitik anzugeben, dass sie ihren Beitritt zu diesen Grundsätzen offenlegt und sie tatsächlich einhält, und sich selbst zu zertifizieren, indem sie gegenüber dem Handelsministerium der Vereinigten Staaten erklärt, dass sie im Einklang mit den genannten Grundsätzen handelt [15].

18. Organisationen können sich auf verschiedene Arten für das Konzept des sicheren Hafens qualifizieren. So können sie sich z. B. „einem vom Privatsektor entwickelten Datenschutzprogramm anschließ[en], das sich an diese Grundsätze hält, [oder sich] qualifizieren, wenn sie eigene Maßnahmen zum Schutz personenbezogener Daten entwickeln, sofern diese den Grundsätzen entsprechen. … Zudem können Organisationen, die Gesetzen, Regulierungs-, Verwaltungs- oder anderen Rechtsvorschriften (oder Regeln) unterliegen, die wirksam personenbezogene Daten schützen, ebenfalls in den Genuss der Vorteile des ‚sicheren Hafens‘ gelangen.“ [16]

19. Es gibt mehrere – aus einer Mischung von privater Schiedsgerichtsbarkeit und der Kontrolle durch die öffentliche Hand bestehende – Mechanismen, mit denen die Einhaltung der Grundsätze des sicheren Hafens überprüft werden kann. So kann die Kontrolle mittels eines Systems zur außergerichtlichen Regelung von Streitigkeiten durch einen unabhängigen Dritten sichergestellt werden. Darüber hinaus können sich die Unternehmen verpflichten, mit dem Gremium der Union in Datenschutzfragen zusammenzuarbeiten. Schließlich sind die Federal Trade Commission (FTC) auf der Grundlage der ihr nach Section 5 des Federal Trade Commission Act übertragenen Befugnisse und das Department of Transportation auf der Grundlage der ihm durch Title 49 Section 41712 des United States Code übertragenen Befugnisse für die Behandlung von Beschwerden zuständig.

20. Nach dem Wortlaut von Anhang I Abs. 4 der Entscheidung 2000/520 kann die Geltung der Grundsätze des sicheren Hafens u. a. insoweit begrenzt werden, „als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss“, sowie durch „Gesetzesrecht, staatliche Regulierungsvorschriften oder Fallrecht, die unvereinbare Verpflichtungen oder ausdrückliche Ermächtigungen schaffen, vorausgesetzt, die Organisation kann in Wahrnehmung dieser Ermächtigungen nachweisen, dass die Nichteinhaltung der Grundsätze sich auf das Ausmaß beschränkte, das die Einhaltung übergeordneter berechtigter Interessen aufgrund eben dieser Ermächtigung erforderte“ [17].

12 — Vgl. Anhang I unter „Datenintegrität“.

13 — Vgl. Anhang I unter „Auskunftsrecht“.

14 — Vgl. Anhang I unter „Durchsetzung“.

15 — Art. 1 Abs. 2 und 3 der Entscheidung 2000/520. Vgl. auch Anhang II, FAQ 6.

16 — Anhang I Abs. 3.

17 — Vgl. auch Anhang IV Teil B.

21. Darüber hinaus hängt die Möglichkeit der zuständigen Behörden der Mitgliedstaaten zur Aussetzung der Datenübermittlungen von mehreren, in Art. 3 Abs. 1 der Entscheidung 2000/520 aufgeführten Voraussetzungen ab.

22. Das vorliegende Vorabentscheidungsersuchen gibt Anlass, sich mit der Tragweite der Entscheidung 2000/520 im Hinblick auf die Art. 7, 8 und 47 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) sowie die Art. 25 Abs. 6 und 28 der Richtlinie 95/46 zu befassen. Dieses Ersuchen ergeht im Rahmen eines Rechtsstreits zwischen Herrn Schrems und dem Data Protection Commissioner (im Folgenden: Commissioner) wegen dessen Weigerung, eine von Herrn Schrems eingelegte Beschwerde zu prüfen, die sich dagegen richtet, dass die Facebook Ireland Ltd (im Folgenden: Facebook Ireland) personenbezogene Daten ihrer Nutzer in die Vereinigten Staaten übermittelt und auf dort befindlichen Servern speichert.

23. Herr Schrems ist ein österreichischer Staatsangehöriger mit Wohnsitz in Österreich. Seit 2008 nutzt er das soziale Netzwerk Facebook.

24. Von allen Facebook-Nutzern mit Wohnsitz im Hoheitsgebiet der Union wird verlangt, dass sie einen Vertrag mit Facebook Ireland unterzeichnen, bei der es sich um eine Tochtergesellschaft der Facebook Inc. mit Sitz in den Vereinigten Staaten (im Folgenden: Facebook USA) handelt. Die Daten der Nutzer von Facebook Ireland mit Wohnsitz im Hoheitsgebiet der Union werden ganz oder teilweise auf Server von Facebook USA übertragen, die sich im Hoheitsgebiet der Vereinigten Staaten befinden, und dort gespeichert.

25. Herr Schrems legte am 25. Juni 2013 eine Beschwerde beim Commissioner ein und machte im Wesentlichen geltend, das Recht und die Praxis der Vereinigten Staaten böten keinen wirklichen Schutz der im Hoheitsgebiet der Vereinigten Staaten gespeicherten Daten vor staatlicher Überwachung. Dies ergebe sich aus Enthüllungen von Herrn Snowden ab Mai 2013 betreffend die Tätigkeiten der amerikanischen Nachrichtendienste und insbesondere der National Security Agency (NSA).

26. Aus diesen Enthüllungen ergibt sich u. a., dass die NSA ein als „PRISM“ bezeichnetes Programm aufgelegt haben soll, in dessen Rahmen sie freien Zugang zu großen Datenmengen auf Servern in den Vereinigten Staaten erlangt habe, die sich im Besitz oder unter der Kontrolle einer Reihe im Internet- und Technologiesektor tätiger Gesellschaften wie Facebook USA befänden.

27. Der Commissioner war der Ansicht, nicht zur Prüfung der Beschwerde verpflichtet zu sein, weil diese einer rechtlichen Grundlage entbehre. Es lägen keine Beweise dafür vor, dass die NSA auf die Daten von Herrn Schrems zugegriffen habe. Darüber hinaus sei die Beschwerde aufgrund der Entscheidung 2000/520 zurückzuweisen, mit der die Kommission festgestellt habe, dass die Vereinigten Staaten im Rahmen der Safe-Harbor-Regelung ein angemessenes Schutzniveau der übermittelten personenbezogenen Daten gewährleisteten. Jede Frage, die sich auf die Angemessenheit des Schutzes dieser Daten in den Vereinigten Staaten beziehe, sei im Einklang mit dieser Entscheidung zu klären, was ihn daran hindere, das mit der Beschwerde aufgeworfene Problem zu untersuchen.

28. Die nationalen Rechtsvorschriften, die den Commissioner bewogen, die Beschwerde zurückzuweisen, sehen Folgendes vor.

29. Section 10(1) des Data Protection Act 1988 in der durch den Data Protection (Amendment) Act 2003 geänderten Fassung (im Folgenden: Data Protection Act) verleiht ihm die Befugnis zur Prüfung von Beschwerden; sie lautet:

„a) Der Commissioner kann prüfen oder prüfen lassen, ob Bestimmungen dieses Gesetzes in Bezug auf einen Einzelnen verletzt wurden, verletzt werden oder verletzt zu werden drohen, weil dieser sich bei ihm über einen Verstoß gegen eine dieser Bestimmungen beschwert oder weil er anderweitig der Ansicht ist, dass ein solcher Verstoß vorliegen könnte.

b) Wird der Commissioner mit einer Beschwerde nach Buchst. a dieser Subsection befasst, wird er

(i) die Beschwerde untersuchen oder untersuchen lassen, es sei denn, er kommt zu dem Schluss, dass sie böswillig oder missbräuchlich ist, und,

(ii) falls es ihm oder ihr nicht gelingt, innerhalb einer angemessenen Frist eine gütliche Einigung der betreffenden Parteien über den Gegenstand der Beschwerde herbeizuführen, dem Beschwerdeführer seine oder ihre Entscheidung über die Beschwerde schriftlich mit dem Hinweis übermitteln, dass der Beschwerdeführer, sofern die Entscheidung ihn beschwert, gemäß Section 26 dieses Gesetzes innerhalb von 21 Tagen nach Erhalt der Mitteilung Klage gegen sie erheben kann.“

30. Im vorliegenden Fall kam der Commissioner zu dem Schluss, dass die Beschwerde von Herrn Schrems in dem Sinne „böswillig oder missbräuchlich“ sei, dass sie rechtlich unhaltbar und damit zum Scheitern verurteilt sei. Deshalb lehnte er es ab, die Beschwerde zu untersuchen.

31. Section 11 des Data Protection Act regelt die Übermittlung personenbezogener Daten ins Ausland. Section 11(2)(a) sieht vor:

„Wird in unter dieses Gesetz fallenden Verfahren die Frage aufgeworfen,

(i) ob ein Land oder Gebiet außerhalb des Europäischen Wirtschaftsraums [(EWR)], in das personenbezogene Daten übermittelt werden sollen, das in Subsection (1) dieser Section beschriebene angemessene Schutzniveau gewährleistet, und

(ii) hat die Gemeinschaft eine Feststellung zu derartigen Übermittlungen getroffen,

wird die Frage im Einklang mit dieser Feststellung geklärt.“

32. In Section 11(2)(b) des Data Protection Act wird der Begriff „Feststellung der Gemeinschaft“ wie folgt definiert:

„Im Sinne von Buchst. a dieser Subsection bedeutet ‚Feststellung der Gemeinschaft‘ eine Feststellung, die die … Kommission für die Zwecke von Art. 25 Abs. 4 oder 6 der [Richtlinie 95/46] im Rahmen des in Art. 31 Abs. 2 der Richtlinie vorgesehenen Verfahrens dazu getroffen hat, ob das in Subsection (1) dieser Section beschriebene angemessene Schutzniveau von einem Land oder Gebiet außerhalb des [EWR] gewährleistet wird.“

33. Der Commissioner wies darauf hin, dass die Entscheidung 2000/520 für die Zwecke von Section 11(2)(a) des Data Protection Act eine „Feststellung der Gemeinschaft“ sei, so dass nach diesem Gesetz jede die Angemessenheit des Datenschutzes in dem Drittland, in das Daten übermittelt würden, betreffende Frage im Einklang mit dieser Feststellung geklärt werden müsse. Da es sich dabei um den

Kern der Beschwerde von Herrn Schrems handelte – dass nämlich personenbezogene Daten in ein Drittland übermittelt würden, das in der Praxis kein angemessenes Schutzniveau gewährleiste –, war der Commissioner der Ansicht, das Wesen und die bloße Existenz der Entscheidung 2000/520 hinderten ihn daran, diese Frage zu untersuchen.

34. Herr Schrems erhob gegen die Entscheidung des Commissioner, seine Beschwerde zurückzuweisen, Klage vor dem High Court. Nach Prüfung der im Ausgangsverfahren vorgelegten Beweise stellte der High Court fest, dass die elektronische Überwachung und Erfassung personenbezogener Daten zur Erreichung notwendiger und unerlässlicher Ziele im öffentlichen Interesse diene, nämlich der Aufrechterhaltung der nationalen Sicherheit und der Verhütung schwerer Kriminalität. Mit der Überwachung und Erfassung der von der Union in die Vereinigten Staaten übermittelten personenbezogenen Daten würden legitime Ziele im Kampf gegen den Terrorismus verfolgt.

35. Die Enthüllungen von Herrn Snowden zeigten jedoch, dass die NSA und weitere ähnliche Behörden erhebliche Exzesse begangen hätten. Zwar gebe es eine gerichtliche Aufsicht durch den im Rahmen des Foreign Intelligence Surveillance Act of 1978 tätigen Foreign Intelligence Surveillance Court (FISC) [18], doch finde das Verfahren vor ihm unter Geheimhaltung und *ex parte* statt. Abgesehen davon, dass Entscheidungen über den Zugang zu personenbezogenen Daten auf der Grundlage des Rechts der Vereinigten Staaten ergingen, hätten Unionsbürger zudem keinen wirksamen Anspruch auf rechtliches Gehör zur Frage der Überwachung und Erfassung ihrer Daten.

36. Aus den umfangreichen Unterlagen, die den im Ausgangsverfahren vorgelegten eidesstattlichen Erklärungen beigefügt seien, ergebe sich eindeutig, dass die Richtigkeit eines Großteils der Enthüllungen von Herrn Snowden nicht in Frage gestellt werde. Daraus sei zu schließen, dass die NSA und andere amerikanische Sicherheitsbehörden wie das Federal Bureau of Investigation (FBI) auf personenbezogene Daten, die in die Vereinigten Staaten übermittelt würden, im Rahmen einer massenhaften und undifferenzierten Überwachung und Erfassung zugreifen könnten.

37. Nach irischem Recht verlange der Stellenwert der Verfassungsrechte auf Privatsphäre und Unverletzlichkeit der Wohnung, dass jeder Eingriff in diese Rechte rechtmäßig und verhältnismäßig sei. Der massenhafte und undifferenzierte Zugriff auf personenbezogene Daten stehe nicht im Einklang mit dem Erfordernis der Verhältnismäßigkeit und sei daher als Verstoß gegen die irische Verfassung anzusehen [19].

38. Die Erfassung elektronischer Kommunikation könne nur dann als verfassungsgemäß angesehen werden, wenn dargetan werde, dass eine ganz bestimmte Erfassung der Kommunikation und die Überwachung von Einzelpersonen oder Personengruppen im Interesse der nationalen Sicherheit und der Verbrechensbekämpfung objektiv gerechtfertigt seien und dass es angemessene und nachprüfbare Schutzmechanismen gebe.

39. Wäre die vorliegende Rechtssache allein nach irischem Recht zu entscheiden, wäre ein wesentlicher Streitpunkt, ob die Vereinigten Staaten „ein angemessenes Schutzniveau der Privatsphäre sowie der Grundrechte und Grundfreiheiten“ im Sinne von Section 11(1) des Data Protection Act gewährleisteten. Nach irischem Recht, insbesondere den Anforderungen seiner Verfassung, hätte der Commissioner die Beschwerde von Herrn Schrems folglich nicht zurückweisen dürfen, sondern hätte diesen Punkt prüfen müssen.

18 — Vgl. Section 702 dieses Gesetzes in der durch den Foreign Intelligence Surveillance Act of 2008 geänderten Fassung. Aufgrund dieser Section unterhält die NSA eine Datenbank namens „PRISM“ (vgl. Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection vom 27. November 2013).

19 — Der High Court nennt insbesondere den Respekt der Menschenwürde und die Freiheit des Individuums (Präambel), die persönliche Freiheit (Art. 40 Abs. 3 Unterabs. 1 und 2), die Unverletzlichkeit der Wohnung (Art. 40 Abs. 5) und den Schutz des Familienlebens (Art. 41).

40. Der High Court stellt jedoch fest, dass die Rechtssache, mit der er befasst sei, die Durchführung des Rechts der Union im Sinne von Art. 51 Abs. 1 der Charta betreffe, so dass die Rechtmäßigkeit der Entscheidung des Commissioner anhand des Unionsrechts zu prüfen sei.

41. Der Commissioner sei mit folgendem Problem konfrontiert gewesen. Gemäß Section 11(2)(a) des Data Protection Act sei er verpflichtet, die Frage der Angemessenheit des im Drittland bestehenden Schutzes „im Einklang“ mit einer von der Kommission gemäß Art. 25 Abs. 6 der Richtlinie 95/46 getroffenen Feststellung der Gemeinschaft zu beurteilen. Folglich könne er nicht von einer solchen Feststellung abweichen. Da die Kommission in ihrer Entscheidung 2000/520 festgestellt habe, dass die Vereinigten Staaten ein angemessenes Schutzniveau für die Verarbeitung von Daten durch Firmen gewährleisteten, die den Grundsätzen des sicheren Hafens beigetreten seien, müsse der Commissioner eine Beschwerde, mit der die Unangemessenheit eines solchen Schutzes gerügt werde, zwangsläufig zurückweisen.

42. Unter Hinweis darauf, dass sich der Commissioner somit ganz genau an den Wortlaut der Richtlinie 95/46 und der Entscheidung 2000/520 gehalten habe, stellt der High Court fest, dass die Kritik von Herrn Schrems in Wirklichkeit die Bestimmungen der Safe-Harbor-Regelung selbst und nicht die Art und Weise betreffe, in der der Commissioner sie angewandt habe, hebt aber hervor, dass weder die Gültigkeit der Richtlinie 95/46 noch die Gültigkeit der Entscheidung 2000/520 direkt in Frage gestellt würden.

43. Die Kernfrage gehe deshalb dahin, ob der Commissioner aus unionsrechtlicher Sicht und insbesondere im Hinblick auf das nachfolgende Inkrafttreten der Art. 7 und 8 der Charta absolut an die in der Entscheidung 2000/520 zum Ausdruck kommende Feststellung der Kommission zur Angemessenheit des Schutzes personenbezogener Daten im Recht und in der Praxis der Vereinigten Staaten gebunden sei.

44. Der High Court führt weiter aus, in dem Verfahren, mit dem er befasst sei, seien die Handlungen von Facebook Ireland und Facebook USA als solche nicht gerügt worden. Art. 3 Abs. 1 Buchst. b der Entscheidung 2000/520, der es den zuständigen nationalen Behörden ermögliche, ein Unternehmen anzuweisen, die Datenübermittlung in ein Drittland auszusetzen, gelte jedoch nur für Fälle, in denen sich die Beschwerde – anders als im vorliegenden Fall – gegen das Verhalten des betreffenden Unternehmens richte.

45. Gerügt werde daher nicht das Verhalten von Facebook USA als solches, sondern die Tatsache, dass die Kommission anerkannt habe, dass das Recht und die Praxis der Vereinigten Staaten einen angemessenen Datenschutz gewährleisteten, obgleich aus den Enthüllungen von Herrn Snowden klar hervorgehe, dass die amerikanischen Behörden auf personenbezogene Daten der im Unionsgebiet lebenden Bevölkerung massenhaft und undifferenziert zugreifen könnten [20].

46. Insoweit sei schwer vorstellbar, wie die Entscheidung 2000/520 in der Praxis den Anforderungen der Art. 7 und 8 der Charta gerecht werden könne, erst recht im Hinblick auf die vom Gerichtshof in seinem Urteil Digital Rights Ireland u. a. [21] aufgestellten Grundsätze. Insbesondere würde die in Art. 7 der Charta und in den sich aus den gemeinsamen Traditionen der Mitgliedstaaten ergebenden Grundwerten vorgesehene Garantie beeinträchtigt, wenn die Behörden auf die elektronische Kommunikation auf beliebiger und pauschaler Grundlage zugreifen könnten, ohne dass es einer objektiven, auf Erwägungen der nationalen Sicherheit oder der Verhütung eines gerade mit den Betroffenen in Zusammenhang stehenden Verbrechens basierenden und durch angemessene und

20 — Der High Court führt insoweit aus, das Hauptvorbringen von Herrn Schrems vor ihm habe darin bestanden, dass der Commissioner im Licht der jüngsten Enthüllungen von Herrn Snowden und der Tatsache, dass den Nachrichtendiensten der Vereinigten Staaten in großem Umfang private Daten zur Verfügung gestellt worden seien, nicht zu dem Schluss hätte kommen dürfen, dass in diesem Drittland ein angemessenes Schutzniveau für diese Daten bestehe.

21 — C-293/12 und C-594/12, EU:C:2014:238, Rn. 65 bis 69.

nachprüfbare Schutzmechanismen flankierten Rechtfertigung bedürfte. Da die Klage von Herrn Schrems darauf hindeute, dass die Entscheidung 2000/520 möglicherweise *in abstracto* unvereinbar mit den Art. 7 und 8 der Charta sei, könnte der Gerichtshof den Standpunkt einnehmen, dass die Richtlinie 95/46, speziell ihr Art. 25 Abs. 6, und die Entscheidung 2000/520 in einer Weise ausgelegt werden könnten, die es den nationalen Behörden erlauben würde, eigene Ermittlungen anzustellen, um zu klären, ob die Übermittlung personenbezogener Daten in ein Drittland den Anforderungen der Art. 7 und 8 der Charta genüge.

47. Unter diesen Umständen hat der High Court beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

Ist ein unabhängiger Amtsträger, der von Rechts wegen mit der Handhabung und der Durchsetzung von Rechtsvorschriften über den Datenschutz betraut ist, bei der Prüfung einer bei ihm eingelegten Beschwerde, dass personenbezogene Daten in ein Drittland (im vorliegenden Fall in die Vereinigten Staaten von Amerika) übermittelt würden, dessen Recht und Praxis keinen angemessenen Schutz der Betroffenen gewährleisteten, im Hinblick auf die Art. 7, 8 und 47 der Charta, unbeschadet der Bestimmungen von Art. 25 Abs. 6 der Richtlinie 95/46, absolut an die in der Entscheidung 2000/520 enthaltene gegenteilige Feststellung der Union gebunden?

Oder kann und/oder muss der Amtsträger stattdessen im Licht tatsächlicher Entwicklungen, die seit der erstmaligen Veröffentlichung der Entscheidung der Kommission eingetreten sind, eigene Ermittlungen in dieser Sache anstellen?

II – **Würdigung**

48. Mit den beiden Fragen des High Court wird der Gerichtshof aufgefordert, die Befugnisse zu präzisieren, über die die nationalen Kontrollstellen verfügen, wenn sie mit einer Beschwerde über eine Übermittlung personenbezogener Daten an ein Unternehmen mit Sitz in einem Drittland befasst sind und zur Stützung dieser Beschwerde behauptet wird, dass dieses Drittland kein angemessenes Schutzniveau für die übermittelten Daten gewährleiste, obwohl die Kommission auf der Grundlage von Art. 25 Abs. 6 der Richtlinie 95/46 eine Entscheidung erlassen hat, mit der die Angemessenheit des von diesem Drittland gewährleisteten Schutzniveaus anerkannt wird.

49. Ich weise darauf hin, dass die von Herrn Schrems beim Commissioner eingelegte Beschwerde zwei Dimensionen aufweist. Mit ihr soll die Übermittlung personenbezogener Daten durch Facebook Ireland an Facebook USA beanstandet werden. Herr Schrems beantragt, diese Übermittlung auszusetzen, da die Vereinigten Staaten kein angemessenes Schutzniveau der im Rahmen der Safe-Harbor-Regelung übermittelten personenbezogenen Daten gewährleisteten. Er wirft diesem Drittland konkret vor, das Programm PRISM aufgelegt zu haben, das es der NSA ermögliche, frei auf große Datenmengen zuzugreifen, die auf Servern in den Vereinigten Staaten gespeichert seien. Somit betrifft die Beschwerde speziell Übermittlungen personenbezogener Daten von Facebook Ireland an Facebook USA; zugleich wird mit ihr allgemeiner das im Rahmen der Safe-Harbor-Regelung für solche Daten gewährleistete Schutzniveau in Frage gestellt.

50. Der Commissioner hat die Ansicht vertreten, die bloße Existenz einer Entscheidung der Kommission, mit der anerkannt werde, dass die Vereinigten Staaten im Rahmen der Safe-Harbor-Regelung ein angemessenes Schutzniveau gewährleisteten, hindere ihn daran, die Beschwerde zu prüfen.

51. Die beiden Fragen, mit denen in Erfahrung gebracht werden soll, ob Art. 28 der Richtlinie 95/46 im Licht der Art. 7 und 8 der Charta dahin auszulegen ist, dass eine von der Kommission auf der Grundlage von Art. 25 Abs. 6 dieser Richtlinie erlassene Entscheidung eine nationale Kontrollstelle daran hindert, eine Beschwerde zu prüfen, mit der gerügt wird, dass ein Drittland kein angemessenes Schutzniveau der übermittelten personenbezogenen Daten gewährleiste, und die Übermittlung dieser Daten gegebenenfalls auszusetzen, sind daher zusammen zu prüfen.

52. Art. 7 der Charta garantiert das Recht auf Achtung des Privatlebens, während ihr Art. 8 ausdrücklich das Recht auf den Schutz personenbezogener Daten vorsieht. Art. 8 Abs. 2 und 3 bestimmt, dass diese Daten nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden dürfen, dass jede Person das Recht hat, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken, und dass die Einhaltung dieser Vorschriften von einer unabhängigen Stelle überwacht wird.

A – *Zu den Befugnissen der nationalen Kontrollstellen im Fall einer Angemessenheitsentscheidung der Kommission*

53. Nach den Angaben von Herrn Schrems in seinen für die Zwecke der im Ausgangsverfahren in Rede stehenden Beschwerde abgegebenen Erklärungen betrifft die zentrale Frage die Übermittlung personenbezogener Daten von Facebook Ireland an Facebook USA im Licht des allgemeinen Zugangs, den die NSA und andere amerikanische Sicherheitsbehörden aufgrund der ihnen nach den amerikanischen Rechtsvorschriften zustehenden Befugnisse zu den bei Facebook USA gespeicherten Daten haben.

54. Herr Schrems führt aus, wenn eine nationale Kontrollstelle mit einer Beschwerde befasst werde, mit der die Feststellung, dass ein Drittland ein angemessenes Schutzniveau der übermittelten Daten gewährleiste, in Frage gestellt werde, sei sie, wenn sie über Anhaltspunkte dafür verfüge, dass das Vorbringen in dieser Beschwerde begründet sei, befugt, die Aussetzung der Datenübermittlung durch das in der Beschwerde bezeichnete Unternehmen anzuordnen.

55. In Anbetracht der Verpflichtungen des Commissioner, die Grundrechte von Herrn Schrems zu schützen, müsse er nicht nur eine Untersuchung durchführen, sondern auch, falls der Beschwerde stattgegeben werde, von seinen Befugnissen zur Aussetzung der Datenübermittlung zwischen Facebook Ireland und Facebook USA Gebrauch machen.

56. Der Commissioner hat die Beschwerde jedoch auf der Grundlage der Bestimmungen des Data Protection Act zurückgewiesen, in denen seine Befugnisse aufgezählt werden. Dieser Schlussfolgerung lag seine Auffassung zugrunde, dass er an die Entscheidung 2000/520 gebunden sei.

57. Das zentrale Problem in der vorliegenden Rechtssache besteht folglich darin, ob die in der Entscheidung 2000/520 enthaltene Beurteilung der Kommission hinsichtlich der Angemessenheit des Schutzniveaus die nationale Datenschutzbehörde absolut bindet und sie daran hindert, Behauptungen zu untersuchen, mit denen diese Feststellung in Frage gestellt werden soll. Die Vorlagefragen betreffen somit den Umfang der Untersuchungsbefugnisse der nationalen Datenschutzbehörden im Fall des Vorliegens einer Angemessenheitsentscheidung der Kommission.

58. Nach Auffassung der Kommission ist der Verzahnung zwischen ihren eigenen Befugnissen und denen der nationalen Datenschutzbehörden Rechnung zu tragen. Die Zuständigkeiten Letzterer konzentrierten sich auf die Anwendung der einschlägigen Rechtsvorschriften in Einzelfällen, während die allgemeine Überprüfung der Anwendung der Entscheidung 2000/520, einschließlich ihrer etwaigen Aussetzung oder Aufhebung, in die Zuständigkeit der Kommission falle.

59. Die Kommission macht geltend, Herr Schrems habe keine konkreten Argumente vorgebracht, die die Annahme zuließen, dass er unmittelbar Gefahr laufe, aufgrund der Datenübermittlung zwischen Facebook Ireland und Facebook USA schwerwiegende Schäden zu erleiden. Aufgrund ihrer abstrakten und allgemeinen Natur seien die von Herrn Schrems geäußerten Besorgnisse über die von den amerikanischen Sicherheitsbehörden aufgelegten Überwachungsprogramme vielmehr mit denen identisch, die die Kommission dazu bewogen hätten, eine Überprüfung der Entscheidung 2000/520 einzuleiten.

60. Die nationalen Kontrollstellen würden in ihre Zuständigkeit für die Neuverhandlung der Bedingungen dieser Entscheidung mit den Vereinigten Staaten oder, falls erforderlich, für deren Aussetzung eingreifen, wenn sie auf der Grundlage von Beschwerden, in denen lediglich strukturelle und abstrakte Besorgnisse geäußert würden, Maßnahmen träfen.

61. Ich teile den Standpunkt der Kommission nicht. Meiner Meinung nach kann eine von der Kommission auf der Grundlage von Art. 25 Abs. 6 der Richtlinie 95/46 erlassene Entscheidung die Befugnisse, die den nationalen Kontrollstellen nach Art. 28 dieser Richtlinie zustehen, weder aufheben noch auch nur verringern. Werden nationale Kontrollstellen im Rahmen von Einzelbeschwerden angerufen, sind sie entgegen dem Vorbringen der Kommission meines Erachtens nicht daran gehindert, sich aufgrund ihrer Ermittlungsbefugnisse und ihrer Unabhängigkeit ihre eigene Meinung zu dem von einem Drittland gewährleisteten allgemeinen Schutzniveau zu bilden und daraus Konsequenzen zu ziehen, wenn sie über Einzelfälle entscheiden.

62. Aus einer ständigen Rechtsprechung des Gerichtshofs ergibt sich, dass bei der Auslegung von Unionsvorschriften nicht nur deren Wortlaut zu berücksichtigen ist, sondern auch ihr Zusammenhang und die Ziele, die mit der Regelung, zu der sie gehören, verfolgt werden [22].

63. Der 62. Erwägungsgrund der Richtlinie 95/46 lautet: „Die Einrichtung unabhängiger Kontrollstellen in den Mitgliedstaaten ist ein wesentliches Element des Schutzes der Personen bei der Verarbeitung personenbezogener Daten."

64. In Art. 28 Abs. 1 Unterabs. 1 dieser Richtlinie heißt es: „Die Mitgliedstaaten sehen vor, dass eine oder mehrere öffentliche Stellen beauftragt werden, die Anwendung der von den Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen." Art. 28 Abs. 1 Unterabs. 2 der Richtlinie bestimmt: „Diese Stellen nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr."

65. In Art. 28 Abs. 3 der Richtlinie 95/46 werden die Befugnisse aufgezählt, über die jede Kontrollstelle verfügt, nämlich Ermittlungsbefugnisse, wirksame Einwirkungsbefugnisse, die es ihnen u. a. ermöglichen, eine Verarbeitung vorläufig oder endgültig zu verbieten, sowie das Klagerecht oder eine Anzeigebefugnis bei Verstößen gegen die einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie.

66. Darüber hinaus heißt es in Art. 28 Abs. 4 Unterabs. 1 der Richtlinie 95/46: „Jede Person … kann sich zum Schutz der die Person betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten an jede Kontrollstelle mit einer Eingabe wenden." Art. 28 Abs. 4 Unterabs. 2 dieser Richtlinie sieht vor: „Jede Kontrollstelle kann insbesondere von jeder Person mit dem Antrag befasst werden, die Rechtmäßigkeit einer Verarbeitung zu überprüfen, wenn einzelstaatliche Vorschriften gemäß Artikel 13 Anwendung finden." Nach der letztgenannten

22 — Vgl. u. a. Urteil Koushkaki (C-84/12, EU:C:2013:862, Rn. 34 und die dort angeführte Rechtsprechung).

Vorschrift können die Mitgliedstaaten Rechtsvorschriften erlassen, die mehrere in der Richtlinie 95/46 vorgesehene Pflichten und Rechte beschränken, sofern eine solche Beschränkung u. a. für die Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten notwendig ist.

67. Wie der Gerichtshof bereits festgestellt hat, ergibt sich das Erfordernis, die Einhaltung der Unionsvorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch eine unabhängige Stelle zu überwachen, auch aus dem Primärrecht der Union, insbesondere aus Art. 8 Abs. 3 der Charta und aus Art. 16 Abs. 2 AEUV [23]. Er hat darüber hinaus darauf hingewiesen, dass „[d]ie Einrichtung unabhängiger Kontrollstellen in den Mitgliedstaaten … daher … ein wesentliches Element des Schutzes der Personen bei der Verarbeitung personenbezogener Daten dar[stellt]“ [24].

68. Der Gerichtshof hat ferner entschieden, dass „Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 dahin auszulegen ist, dass die für die Überwachung der Verarbeitung personenbezogener Daten zuständigen Kontrollstellen mit einer Unabhängigkeit ausgestattet sein müssen, die es ihnen ermöglicht, ihre Aufgaben ohne äußere Einflussnahme wahrzunehmen. Diese Unabhängigkeit schließt u. a. jede Anordnung und jede sonstige wie auch immer geartete äußere Einflussnahme aus, sei sie unmittelbar oder mittelbar, an denen ihre Entscheidungen ausgerichtet werden könnten und durch die in Frage gestellt werden könnte, dass die genannten Kontrollstellen ihre Aufgabe erfüllen, zwischen dem Schutz des Rechts auf Privatsphäre und dem freien Verkehr personenbezogener Daten ein ausgewogenes Verhältnis herzustellen.“ [25]

69. Der Gerichtshof hat darüber hinaus klargestellt, dass „[d]ie Gewährleistung der Unabhängigkeit der nationalen Kontrollstellen … die wirksame und zuverlässige Kontrolle der Einhaltung der Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sicherstellen soll“ [26]. Diese Gewährleistung der Unabhängigkeit wurde eingeführt, „um die von [den] Entscheidungen [dieser nationalen Kontrollstellen] betroffenen Personen und Einrichtungen stärker zu schützen“ [27].

70. Wie u. a. aus dem zehnten Erwägungsgrund und aus Art. 1 der Richtlinie 95/46 hervorgeht, hat diese zum Ziel, innerhalb der Union „bei der Verarbeitung personenbezogener Daten ein hohes Niveau des Schutzes der Grundrechte und Grundfreiheiten zu gewährleisten“ [28]. Nach Auffassung des Gerichtshofs sind „[d]ie in Art. 28 der Richtlinie 95/46 vorgesehenen Kontrollstellen … somit die Hüter dieser Grundrechte und Grundfreiheiten“ [29].

71. Unter Berücksichtigung der bedeutenden Rolle, die den nationalen Kontrollstellen auf dem Gebiet des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten zufällt, müssen ihre Einwirkungsbefugnisse selbst dann unangetastet bleiben, wenn die Kommission auf der Grundlage von Art. 25 Abs. 6 der Richtlinie 95/46 eine Entscheidung erlassen hat.

72. Insoweit deutet nichts darauf hin, dass die Regelungen für die Übermittlung personenbezogener Daten in Drittländer vom sachlichen Anwendungsbereich des Art. 8 Abs. 3 der Charta ausgenommen wären, in dem auf der höchsten Stufe der Normenhierarchie des Unionsrechts die Bedeutung einer Überwachung der Einhaltung der Vorschriften über den Schutz personenbezogener Daten durch eine unabhängige Stelle festgeschrieben wird.

23 — Vgl. Urteile Kommission/Österreich (C-614/10, EU:C:2012:631, Rn. 36) und Kommission/Ungarn (C-288/12, EU:C:2014:237, Rn 47).

24 — Vgl. u. a. Urteil Kommission/Ungarn (C-288/12, EU:C:2014:237, Rn. 48 und die dort angeführte Rechtsprechung); vgl. in diesem Sinne auch Urteil Digital Rights Ireland u. a. (C-293/12 und C-594/12, EU:C:2014:238, Rn. 68 und die dort angeführte Rechtsprechung).

25 — Vgl. u. a. Urteil Kommission/Ungarn (C-288/12, EU:C:2014:237, Rn. 51 und die dort angeführte Rechtsprechung).

26 — Urteil Kommission/Deutschland (C-518/07, EU:C:2010:125, Rn. 25).

27 — Ebd.

28 — Ebd. (Rn. 22 und die dort angeführte Rechtsprechung).

29 — Ebd. (Rn. 23). Vgl. in diesem Sinne auch Urteile Kommission/Österreich (C-614/10, EU:C:2012:631, Rn. 52) und Kommission/Ungarn (C-288/12, EU:C:2014:237, Rn. 53).

73. Wären die nationalen Kontrollstellen an die Entscheidungen der Kommission absolut gebunden, würde dies ihre völlige Unabhängigkeit unweigerlich einschränken. Entsprechend ihrer Rolle als Hüterinnen der Grundrechte müssen die nationalen Kontrollstellen ihnen vorgelegte Beschwerden im übergeordneten Interesse des Schutzes von Einzelpersonen bei der Verarbeitung personenbezogener Daten in völliger Unabhängigkeit untersuchen können.

74. Darüber hinaus besteht, wie die belgische Regierung und das Europäische Parlament in der mündlichen Verhandlung zu Recht festgestellt haben, kein hierarchisches Verhältnis zwischen Kapitel IV der Richtlinie 95/46, das sich auf die Übermittlung personenbezogener Daten in Drittländer bezieht, und ihrem Kapitel VI, das u. a. der Rolle der nationalen Kontrollstellen gewidmet ist. Nichts in Kapitel VI deutet darauf hin, dass die Vorschriften über die nationalen Kontrollstellen den gesonderten Vorschriften über Übermittlungen in Kapitel IV der Richtlinie 95/46 in irgendeiner Weise untergeordnet wären.

75. Aus Art. 25 Abs. 1 dieser Richtlinie, der sich in deren Kapitel IV befindet, geht im Gegenteil ausdrücklich hervor, dass die Genehmigung der Übermittlung personenbezogener Daten in ein Drittland, das ein angemessenes Schutzniveau gewährleistet, nur vorbehaltlich der Beachtung der aufgrund der anderen Bestimmungen der Richtlinie erlassenen einzelstaatlichen Vorschriften gilt.

76. Insoweit erinnere ich daran, dass die Mitgliedstaaten nach dieser Vorschrift in ihren nationalen Rechtsvorschriften vorsehen müssen, dass die Übermittlung personenbezogener Daten, die Gegenstand einer Verarbeitung sind oder nach der Übermittlung verarbeitet werden sollen, in ein Drittland vorbehaltlich der Beachtung der aufgrund der anderen Bestimmungen der Richtlinie 95/46 erlassenen einzelstaatlichen Vorschriften zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet.

77. Mit Art. 28 Abs. 1 dieser Richtlinie werden die nationalen Kontrollstellen beauftragt, die Anwendung der von den Mitgliedstaaten zur Umsetzung der Richtlinie erlassenen einzelstaatlichen Vorschriften im Hoheitsgebiet jedes einzelnen Mitgliedstaats zu überwachen.

78. Die Gegenüberstellung dieser beiden Vorschriften lässt den Schluss zu, dass die in Art. 25 Abs. 1 der Richtlinie 95/46 aufgestellte Regel, wonach die Übermittlung personenbezogener Daten nur zulässig ist, wenn das empfangende Drittland ein angemessenes Schutzniveau für sie gewährleistet, zu den Vorschriften gehört, deren Anwendung die nationalen Kontrollstellen zu überwachen haben.

79. Im Einklang mit Art. 8 Abs. 3 der Charta sind die Befugnisse der nationalen Kontrollstellen zu einer völlig unabhängigen Untersuchung der Beschwerden, mit denen sie im Rahmen von Art. 28 der Richtlinie 95/46 befasst werden, weit auszulegen. Diese Befugnisse können daher nicht durch die Befugnisse eingeschränkt werden, die der Kommission vom Unionsgesetzgeber durch Art. 25 Abs. 6 der Richtlinie zur Feststellung der Angemessenheit des von einem Drittland gebotenen Schutzniveaus verliehen wurden.

80. In Anbetracht ihrer wesentlichen Rolle auf dem Gebiet des Schutzes personenbezogener Daten müssen die nationalen Kontrollstellen eine Untersuchung durchführen können, wenn sie mit einer Beschwerde befasst werden, die Anhaltspunkte enthält, die das von einem Drittland gewährleistete Schutzniveau in Frage stellen könnten, und zwar auch dann, wenn die Kommission in einer auf der Grundlage von Art. 25 Abs. 6 der Richtlinie 95/46 ergangenen Entscheidung festgestellt hat, dass das betreffende Drittland ein angemessenes Schutzniveau gewährleistet.

81. Vertritt eine nationale Kontrollstelle nach den von ihr durchgeführten Ermittlungen die Ansicht, dass die beanstandete Datenübermittlung den Schutz beeinträchtigt, in dessen Genuss die Unionsbürger bei der Verarbeitung ihrer Daten kommen müssen, ist sie unabhängig von der allgemeinen Beurteilung in der Entscheidung der Kommission zur Aussetzung der in Rede stehenden Datenübermittlung befugt.

82. Nach dem Wortlaut von Art. 25 Abs. 2 der Richtlinie 95/46 steht nämlich fest, dass die Angemessenheit des Schutzniveaus, das ein Drittland bietet, anhand einer Reihe von Umständen sowohl tatsächlicher als auch rechtlicher Natur beurteilt wird. Ändert sich einer dieser Umstände und scheint geeignet zu sein, die Angemessenheit des von einem Drittland gebotenen Schutzniveaus in Frage zu stellen, muss die mit einer Beschwerde befasste nationale Kontrollstelle daraus die Konsequenzen für die beanstandete Übermittlung ziehen können.

83. Wie Irland ausgeführt hat, ist der Commissioner zwar ebenso wie die anderen staatlichen Stellen an die Entscheidung 2000/520 gebunden. Aus Art. 288 Abs. 4 AEUV ergibt sich nämlich, dass Beschlüsse eines Unionsorgans in allen ihren Teilen verbindlich sind. Daher bindet die Entscheidung 2000/520 die Mitgliedstaaten, an die sie gerichtet ist.

84. Die Entscheidung 2000/520 bestimmt in ihrem Art. 5 insoweit selbst, dass „[d]ie Mitgliedstaaten … binnen 90 Tagen, nachdem sie von [ihr] in Kenntnis gesetzt worden sind, alle für ihre Umsetzung erforderlichen Maßnahmen [ergreifen]“. Darüber hinaus bestätigt Art. 6 dieser Entscheidung, dass sie „an alle Mitgliedstaaten gerichtet [ist]“.

85. Ich bin jedoch der Ansicht, dass die Bindungswirkung der Entscheidung 2000/520 in Anbetracht der vorerwähnten Bestimmungen der Richtlinie 95/46 und der Charta nicht geeignet ist, jede Untersuchung von Beschwerden durch den Commissioner auszuschließen, mit denen gerügt wird, dass im Rahmen dieser Entscheidung vorgenommene Übermittlungen personenbezogener Daten in die Vereinigten Staaten nicht die unionsrechtlich notwendigen Schutzgarantien aufwiesen. Mit anderen Worten gebietet eine solche Bindungswirkung nicht, dass jede derartige Beschwerde summarisch, d. h. unmittelbar und ohne jede Prüfung ihrer Begründetheit, zurückgewiesen wird.

86. Wie zudem aus der Systematik von Art. 25 der Richtlinie 95/46 hervorgeht, kann die Feststellung, ob ein Drittland ein angemessenes Schutzniveau gewährleistet, entweder von den Mitgliedstaaten oder von der Kommission getroffen werden. Es handelt sich daher um eine geteilte Zuständigkeit.

87. Nach Art. 25 Abs. 6 dieser Richtlinie haben die Mitgliedstaaten, sobald die Kommission feststellt, dass ein Drittland ein angemessenes Schutzniveau im Sinne von Art. 25 Abs. 2 der Richtlinie gewährleistet, die aufgrund dieser Feststellung gebotenen Maßnahmen zu treffen.

88. Da eine solche Entscheidung zur Zulässigkeit der Übermittlungen personenbezogener Daten in ein Drittland führt, dessen Schutzniveau die Kommission als angemessen betrachtet, müssen die Mitgliedstaaten es grundsätzlich ermöglichen, dass derartige Übermittlungen von Unternehmen mit Sitz in ihrem Hoheitsgebiet vorgenommen werden.

89. Art. 25 der Richtlinie 95/46 verleiht der Kommission jedoch keine ausschließliche Zuständigkeit für die Feststellung der Angemessenheit des Schutzniveaus der übermittelten personenbezogenen Daten. Die Systematik dieses Artikels zeigt, dass den Mitgliedstaaten dabei ebenfalls eine Rolle zukommt. Eine Entscheidung der Kommission spielt zwar eine wichtige Rolle für die Vereinheitlichung der in den Mitgliedstaaten geltenden Übermittlungsvoraussetzungen. Diese Vereinheitlichung kann jedoch nur fortbestehen, solange die betreffende Feststellung nicht in Frage gestellt wird.

90. Das Argument, dass die Voraussetzungen für die Übermittlung personenbezogener Daten in ein Drittland vereinheitlicht werden müssten, findet meiner Meinung nach seine Grenze in einer Situation wie der im Ausgangsverfahren in Rede stehenden, in der die Kommission nicht nur darüber unterrichtet wird, dass ihre Feststellung Anlass zu Kritik gibt, sondern auch selbst solche Kritik äußert und Verhandlungen führt, um ihr abzuhelfen.

91. Die Beurteilung der Frage, ob das von einem Drittland gebotene Schutzniveau angemessen ist oder nicht, kann auch zu einer Zusammenarbeit zwischen den Mitgliedstaaten und der Kommission führen. Art. 25 Abs. 3 der Richtlinie 95/46 sieht insoweit vor, dass „[d]ie Mitgliedstaaten und die Kommission … einander über die Fälle [unterrichten], in denen ihres Erachtens ein Drittland kein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet". Wie das Parlament ausführt, zeigt dies deutlich, dass den Mitgliedstaaten und der Kommission bei der Ermittlung von Fällen, in denen ein Drittland kein angemessenes Schutzniveau gewährleistet, eine gleichwertige Rolle zukommt.

92. Die Angemessenheitsentscheidung soll die Übermittlung personenbezogener Daten in das betreffende Drittland gestatten. Dies bedeutet nicht, dass die Kontrollstellen von den Unionsbürgern nicht länger mit einem Antrag befasst werden können, der auf den Schutz ihrer personenbezogenen Daten gerichtet ist. In diesem Zusammenhang ist anzumerken, dass Art. 28 Abs. 4 Unterabs. 1 der Richtlinie 95/46, wonach sich „[j]ede Person … zum Schutz der die Person betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten an jede Kontrollstelle mit einer Eingabe wenden [kann]", keine Ausnahme von diesem Grundsatz für den Fall vorsieht, dass es eine von der Kommission in Anwendung von Art. 25 Abs. 6 dieser Richtlinie erlassene Entscheidung gibt.

93. Somit führt eine von der Kommission in Anwendung der ihr durch die letztgenannte Vorschrift übertragenen Durchführungsbefugnisse erlassene Entscheidung zwar dazu, dass die Übermittlung personenbezogener Daten in ein Drittland gestattet ist, doch kann eine solche Entscheidung nicht die Wirkung haben, dass den Mitgliedstaaten und insbesondere ihren nationalen Kontrollstellen jede Befugnis genommen wird oder auch nur ihre Zuständigkeiten eingeschränkt werden, wenn sie mit mutmaßlichen Grundrechtsverletzungen konfrontiert sind.

94. Eine nationale Kontrollstelle muss in der Lage sein, die in Art. 28 Abs. 3 der Richtlinie 95/46 vorgesehenen Befugnisse auszuüben, zu denen das vorläufige oder endgültige Verbot einer Verarbeitung personenbezogener Daten gehört. Zwar enthält die Aufzählung in dieser Vorschrift nicht ausdrücklich Befugnisse, die sich auf eine Übermittlung von einem Mitgliedstaat in ein Drittland beziehen, doch ist eine solche Übermittlung meiner Meinung nach als Datenverarbeitung einzustufen [30]. Wie sich aus dem Wortlaut der genannten Vorschrift ergibt, ist die Aufzählung überdies nicht erschöpfend. In Anbetracht der wesentlichen Rolle der nationalen Kontrollstellen in dem durch die Richtlinie 95/46 geschaffenen System müssen diese jedenfalls über die Befugnis verfügen, eine Datenübermittlung im Fall einer erwiesenen oder drohenden Beeinträchtigung der Grundrechte auszusetzen.

95. Hinzufügen ist, dass nicht nur gegen den Unabhängigkeitsgrundsatz, sondern auch gegen das Ziel der Richtlinie 95/46, das sich aus deren Art. 1 Abs. 1 ergibt, verstoßen würde, wenn der nationalen Kontrollstelle unter Umständen wie den in der vorliegenden Rechtssache in Rede stehenden ihre Ermittlungsbefugnisse genommen würden.

96. Wie der Gerichtshof festgestellt hat, geht „[a]us den Erwägungsgründen 3, 8 und 10 der Richtlinie 95/46 … hervor, dass der Unionsgesetzgeber beabsichtigte, den freien Verkehr der personenbezogenen Daten zu erleichtern, indem die Rechtsvorschriften der Mitgliedstaaten angeglichen werden, aber die Grundrechte der Personen, insbesondere das Recht auf Schutz des Privatlebens, dabei geschützt werden und ein hohes Schutzniveau in der Union sichergestellt wird. Art. 1 dieser Richtlinie sieht somit vor, dass die Mitgliedstaaten den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten gewährleisten müssen." [31]

30 — Vgl. Schlussanträge des Generalanwalts Léger in der Rechtssache Parlament/Rat und Kommission (C-317/04, EU:C:2005:710, Nrn. 92 bis 95). Vgl. auch Urteil Parlament/Rat und Kommission (C-317/04 und C-318/04, EU:C:2006:346, Rn. 56).

31 — Vgl. u. a. Urteil IPI (C-473/12, EU:C:2013:715, Rn. 28 und die dort angeführte Rechtsprechung).

97. Die Bestimmungen der Richtlinie 95/46 sind daher im Einklang mit deren Ziel auszulegen, das darin besteht, ein hohes Niveau des Schutzes der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihrer Privatsphäre bei der Verarbeitung personenbezogener Daten innerhalb der Union sicherzustellen.

98. Aufgrund der Bedeutung dieses Ziels und der Rolle, die den Mitgliedstaaten bei seiner Erreichung zukommt, können die Mitgliedstaaten und damit die dort angesiedelten nationalen Kontrollstellen nicht absolut an eine Angemessenheitsentscheidung der Kommission gebunden sein, wenn besondere Umstände im Fall der Übermittlung personenbezogener Daten in ein Drittland erhebliche Zweifel an der Beachtung der von der Charta garantierten Grundrechte aufkommen lassen.

99. Der Gerichtshof hat bereits entschieden, dass „die Bestimmungen der Richtlinie 95/46, soweit sie Verarbeitungen personenbezogener Daten betreffen, die zu Beeinträchtigungen der Grundfreiheiten und insbesondere des Rechts auf Achtung des Privatlebens führen können, im Licht der Grundrechte auszulegen sind, die nach ständiger Rechtsprechung zu den allgemeinen Rechtsgrundsätzen gehören, deren Wahrung der Gerichtshof zu sichern hat, und nun in der Charta verankert sind“ [32].

100. Ich verweise zudem auf die Rechtsprechung, wonach „die Mitgliedstaaten nicht nur ihr nationales Recht unionsrechtskonform auszulegen, sondern auch darauf zu achten [haben], dass sie sich nicht auf eine Auslegung einer Vorschrift des abgeleiteten Rechts stützen, die mit den durch die Unionsrechtsordnung geschützten Grundrechten oder den anderen allgemeinen Grundsätzen des Unionsrechts kollidiert“ [33].

101. Der Gerichtshof hat daher in seinem Urteil N. S. u. a. [34] entschieden, dass „eine Anwendung der Verordnung [(EG)] Nr. 343/2003[[35]] auf der Grundlage einer unwiderlegbaren Vermutung, dass die Grundrechte des Asylbewerbers in dem für die Entscheidung über seinen Antrag normalerweise zuständigen Mitgliedstaat beachtet werden, mit der Pflicht der Mitgliedstaaten zu grundrechtskonformer Auslegung und Anwendung der Verordnung Nr. 343/2003 unvereinbar [ist]“ [36].

102. Im Kontext des Status der Mitgliedstaaten als im Verhältnis zueinander für rechtliche und praktische Zwecke im Zusammenhang mit dem Recht auf Asyl sichere Herkunftsländer hat der Gerichtshof insoweit anerkannt, dass die Vermutung gelten muss, dass die Behandlung der Asylbewerber in jedem Mitgliedstaat im Einklang mit den Erfordernissen der Charta, dem am 28. Juli 1951 in Genf unterzeichneten Abkommen über die Rechtsstellung der Flüchtlinge [37] und der am 4. November 1950 in Rom unterzeichneten Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten steht [38]. Der Gerichtshof hat jedoch entschieden, dass „nicht ausgeschlossen werden [kann], dass dieses System in der Praxis auf größere Funktionsstörungen in einem bestimmten Mitgliedstaat stößt, so dass eine ernst zu nehmende Gefahr besteht, dass Asylbewerber bei einer Überstellung in diesen Mitgliedstaat in einer Weise behandelt werden, die mit ihren Grundrechten unvereinbar ist“ [39].

32 — Vgl. u. a. Urteil Google Spain und Google (C-131/12, EU:C:2014:317, Rn. 68 und die dort angeführte Rechtsprechung).

33 — Vgl. u. a. Urteil N. S. u. a. (C-411/10 und C-493/10, EU:C:2011:865, Rn. 77 und die dort angeführte Rechtsprechung).

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

35 — Verordnung des Rates vom 18. Februar 2003 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen in einem Mitgliedstaat gestellten Asylantrags zuständig ist (ABl. L 50, S. 1).

36 — Rn. 99 dieses Urteils.

37 — *United Nations Treaty Series*, vol. 189, S. 150, Nr. 2545 (1954).

38 — Vgl. Urteil N. S. u. a. (C-411/10 und C-493/10, EU:C:2011:865, Rn. 80).

39 — Ebd. (Rn. 81).

103. Infolgedessen hat der Gerichtshof festgestellt, dass „es den Mitgliedstaaten einschließlich der nationalen Gerichte [obliegt], einen Asylbewerber nicht an den ‚zuständigen Mitgliedstaat' im Sinne der Verordnung Nr. 343/2003 zu überstellen, wenn ihnen nicht unbekannt sein kann, dass die systemischen Mängel des Asylverfahrens und der Aufnahmebedingungen für Asylbewerber in diesem Mitgliedstaat ernsthafte und durch Tatsachen bestätigte Gründe für die Annahme darstellen, dass der Antragsteller tatsächlich Gefahr läuft, einer unmenschlichen oder erniedrigenden Behandlung im Sinne von Art. 4 der Charta ausgesetzt zu werden" [40].

104. Die Erkenntnisse aus dem Urteil N. S. u. a. [41] können meines Erachtens auf eine Situation wie die im Ausgangsverfahren in Rede stehende übertragen werden. Somit ist eine Auslegung des abgeleiteten Unionsrechts, die auf einer unwiderlegbaren Vermutung beruhen würde, dass die Grundrechte – sei es von einem Mitgliedstaat, der Kommission oder einem Drittland – beachtet werden, als mit der Pflicht der Mitgliedstaaten zu grundrechtskonformer Auslegung und Anwendung des abgeleiteten Unionsrechts unvereinbar anzusehen. Art. 25 Abs. 6 der Richtlinie 95/46 schreibt daher in Bezug auf die Beurteilung der Angemessenheit des von einem Drittland gebotenen Schutzniveaus durch die Kommission keine solche unwiderlegbare Vermutung der Beachtung der Grundrechte vor. Die dieser Vorschrift zugrunde liegende Vermutung, dass bei der Datenübermittlung an ein Drittland die Grundrechte beachtet werden, muss vielmehr als widerlegbar angesehen werden [42]. Folglich sollte die genannte Vorschrift nicht so ausgelegt werden, dass sie die u. a. in Art. 28 Abs. 3 der Richtlinie 95/46 und in Art. 8 Abs. 3 der Charta enthaltenen Garantien zum Schutz und zur Beachtung des Rechts auf den Schutz personenbezogener Daten in Frage stellt.

105. Ich leite aus dem genannten Urteil daher ab, dass die Mitgliedstaaten bei systemischen Mängeln in dem Drittland, in das personenbezogene Daten übermittelt werden, die Möglichkeit haben müssen, die zur Wahrung der durch die Art. 7 und 8 der Charta geschützten Grundrechte erforderlichen Maßnahmen zu treffen.

106. Darüber hinaus kann der Erlass einer Angemessenheitsentscheidung durch die Kommission, wie die italienische Regierung in ihren Erklärungen ausgeführt hat, nicht dazu führen, dass der Schutz der Unionsbürger bei der Verarbeitung ihrer Daten, wenn diese in ein Drittland übermittelt werden, geringer ist als das Schutzniveau, in dessen Genuss sie kämen, wenn ihre Daten innerhalb der Union verarbeitet würden. Die nationalen Kontrollstellen müssen demzufolge tätig werden und ihre Befugnisse in Bezug auf Datenübermittlungen in Drittländer, die Gegenstand einer Angemessenheitsentscheidung sind, ausüben können. Andernfalls wären die Unionsbürger weniger gut geschützt als bei einer Verarbeitung ihrer Daten innerhalb der Union.

107. Daher bewirkt der Erlass einer Entscheidung nach Art. 25 Abs. 6 der Richtlinie 95/46 durch die Kommission lediglich die Aufhebung des allgemeinen Verbots bei einer Ausfuhr personenbezogener Daten in Drittländer, die ein Schutzniveau gewährleisten, das mit dem von der Richtlinie gebotenen Niveau vergleichbar ist. Mit anderen Worten handelt es sich nicht um die Schaffung einer speziellen Ausnahmeregelung, die den Unionsbürgern im Verhältnis zur allgemeinen, in der Richtlinie für Datenverarbeitungen innerhalb der Union vorgesehenen Regelung weniger Schutz bietet.

40 — Ebd. (Rn. 94).

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

42 — Rn. 104 des genannten Urteils.

108. Der Gerichtshof hat zwar in Rn. 63 seines Urteils Lindqvist [43] ausgeführt, dass „Kapitel IV der Richtlinie 95/46, in dem Artikel 25 steht, … eine Sonderregelung vor[sieht]“. Dies bedeutet meines Erachtens jedoch nicht, dass eine solche Regelung weniger Schutz bieten muss. Zur Erreichung des in Art. 1 Abs. 1 der Richtlinie 95/46 festgelegten Datenschutzziels erlegt deren Art. 25 den Mitgliedstaaten und der Kommission vielmehr eine Reihe von Verpflichtungen auf [44]; zudem wird in Art. 25 der Grundsatz aufgestellt, dass die Übermittlung personenbezogener Daten in ein Drittland, das kein angemessenes Schutzniveau bietet, zu untersagen ist [45].

109. Was konkret die Safe-Harbor-Regelung angeht, sieht die Kommission ein Tätigwerden der nationalen Kontrollstellen und die Aussetzung der Datenübermittlungen durch diese nur in dem durch Art. 3 Abs. 1 Buchst. b der Entscheidung 2000/520 vorgegebenen Rahmen vor.

110. Der achte Erwägungsgrund dieser Entscheidung lautet: „Im Interesse der Transparenz und um die Fähigkeit der zuständigen Behörden in den Mitgliedstaaten zu erhalten, den Schutz von Personen bei der Verarbeitung ihrer personenbezogenen Daten zu gewährleisten, ist es ungeachtet der Feststellung des angemessenen Schutzniveaus notwendig, in dieser Entscheidung die besonderen Umstände zu nennen, unter denen die Aussetzung bestimmter Datenübermittlungen gerechtfertigt sein sollte.“

111. Im Rahmen der vorliegenden Rechtssache ist speziell die Anwendung von Art. 3 Abs. 1 Buchst. b der genannten Entscheidung erörtert worden. Nach dieser Vorschrift können die nationalen Kontrollstellen die Aussetzung von Datenübermittlungen beschließen, wenn „eine hohe Wahrscheinlichkeit besteht, dass die Grundsätze verletzt werden; wenn Grund zur Annahme besteht, dass die jeweilige Durchsetzungsinstanz nicht rechtzeitig angemessene Maßnahmen ergreift bzw. ergreifen wird, um den Fall zu lösen; wenn die fortgesetzte Datenübermittlung für die betroffenen Personen das unmittelbar bevorstehende Risiko eines schweren Schadens schaffen würde und wenn die zuständigen Behörden in den Mitgliedstaaten die Organisation unter den gegebenen Umständen in angemessener Weise unterrichtet und ihr Gelegenheit zu Stellungnahme gegeben haben“.

112. Die genannte Vorschrift stellt mehrere Voraussetzungen auf, die im Verlauf des vorliegenden Verfahrens Gegenstand unterschiedlicher Auslegungen durch die Parteien waren [46]. Ohne bei diesen Auslegungen ins Detail gehen zu wollen, geht aus ihnen hervor, dass die genannten Voraussetzungen die Befugnis der nationalen Kontrollstellen zur Aussetzung von Datenübermittlungen stark einschränken.

113. Entgegen dem Vorbringen der Kommission ist Art. 3 Abs. 1 Buchst. b der Entscheidung 2000/520 jedoch im Einklang mit dem Ziel des Schutzes personenbezogener Daten, das die Richtlinie 95/46 verfolgt, sowie im Licht von Art. 8 der Charta auszulegen. Das Gebot einer grundrechtskonformen Auslegung spricht für eine weite Auslegung dieser Vorschrift.

114. Folglich können die in Art. 3 Abs. 1 Buchst. b der Entscheidung 2000/520 vorgesehenen Voraussetzungen eine nationale Kontrollstelle meines Erachtens nicht daran hindern, die Befugnisse, mit denen sie nach Art. 28 Abs. 3 der Richtlinie 95/46 ausgestattet ist, in völliger Unabhängigkeit auszuüben.

43 — C-101/01, EU:C:2003:596.

44 — Rn. 65.

45 — Rn. 64.

46 — Herr Schrems sieht die erste Voraussetzung, wonach „eine hohe Wahrscheinlichkeit besteht, dass die Grundsätze verletzt werden“, nicht als erfüllt an. Es wird nicht behauptet, dass Facebook USA als selbstzertifizierte Einrichtung, an die Daten übermittelt werden, infolge des massenhaften und undifferenzierten Zugriffs amerikanischer Behörden auf die in ihrem Besitz befindlichen Daten selbst gegen die Grundsätze des sicheren Hafens verstoßen habe. Die Grundsätze des sicheren Hafens werden nämlich durch das Recht der Vereinigten Staaten, das nach Anhang I Abs. 4 der Entscheidung 2000/520 Gesetzesrecht, staatliche Regulierungsvorschriften und Fallrecht umfasst, ausdrücklich eingeschränkt.

115. Wie die belgische und die österreichische Regierung in der mündlichen Verhandlung im Wesentlichen ausgeführt haben, ist der „Notausgang“, den Art. 3 Abs. 1 Buchst. b der Entscheidung 2000/520 darstellt, so eng, dass er schwierig in die Praxis umzusetzen ist. Er stellt kumulative Kriterien auf und setzt die Messlatte zu hoch an. Im Licht von Art. 8 Abs. 3 der Charta darf der Handlungsspielraum der nationalen Kontrollstellen in Bezug auf die sich aus Art. 28 Abs. 3 der Richtlinie 95/46 ergebenden Rechte aber nicht derart eingeschränkt werden, dass diese nicht mehr ausgeübt werden können.

116. Das Parlament hat insoweit zu Recht darauf hingewiesen, dass der Unionsgesetzgeber darüber entschieden habe, welche Befugnisse den nationalen Kontrollstellen zukommen sollten. Die der Kommission vom Unionsgesetzgeber in Art. 25 Abs. 6 der Richtlinie 95/46 verliehene Durchführungsbefugnis berührt jedoch nicht die Befugnisse, die er den nationalen Kontrollstellen in Art. 28 Abs. 3 dieser Richtlinie übertragen hat. Mit anderen Worten verfügt die Kommission nicht über die Zuständigkeit, die Befugnisse der nationalen Kontrollstellen einzuschränken.

117. Um einen angemessenen Schutz der Grundrechte natürlicher Personen bei der Verarbeitung personenbezogener Daten sicherzustellen, müssen die nationalen Kontrollstellen daher zur Durchführung von Untersuchungen ermächtigt sein, wenn Verstöße gegen diese Rechte geltend gemacht werden. Kommen sie nach solchen Ermittlungen zu dem Schluss, dass in einem Drittland, das von einer Angemessenheitsentscheidung erfasst wird, ernsthafte Anhaltspunkte für eine Beeinträchtigung des Rechts der Unionsbürger auf den Schutz ihrer personenbezogenen Daten bestehen, müssen sie die Datenübermittlung an einen in diesem Drittland ansässigen Empfänger aussetzen können.

118. Anders ausgedrückt: Unabhängig von den restriktiven Voraussetzungen, die in Art. 3 Abs. 1 Buchst. b der Entscheidung 2000/520 festgelegt sind, müssen die nationalen Kontrollstellen ihre Ermittlungen durchführen und gegebenenfalls eine Datenübermittlung aussetzen können.

119. Darüber hinaus sollten die nationalen Kontrollstellen aufgrund ihrer in einem Klagerecht oder einer Anzeigebefugnis bestehenden Befugnisse aus Art. 28 Abs. 3 der Richtlinie 95/46 bei Verstößen gegen die einzelstaatlichen Vorschriften zur Umsetzung der Richtlinie, wenn sie Kenntnis von Tatsachen haben, die belegen, dass ein Drittland kein angemessenes Schutzniveau gewährleistet, ein nationales Gericht anrufen können, das gegebenenfalls selbst darüber entscheiden kann, ob es den Gerichtshof um Vorabentscheidung über die Gültigkeit einer Angemessenheitsentscheidung der Kommission ersucht.

120. Nach alledem ist Art. 28 der Richtlinie 95/46 im Licht der Art. 7 und 8 der Charta dahin auszulegen, dass eine von der Kommission auf der Grundlage von Art. 25 Abs. 6 dieser Richtlinie erlassene Entscheidung eine nationale Kontrollstelle nicht daran hindert, eine Beschwerde zu untersuchen, mit der geltend gemacht wird, dass ein Drittland kein angemessenes Schutzniveau übermittelter personenbezogener Daten gewährleiste, und die Übermittlung dieser Daten gegebenenfalls auszusetzen.

121. Auch wenn der High Court in seiner Vorlageentscheidung hervorhebt, dass Herr Schrems mit der Klage im Ausgangsverfahren formal weder die Gültigkeit der Richtlinie 95/46 noch die Gültigkeit der Entscheidung 2000/520 angefochten habe, geht aus der Vorlageentscheidung hervor, dass sich die Kritik von Herrn Schrems in erster Linie gegen die Feststellung richtet, dass die Vereinigten Staaten im Rahmen der Safe-Harbor-Regelung ein angemessenes Schutzniveau der übermittelten personenbezogenen Daten gewährleisteten.

122. Auch aus den Erklärungen des Commissioner geht hervor, dass mit der Beschwerde von Herrn Schrems die Entscheidung 2000/520 unmittelbar in Frage gestellt werden soll. Mit der Einlegung seiner Beschwerde habe er den Wortlaut und die Funktionsweise der Safe-Harbor-Regelung als solcher anfechten wollen, weil die Massenüberwachung der in die Vereinigten Staaten übermittelten personenbezogenen Daten zeige, dass das Recht dieses Drittlands und die dort bestehenden Praktiken keinen wirklichen Schutz der genannten Daten böten.

123. Darüber hinaus weist das vorlegende Gericht selbst darauf hin, dass die durch Art. 7 der Charta und durch die gemeinsamen Grundwerte der Verfassungstraditionen der Mitgliedstaaten gebotene Garantie aufgegeben würde, wenn den Behörden gestattet würde, auf die elektronische Kommunikation in beliebiger und pauschaler Weise zuzugreifen, ohne dass es einer objektiven, auf Erwägungen der nationalen Sicherheit oder der Verhütung eines gerade mit den Betroffenen in Zusammenhang stehenden Verbrechens basierenden und durch angemessene und nachprüfbare Schutzmechanismen flankierten Rechtfertigung bedürfte [47]. Das vorlegende Gericht äußert daher indirekt Zweifel an der Gültigkeit der Entscheidung 2000/520.

124. Die Beurteilung der Frage, ob die Vereinigten Staaten im Rahmen der Safe-Harbor-Regelung ein angemessenes Schutzniveau der übermittelten personenbezogenen Daten gewährleisten, führt daher zwangsläufig zur Befassung mit der Gültigkeit dieser Entscheidung.

125. Insoweit ist festzustellen, dass der Gerichtshof, auch wenn er im Wege eines Vorabentscheidungsersuchens ausschließlich mit einer Frage nach der Auslegung des Unionsrechts befasst wird, im Rahmen des durch Art. 267 AEUV geschaffenen Instruments der Zusammenarbeit zwischen ihm und den nationalen Gerichten unter bestimmten besonderen Umständen gehalten sein kann, die Gültigkeit von Bestimmungen des abgeleiteten Rechts zu prüfen.

126. Daher hat der Gerichtshof wiederholt von Amts wegen einen Rechtsakt für ungültig erklärt, den er lediglich auslegen sollte [48]. Darüber hinaus hat er wie folgt entschieden: „Haben die von einem staatlichen Gericht vorgelegten, scheinbar auf eine Auslegung zielenden Fragen in Wahrheit eher die Gültigkeit der betroffenen Rechtsakte [der Union] zum Gegenstand, so ist der Gerichtshof dennoch gehalten, die Fragen sogleich zu bescheiden, anstatt das vorlegende Gericht zu einem Formalismus zu nötigen, der das Verfahren nach Artikel [267 AEUV] nur verzögern würde und mit dessen Wesen unvereinbar wäre.“ [49] Der Gerichtshof hat ferner bereits ausgeführt, dass die von einem vorlegenden Gericht geäußerten Zweifel an der Vereinbarkeit eines abgeleiteten Rechtsakts mit den Vorschriften über den Grundrechtsschutz so zu verstehen sind, dass damit die Gültigkeit dieses Rechtsakts im Hinblick auf das Unionsrecht in Frage gestellt wird [50].

127. Aus der Rechtsprechung des Gerichtshofs ergibt sich überdies, dass für die Rechtsakte der Organe, Institutionen und Einrichtungen der Union eine Vermutung der Rechtmäßigkeit gilt, die besagt, dass diese Akte Rechtswirkungen entfalten, solange sie nicht zurückgenommen, im Rahmen einer Nichtigkeitsklage für nichtig erklärt oder auf ein Vorabentscheidungsersuchen oder eine Einrede der Rechtswidrigkeit hin für ungültig erklärt wurden. Allein der Gerichtshof ist befugt, die Ungültigkeit eines Unionsrechtsakts festzustellen; diese Zuständigkeit soll Rechtssicherheit gewährleisten, indem sie die einheitliche Anwendung des Unionsrechts sicherstellt. In Ermangelung einer Feststellung der Ungültigkeit, einer Änderung oder einer Aufhebung durch die Kommission bleibt die Entscheidung in allen ihren Teilen verbindlich und behält ihre unmittelbare Geltung in jedem Mitgliedstaat [51].

47 — Rn. 24 der Vorlageentscheidung.

48 — Vgl. u. a. Urteile Strehl (62/76, EU:C:1977:18, Rn. 10 bis 17), Roquettes Frères (145/79, EU:C:1980:234, Rn. 6) und Schutzverband der Spirituosen-Industrie (C-457/05, EU:C:2007:576, Rn. 32 bis 39).

49 — Urteil Schwarze (16/65, EU:C:1965:117, S. 1165).

50 — Vgl. Urteil Hauer (44/79, EU:C:1979:290, Rn. 16).

51 — Vgl. u. a. Urteil CIVAD (C-533/10, EU:C:2012:347, Rn. 39 bis 41 und die dort angeführte Rechtsprechung).

128. Um dem vorlegenden Gericht eine vollständige Antwort zu liefern und die Zweifel zu zerstreuen, die im Lauf des vorliegenden Verfahrens an der Gültigkeit der Entscheidung 2000/520 geäußert worden sind, sollte der Gerichtshof deshalb meiner Meinung nach die Gültigkeit dieser Entscheidung prüfen.

129. Gleichwohl ist auch klarzustellen, dass sich die Prüfung der Gültigkeit der Entscheidung 2000/520 auf die Rügen beschränken muss, die im Rahmen des vorliegenden Verfahrens erörtert worden sind. Alle Aspekte, die sich auf die Funktionsweise der Safe-Harbor-Regelung beziehen, sind in diesem Rahmen nämlich nicht erörtert worden, weshalb nach meinem Dafürhalten hier keine erschöpfende Prüfung der Schwächen dieser Regelung vorgenommen werden kann.

130. Dagegen ist die Frage, ob der pauschale und ungezielte Zugriff der amerikanischen Nachrichtendienste auf die übermittelten Daten die Rechtmäßigkeit der Entscheidung 2000/520 beeinträchtigen kann, im Rahmen des vorliegenden Verfahrens vor dem Gerichtshof erörtert worden. Daher kann die Gültigkeit der Entscheidung aus diesem Blickwinkel geprüft werden.

B – *Zur Gültigkeit der Entscheidung 2000/520*

1. Zu den bei der Prüfung der Gültigkeit der Entscheidung 2000/520 zu berücksichtigenden Gesichtspunkten

131. Nach der Rechtsprechung ist „[i]m Rahmen einer Nichtigkeitsklage … die Rechtmäßigkeit eines Rechtsakts anhand der tatsächlichen und rechtlichen Gesichtspunkte zu prüfen, die zum Zeitpunkt des Erlasses des Rechtsakts vorliegen, da die Beurteilung der Kommission nur beanstandet werden kann, wenn sie in Anbetracht der Informationen, über die diese beim Erlass des in Rede stehenden Rechtsakts verfügte, offensichtlich falsch zu sein scheint“ [52].

132. In seinem Urteil Gaz de France – Berliner Investissement [53] hat der Gerichtshof an den Grundsatz erinnert, wonach „bei der Beurteilung der Gültigkeit eines Aktes, die der Gerichtshof im Rahmen eines Vorabentscheidungsersuchens vorzunehmen hat, normalerweise von der zum Zeitpunkt des Erlasses dieses Aktes bestehenden Lage auszugehen ist“ [54]. Er hat allerdings offenbar anerkannt, dass „die Gültigkeit eines Aktes in bestimmten Fällen anhand neuer, nach seinem Erlass eingetretener Gesichtspunkte beurteilt werden kann“ [55].

133. Der vom Gerichtshof damit skizzierten Öffnung kommt im Rahmen der vorliegenden Rechtssache meines Erachtens besondere Bedeutung zu.

134. Die auf der Grundlage von Art. 25 Abs. 6 der Richtlinie 95/46 ergangenen Entscheidungen der Kommission weisen nämlich besondere Merkmale auf. Mit ihnen soll beurteilt werden, ob das von einem Drittland gebotene Schutzniveau personenbezogener Daten angemessen ist oder nicht. Hierbei handelt es sich um eine Beurteilung, die sich nach Maßgabe des im Drittland bestehenden tatsächlichen und rechtlichen Kontexts unweigerlich ändern wird.

52 — Vgl. u. a. Urteil BVGD/Kommission (T-104/07 und T-339/08, EU:T:2013:366, Rn. 291) unter Bezugnahme auf das Urteil IECC/Kommission (C-449/98 P, EU:C:2001:275, Rn. 87).

53 — C-247/08, EU:C:2009:600.

54 — Rn. 49 und die dort angeführte Rechtsprechung.

55 — Rn. 50 und die dort angeführte Rechtsprechung. Vgl. in diesem Sinne Lenaerts, K., Maselis, I., und Gutman, K., *EU Procedural Law*, Oxford University Press, 2014, die ausführen, dass „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“ (Abschnitt 10.16, S. 471).

135. In Anbetracht dessen, dass die Angemessenheitsentscheidung eine Entscheidung besonderer Art darstellt, bedarf die Regel, wonach die Beurteilung ihrer Gültigkeit nur anhand von Gesichtspunkten vorgenommen werden kann, die zum Zeitpunkt ihres Erlasses vorlagen, vorliegend der Nuancierung. Diese Regel würde sonst dazu führen, dass bei einer vom Gerichtshof mehrere Jahre nach dem Erlass einer Angemessenheitsentscheidung vorzunehmenden Beurteilung ihrer Gültigkeit später aufgetretene Ereignisse nicht berücksichtigen werden könnten, obwohl ein Vorabentscheidungsersuchen zur Beurteilung der Gültigkeit zeitlich nicht begrenzt ist und gerade aufgrund späterer, die Schwächen des betreffenden Rechtsakts offenbarender Tatsachen veranlasst sein kann.

136. Im vorliegenden Fall zeugt die Tatsache, dass die Entscheidung 2000/520 seit etwa 15 Jahren in Kraft ist, davon, dass die Kommission ihre Bewertung aus dem Jahr 2000 stillschweigend bestätigt hat. Ist der Gerichtshof im Rahmen eines Vorabentscheidungsersuchens aufgerufen, die Gültigkeit einer Bewertung, an der die Kommission über die Jahre hinweg festgehalten hat, zu beurteilen, ist es daher nicht nur möglich, sondern auch angemessen, dass er bei dieser Bewertung die neuen, seit dem Erlass der Angemessenheitsentscheidung eingetretenen Umstände heranziehen kann.

137. Unter Berücksichtigung der besonderen Natur der Angemessenheitsentscheidung muss diese von der Kommission regelmäßig überprüft werden. Ändert die Kommission ihre Entscheidung im Anschluss an neue, in der Zwischenzeit eingetretene Ereignisse nicht ab, bestätigt sie stillschweigend, aber zwangsläufig die ursprünglich vorgenommene Würdigung. Sie bekräftigt damit ihre Feststellung, dass das betreffende Drittland ein angemessenes Schutzniveau für die übermittelten personenbezogenen Daten gewährleistet. Es obliegt dem Gerichtshof, zu prüfen, ob diese Feststellung trotz der später eingetretenen Umstände weiterhin gültig ist.

138. Um eine effektive gerichtliche Kontrolle einer derartigen Entscheidung sicherzustellen, ist die Beurteilung ihrer Gültigkeit deshalb meiner Meinung nach unter Berücksichtigung des aktuellen tatsächlichen und rechtlichen Kontexts vorzunehmen.

2. Zum Begriff des angemessenen Schutzniveaus

139. Art. 25 der Richtlinie 95/46 beruht vollständig auf dem Grundsatz, dass die Übermittlung personenbezogener Daten in ein Drittland nicht zulässig ist, es sei denn, dieses Drittland gewährleistet ein angemessenes Schutzniveau solcher Daten. Dieser Artikel soll somit die Kontinuität des von der Richtlinie im Fall einer Übermittlung personenbezogener Daten in ein Drittland gewährten Schutzes sicherstellen. Insoweit ist darauf hinzuweisen, dass die Richtlinie ein hohes Schutzniveau für Unionsbürger bei der Verarbeitung ihrer personenbezogenen Daten bietet.

140. Unter Berücksichtigung der wichtigen Rolle, die der Schutz personenbezogener Daten im Hinblick auf das Grundrecht auf Achtung des Privatlebens spielt, muss solch ein hohes Schutzniveau daher auch im Fall der Übermittlung personenbezogener Daten in ein Drittland garantiert werden.

141. Meines Erachtens darf die Kommission auf der Grundlage von Art. 25 Abs. 6 der Richtlinie 95/46 deshalb nur feststellen, dass ein Drittland ein angemessenes Schutzniveau gewährleistet, wenn sie nach einer Gesamtbewertung des Rechts und der Praxis im fraglichen Drittland nachzuweisen vermag, dass es ein Schutzniveau bietet, das dem von der Richtlinie gebotenen Niveau der Sache nach gleichwertig ist, auch wenn sich die Modalitäten dieses Schutzes von denen unterscheiden können, die es im Allgemeinen innerhalb der Union gibt.

142. Obwohl der englische Begriff „adequate“ unter sprachlichen Gesichtspunkten so verstanden werden könnte, als bezeichne er ein gerade noch zufriedenstellendes oder hinreichendes Schutzniveau und habe daher ein anderes semantisches Feld als der französische Begriff „adéquat“, ist darauf hinzuweisen, dass das Ziel der Erreichung eines hohen Schutzniveaus der Grundrechte, wie es die Richtlinie 95/46 verlangt, die einzige Leitlinie für die Auslegung dieses Begriffs sein sollte.

143. Die Prüfung des von einem Drittland gebotenen Schutzniveaus muss zwei grundlegende Elemente abdecken, nämlich den Inhalt der geltenden Vorschriften und die Mittel zur Sicherung ihrer Beachtung [56].

144. Um ein Schutzniveau zu erreichen, das dem innerhalb der Union bestehenden Niveau der Sache nach gleichwertig ist, müsste die Safe-Harbor-Regelung, die zu einem großen Teil auf der Selbstzertifizierung und Selbstbewertung durch die freiwillig an ihr teilnehmenden Unternehmen beruht, nach meinem Dafürhalten mit angemessenen Garantien und einem hinreichenden Kontrollmechanismus versehen sein. Dabei sollten Übermittlungen personenbezogener Daten in Drittländer keinen schwächeren Schutz genießen als Verarbeitungen, die innerhalb der Union vorgenommen werden.

145. In diesem Zusammenhang ist vorab darauf hinzuweisen, dass innerhalb der Union ein Ansatz vorherrscht, wonach ein externer Kontrollmechanismus in Form einer unabhängigen Stelle ein notwendiges Element jedes Systems zur Gewährleistung der Beachtung der Vorschriften für den Schutz personenbezogener Daten darstellt.

146. Um die praktische Wirksamkeit von Art. 25 Abs. 1 bis 3 der Richtlinie 95/46 zu gewährleisten, ist darüber hinaus zu berücksichtigen, dass es sich bei der Angemessenheit des von einem Drittland gebotenen Schutzniveaus um einen evolutiven Sachverhalt handelt, der sich im Lauf der Zeit nach Maßgabe einer Reihe von Faktoren ändern kann. Die Mitgliedstaaten und die Kommission müssen daher ständig jede Änderung der Gegebenheiten, die möglicherweise eine Neubewertung der Angemessenheit des von einem Drittland gebotenen Schutzniveaus erforderlich macht, aufmerksam verfolgen. Eine Bewertung der Angemessenheit dieses Schutzniveaus kann keineswegs zu einem bestimmten Zeitpunkt fixiert und anschließend, unabhängig von jeder Änderung der Gegebenheiten, die zeigt, dass das gebotene Schutzniveau in Wirklichkeit nicht mehr angemessen ist, unbegrenzt beibehalten werden.

147. Die Verpflichtung für das Drittland, ein angemessenes Schutzniveau zu gewährleisten, stellt daher eine fortlaufende Verpflichtung dar. Wird zu einem bestimmten Zeitpunkt eine Bewertung vorgenommen, setzt die Aufrechterhaltung der Angemessenheitsentscheidung voraus, dass seitdem kein Umstand eingetreten ist, der geeignet ist, die ursprüngliche Bewertung der Kommission in Frage zu stellen.

148. Es darf nämlich nicht außer Acht gelassen werden, dass das Ziel von Art. 25 der Richtlinie 95/46 darin besteht, zu verhindern, dass personenbezogene Daten in ein Drittland übermittelt werden, das unter Verstoß gegen das durch Art. 8 der Charta garantierte Grundrecht auf den Schutz personenbezogener Daten kein angemessenes Schutzniveau gewährleistet.

149. Es ist hervorzuheben, dass die der Kommission vom Unionsgesetzgeber in Art. 25 Abs. 6 der Richtlinie 95/46 verliehene Befugnis zur Feststellung, dass ein Drittland ein angemessenes Schutzniveau gewährleistet, ausdrücklich von dem Erfordernis abhängig gemacht wird, dass dieses Drittland ein Schutzniveau im Sinne von Art. 25 Abs. 2 gewährleistet. Sind neue Umstände geeignet, die ursprüngliche Bewertung der Kommission in Frage zu stellen, sollte sie ihre Entscheidung entsprechend anpassen.

56 — Vgl. S. 5 der von der Gruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten am 24. Juli 1998 angenommenen Arbeitsunterlage WP 12 der Kommission mit dem Titel „Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU“.

3. Würdigung

150. Wie bereits ausgeführt, heißt es in Art. 25 Abs. 6 der Richtlinie 95/46: „Die Kommission kann nach dem Verfahren des Artikels 31 Absatz 2 feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen, die es insbesondere infolge der Verhandlungen gemäß Absatz 5 eingegangen ist, hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet.“ In Verbindung mit Art. 25 Abs. 2 dieser Richtlinie bedeutet deren Art. 25 Abs. 6, dass die Kommission bei der Feststellung, dass ein Drittland ein angemessenes Schutzniveau gewährleistet, eine Gesamtbewertung der in diesem Drittland geltenden Rechtsvorschriften und ihrer Anwendung vornehmen muss.

151. Wir haben gesehen, dass die Beibehaltung der Entscheidung 2000/520 durch die Kommission trotz des Eintritts neuer tatsächlicher und rechtlicher Umstände als bewusste Bestätigung ihrer ursprünglichen Bewertung zu verstehen ist.

152. Im Rahmen eines Vorabentscheidungsersuchens ist es nicht Aufgabe des Gerichtshofs, über den dem Rechtsstreit zugrunde liegenden Sachverhalt zu entscheiden, der das nationale Gericht zu diesem Ersuchen veranlasst hat [57].

153. Ich werde mich daher auf den vom vorlegenden Gericht in seinem Vorabentscheidungsersuchen angegebenen Sachverhalt stützen, den die Kommission im Übrigen selbst in weiten Teilen als feststehend anerkennt [58].

154. Die vor dem Gerichtshof erhobenen Einwände gegen die Bewertung der Kommission, wonach die Safe-Harbor-Regelung ein angemessenes Schutzniveau für die aus der Union in die Vereinigten Staaten übermittelten personenbezogenen Daten gewährleiste, lassen sich wie folgt beschreiben.

155. In seinem Vorabentscheidungsersuchen geht das vorlegende Gericht von zwei Tatsachenfeststellungen aus. Zum einen könne auf personenbezogene Daten, die Unternehmen wie Facebook Ireland ihrer Muttergesellschaft mit Sitz in den Vereinigten Staaten übermittelten, anschließend von der NSA und anderen amerikanischen Sicherheitsbehörden im Rahmen einer massenhaften und ungezielten Überwachungs- und Erfassungstätigkeit zugegriffen werden. Infolge der Enthüllungen von Herrn Snowden ließen die verfügbaren Beweise nämlich gegenwärtig keine andere plausible Schlussfolgerung zu [59]. Zum anderen hätten die Unionsbürger keinen wirksamen Anspruch auf rechtliches Gehör zur Frage der Überwachung und Erfassung ihrer Daten durch die NSA und andere amerikanische Sicherheitsbehörden [60].

156. Diese Tatsachenfeststellungen des High Court werden durch die von der Kommission selbst getroffenen Feststellungen untermauert.

157. So ist die Kommission in ihrer oben genannten Mitteilung über die Funktionsweise der Safe-Harbor-Regelung aus Sicht der EU-Bürger und der in der EU niedergelassenen Unternehmen von der Feststellung ausgegangen, dass die Informationen über Umfang und Reichweite der amerikanischen Überwachungsprogramme, die im Lauf des Jahres 2013 bekannt geworden seien, Zweifel an der Kontinuität des Schutzes der auf der Grundlage der Safe-Harbor-Regelung rechtmäßig in die Vereinigten Staaten übermittelten personenbezogenen Daten geweckt hätten. Alle Unternehmen, die

57 — Vgl. u. a. Urteil Fallimento Traghetti del Mediterraneo (C-140/09, EU:C:2010:335, Rn. 22 und die dort angeführte Rechtsprechung).

58 — Vgl. die in Fn. 2 erwähnte Mitteilung der Kommission und die Mitteilung der Kommission an das Europäische Parlament und den Rat über die Funktionsweise der Safe-Harbor-Regelung aus Sicht der EU-Bürger und der in der EU niedergelassenen Unternehmen (COM[2013] 847 final).

59 — Rn. 7 Buchst. c der Vorlageentscheidung.

60 — Rn. 7 Buchst. b der Vorlageentscheidung.

am Programm PRISM beteiligt seien und den amerikanischen Behörden den Zugriff auf in den Vereinigten Staaten gespeicherte und verarbeitete Daten gestatteten, seien der Safe-Harbor-Regelung beigetreten. Safe Harbor sei auf diese Weise zu einem Informationskanal geworden, über den die amerikanischen Nachrichtendienste auf personenbezogene Daten zugreifen könnten, die ursprünglich innerhalb der Union verarbeitet worden seien [61].

158. Daraus ergibt sich, dass das Recht und die Praxis der Vereinigten Staaten eine massenhafte Erhebung der im Rahmen der Safe-Harbor-Regelung übermittelten personenbezogenen Daten von Unionsbürgern zulassen, ohne dass diese in den Genuss eines effektiven gerichtlichen Rechtsschutzes kommen.

159. Diese Tatsachenfeststellungen zeigen nach meinem Dafürhalten, dass die Entscheidung 2000/520 keine hinreichenden Garantien enthält. Aufgrund dieses Mangels an Garantien ist die Entscheidung auf eine Weise durchgeführt worden, die den Erfordernissen der Charta und der Richtlinie 95/46 nicht genügt.

160. Eine von der Kommission auf der Grundlage von Art. 25 Abs. 6 der Richtlinie 95/46 erlassene Entscheidung hat jedoch die Feststellung zum Gegenstand, dass ein Drittland ein angemessenes Schutzniveau „gewährleistet“. Der im Präsens konjugierte Begriff „gewährleistet“ impliziert, dass eine solche Entscheidung, um aufrechterhalten werden zu können, ein Drittland betreffen muss, das nach ihrem Erlass weiterhin ein angemessenes Schutzniveau garantiert.

161. In Wirklichkeit haben die besagten Enthüllungen über die Handlungen der NSA, die im Rahmen der Safe-Harbor-Regelung übermittelte Daten verwendet haben soll, die Schwächen der durch die Entscheidung 2000/520 gebildeten Rechtsgrundlage offenbart.

162. Die im Rahmen des vorliegenden Verfahrens aufgezeigten Schwächen finden sich insbesondere in Anhang I Abs. 4 dieser Entscheidung.

163. Dort heißt es: „Die Geltung [der] Grundsätze [des sicheren Hafens] kann begrenzt werden a) insoweit, als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss, b) durch Gesetzesrecht, staatliche Regulierungsvorschriften oder Fallrecht, die unvereinbare Verpflichtungen oder ausdrückliche Ermächtigungen schaffen, vorausgesetzt, die Organisation kann in Wahrnehmung dieser Ermächtigungen nachweisen, dass die Nichteinhaltung der Grundsätze sich auf das Ausmaß beschränkte, das die Einhaltung übergeordneter berechtigter Interessen aufgrund eben dieser Ermächtigung erforderte …“

164. Das Problem ist hauptsächlich darauf zurückzuführen, wie die amerikanischen Behörden von den in der genannten Vorschrift vorgesehenen Ausnahmen Gebrauch machen. Aufgrund ihrer zu allgemeinen Formulierung beschränkt sich die Umsetzung dieser Ausnahmen durch die erwähnten Behörden nicht auf das unbedingt erforderliche Maß.

165. Zu dieser zu allgemeinen Formulierung kommt hinzu, dass die Unionsbürger über keinen geeigneten Rechtsbehelf verfügen, um dagegen vorzugehen, dass ihre personenbezogenen Daten zu anderen Zwecken als denen verarbeitet werden, für die sie ursprünglich erhoben und anschließend in die Vereinigten Staaten übermittelt wurden.

61 — S. 18 ihrer Mitteilung.

166. Die in der Entscheidung 2000/520, insbesondere aufgrund von Erfordernissen der nationalen Sicherheit, vorgesehenen Ausnahmen von der Anwendung der Grundsätze des sicheren Hafens hätten mit der Einführung eines zur Vermeidung der festgestellten Verstöße gegen das Recht auf Privatsphäre geeigneten unabhängigen Kontrollmechanismus einhergehen müssen.

167. Daher haben die Enthüllungen über die Praktiken der amerikanischen Nachrichtendienste in Bezug auf die pauschale Überwachung der im Rahmen der Safe-Harbor-Regelung übermittelten Daten einige Schwächen der Entscheidung 2000/520 offenbart.

168. Aus dem im Rahmen der vorliegenden Rechtssache angeführten Vorbringen ergibt sich kein Verstoß von Facebook gegen die Grundsätze des sicheren Hafens. Gewährt ein zertifiziertes Unternehmen wie Facebook USA den amerikanischen Behörden Zugang zu Daten, die ihm aus einem Mitgliedstaat übermittelt wurden, ist davon auszugehen, dass es dies tut, um die amerikanischen Rechtsvorschriften einzuhalten. Da die Entscheidung 2000/520 dies aufgrund der weiten Formulierung der in ihr enthaltenen Ausnahmen ausdrücklich zulässt, wird im Rahmen der vorliegenden Rechtssache in Wirklichkeit die Frage nach der Vereinbarkeit solcher Ausnahmen mit dem Primärrecht der Union aufgeworfen.

169. Aus einer ständigen Rechtsprechung des Gerichtshofs geht insoweit hervor, dass die Achtung der Menschenrechte eine Voraussetzung für die Rechtmäßigkeit der Handlungen der Union ist und dass Maßnahmen, die mit ihrer Achtung unvereinbar sind, in der Union nicht als rechtens anerkannt werden können [62].

170. Aus der Rechtsprechung des Gerichtshofs ergibt sich überdies, dass die Weitergabe personenbezogener Daten an – öffentliche oder private – Dritte „unabhängig von der späteren Verwendung der übermittelten Informationen“ einen Eingriff in das Recht auf Achtung des Privatlebens darstellt [63]. In seinem Urteil Digital Rights Ireland u. a. [64] hat der Gerichtshof darüber hinaus bestätigt, dass die Gestattung des Zugriffs der zuständigen nationalen Behörden auf solche Daten eine zusätzliche Beeinträchtigung dieses Grundrechts darstellt [65]. Außerdem wird jede Form der Verarbeitung personenbezogener Daten von Art. 8 der Charta erfasst und stellt einen Eingriff in das Recht auf den Schutz solcher Daten dar [66]. Auch der Zugang der amerikanischen Nachrichtendienste zu den übermittelten Daten greift daher in das durch Art. 8 der Charta garantierte Grundrecht auf den Schutz personenbezogener Daten ein, da ein solcher Zugang eine Verarbeitung dieser Daten darstellt.

171. Wie der Gerichtshof in dem genannten Urteil festgestellt hat, ist ein solcher Eingriff in Anbetracht der erheblichen Zahl betroffener Nutzer und der Mengen übermittelter Daten von großem Ausmaß und als besonders schwerwiegend anzusehen. Aufgrund dieser Gesichtspunkte, verbunden mit dem geheimen Charakter des Zugriffs auf die an Unternehmen mit Sitz in den Vereinigten Staaten übermittelten personenbezogenen Daten durch die amerikanischen Behörden, ist der Eingriff äußerst gravierend.

172. Hinzu kommt, dass Unionsbürger, die Facebook nutzen, nicht darüber unterrichtet werden, dass ihre personenbezogenen Daten für die amerikanischen Sicherheitsbehörden allgemein zugänglich sein werden.

62 — Vgl. u. a. Urteil Kadi und Al Barakaat International Foundation/Rat und Kommission (C-402/05 P und C-415/05 P, EU:C:2008:461, Rn. 284 und die dort angeführte Rechtsprechung).

63 — Urteil Österreichischer Rundfunk u. a. (C-465/00, C-138/01 und C-139/01, EU:C:2003:294, Rn. 74).

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

65 — Rn. 35.

66 — Rn. 36.

173. Außerdem ist hervorzuheben, dass die Unionsbürger nach den Feststellungen des vorlegenden Gerichts in den Vereinigten Staaten keinen wirksamen Anspruch auf rechtliches Gehör zur Frage der Überwachung und Erfassung ihrer Daten haben. Es gebe zwar eine Aufsicht durch den FISC, doch finde das Verfahren vor ihm unter Geheimhaltung und *ex parte* statt[67]. Meines Erachtens handelt es sich hierbei um einen Eingriff in das durch Art. 47 der Charta geschützte Recht der Unionsbürger auf einen wirksamen Rechtsbehelf.

174. Der Eingriff in die durch die Art. 7, 8 und 47 der Charta geschützten Grundrechte, den die Ausnahmen von den Grundsätzen des sicheren Hafens in Anhang I Abs. 4 der Entscheidung 2000/520 erlauben, ist somit dargetan.

175. Nunmehr ist zu prüfen, ob dieser Eingriff gerechtfertigt ist oder nicht.

176. Nach Art. 52 Abs. 1 der Charta muss jede Einschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten gesetzlich vorgesehen sein und ihren Wesensgehalt achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen dieser Rechte und Freiheiten nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

177. In Anbetracht dieser Voraussetzungen für die Zulässigkeit von Einschränkungen der Ausübung der durch die Charta geschützten Rechte und Freiheiten zweifle ich stark daran, dass von den in der vorliegenden Rechtssache in Rede stehenden Einschränkungen angenommen werden kann, dass sie den Wesensgehalt der Art. 7 und 8 der Charta achten. Der Zugang der amerikanischen Nachrichtendienste zu den übermittelten Daten erstreckt sich nämlich offenbar auf den Inhalt der elektronischen Kommunikation, was in den Wesensgehalt des Grundrechts auf Achtung des Privatlebens und der übrigen in Art. 7 der Charta verankerten Rechte eingreifen würde. Da die weite Formulierung der in Anhang I Abs. 4 der Entscheidung 2000/520 vorgesehenen Einschränkungen es zudem potenziell erlaubt, die Anwendung sämtlicher Grundsätze des sicheren Hafens auszuschließen, könnte davon ausgegangen werden, dass diese Einschränkungen in den Wesensgehalt des Grundrechts auf den Schutz personenbezogener Daten eingreifen[68].

178. Hinsichtlich der Frage, ob der festgestellte Eingriff einer dem Gemeinwohl dienenden Zielsetzung entspricht, erinnere ich zunächst daran, dass die Geltung der Grundsätze des sicheren Hafens nach dem Wortlaut von Anhang I Abs. 4 Buchst. b der Entscheidung 2000/520 begrenzt werden kann „durch Gesetzesrecht, staatliche Regulierungsvorschriften oder Fallrecht, die unvereinbare Verpflichtungen oder ausdrückliche Ermächtigungen schaffen, vorausgesetzt, die Organisation kann in Wahrnehmung dieser Ermächtigungen nachweisen, dass die Nichteinhaltung der Grundsätze sich auf das Ausmaß beschränkte, das die Einhaltung übergeordneter berechtigter Interessen aufgrund eben dieser Ermächtigung erforderte“.

179. Festzustellen ist, dass die „berechtigten Interessen“, von denen in dieser Vorschrift die Rede ist, nicht präzisiert werden. Daraus ergibt sich eine Unsicherheit hinsichtlich des, potenziell äußerst weiten, Anwendungsbereichs dieser Ausnahme von der Anwendung der Grundsätze des sicheren Hafens durch die beigetretenen Unternehmen.

180. Die Erläuterungen in Anhang IV Teil B („Ausdrückliche rechtliche Ermächtigungen“) der Entscheidung 2000/520 bestätigen diesen Eindruck, insbesondere die Angabe, dass es „eindeutig fest[steht], dass, wenn aufgrund des US-amerikanischen Rechts eine den Grundsätzen des sicheren Hafens entgegenstehende Verpflichtung auferlegt wird, die US-Unternehmen die Gesetze einhalten

67 — Rn. 7 Buchst. b der Vorlageentscheidung.

68 — Vgl. insoweit Urteil Digital Rights Ireland u. a. (C-293/12 und C-594/12, EU:C:2014:238, Rn. 39 und 40).

müssen, und zwar ungeachtet dessen, ob sie auf die Grundsätze des sicheren Hafens verpflichtet sind oder nicht“. In Bezug auf ausdrückliche Ermächtigungen heißt es dort weiter: „Während die Grundsätze des sicheren Hafens darauf abzielen, die Unterschiede zwischen dem US-amerikanischen und den europäischen Rechtssystemen für den Schutz der Privatsphäre zu überbrücken, haben wir uns … den Vorrechten unserer gewählten Gesetzgeber zu fügen.“

181. Meiner Meinung nach ergibt sich daraus, dass diese Ausnahme gegen die Art. 7, 8 und 52 Abs. 1 der Charta verstößt, da mit ihr keine hinreichend genau bestimmte dem Gemeinwohl dienende Zielsetzung verfolgt wird.

182. Die Leichtigkeit und die Allgemeinheit des in der Entscheidung 2000/520 selbst, in ihren Anhängen I Abs. 4 Buchst. b und IV Teil B, vorgesehenen Ausschlusses der Grundsätze des sicheren Hafens in Anwendung amerikanischer Rechtsnormen sind jedenfalls mit der Voraussetzung unvereinbar, wonach Ausnahmen von den Vorschriften über den Schutz personenbezogener Daten auf das unbedingt erforderliche Maß begrenzt sein müssen. Zwar wird die Voraussetzung der Erforderlichkeit erwähnt; abgesehen davon, dass die Beweislast für ihr Vorliegen dem betreffenden Unternehmen auferlegt wird, ist jedoch nicht ersichtlich, wie sich ein solches Unternehmen einer Verpflichtung, von den Grundsätzen des sicheren Hafens abzuweichen, entziehen könnte, die sich aus von ihm zu befolgenden Rechtsvorschriften ergibt.

183. Meines Erachtens ist die Entscheidung 2000/520 daher für ungültig zu erklären, da das Bestehen einer Ausnahmeregelung, die es in ebenso allgemeiner wie ungenauer Weise erlaubt, von den Grundsätzen des sicheren Hafens abzuweichen, für sich allein der Annahme entgegensteht, dass diese Regelung ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, die aus der Union in die Vereinigten Staaten übermittelt werden.

184. Was die erste Kategorie der in Anhang I Abs. 4 Buchst. a der Entscheidung 2000/520 vorgesehenen Grenzen aufgrund von Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung amerikanischer Gesetze angeht, scheint mir nur das erste Ziel hinreichend genau zu sein, um als eine von der Union anerkannte dem Gemeinwohl dienende Zielsetzung im Sinne von Art. 52 Abs. 1 der Charta angesehen werden zu können.

185. Nunmehr ist die Verhältnismäßigkeit des festgestellten Eingriffs zu prüfen.

186. Insoweit ist darauf hinzuweisen, dass „der Grundsatz der Verhältnismäßigkeit nach ständiger Rechtsprechung des Gerichtshofs verlangt, dass die Handlungen der Unionsorgane geeignet sind, die mit der fraglichen Regelung zulässigerweise verfolgten Ziele zu erreichen, und nicht die Grenzen dessen überschreiten, was zur Erreichung dieser Ziele geeignet und erforderlich ist“ [69].

187. Was die gerichtliche Überprüfung der Einhaltung dieser Voraussetzungen anbelangt, „kann, da Grundrechtseingriffe in Rede stehen, der Gestaltungsspielraum des Unionsgesetzgebers anhand einer Reihe von Gesichtspunkten eingeschränkt sein; zu ihnen gehören u. a. der betroffene Bereich, das Wesen des fraglichen durch die Charta gewährleisteten Rechts, Art und Schwere des Eingriffs sowie dessen Zweck“ [70].

188. Meiner Meinung nach unterliegen Entscheidungen, die die Kommission auf der Grundlage von Art. 25 Abs. 6 der Richtlinie 95/46 erlässt, hinsichtlich der Verhältnismäßigkeit der von ihr vorgenommenen Beurteilung der Angemessenheit des Schutzniveaus, das ein Drittland aufgrund „seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen“ bietet, der vollen Kontrolle durch den Gerichtshof.

69 — Urteil Digital Rights Ireland u. a. (C-293/12 und C-594/12, EU:C:2014:238, Rn. 46 und die dort angeführte Rechtsprechung).

70 — Ebd. (Rn. 47 und die dort angeführte Rechtsprechung).

189. Insoweit hat der Gerichtshof in seinem Urteil Digital Rights Ireland u. a.[71] entschieden, dass „angesichts der besonderen Bedeutung des Schutzes personenbezogener Daten für das Grundrecht auf Achtung des Privatlebens und des Ausmaßes und der Schwere des mit der [fraglichen] Richtlinie … verbundenen Eingriffs in dieses Recht der Gestaltungsspielraum des Unionsgesetzgebers eingeschränkt [ist], so dass die Richtlinie einer strikten Kontrolle unterliegt“[72].

190. Ein solcher Eingriff muss geeignet sein, das mit dem fraglichen Unionsrechtsakt verfolgte Ziel zu erreichen, und zur Verwirklichung dieses Ziels erforderlich sein.

191. Insoweit verlangt „[d]er Schutz des Grundrechts auf Achtung des Privatlebens … nach ständiger Rechtsprechung des Gerichtshofs …, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken müssen“[73].

192. Bei seiner Kontrolle berücksichtigt der Gerichtshof auch den Umstand, dass „der Schutz personenbezogener Daten, zu dem Art. 8 Abs. 1 der Charta ausdrücklich verpflichtet, für das in ihrem Art. 7 verankerte Recht auf Achtung des Privatlebens von besonderer Bedeutung ist“[74].

193. Nach Auffassung des Gerichtshofs, der sich insoweit auf die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte bezieht, „muss die fragliche Unionsregelung klare und präzise Regeln für die Tragweite und die Anwendung der fraglichen Maßnahme vorsehen und Mindestanforderungen aufstellen, so dass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen“[75]. Der Gerichtshof führt aus, dass „[d]as Erfordernis, über solche Garantien zu verfügen, … umso bedeutsamer [ist], wenn die personenbezogenen Daten … automatisch verarbeitet werden und eine erhebliche Gefahr des unberechtigten Zugangs zu diesen Daten besteht“[76].

194. Meines Erachtens besteht eine Analogie zwischen Anhang I Abs. 4 Buchst. a der Entscheidung 2000/520 und Art. 13 Abs. 1 der Richtlinie 95/46. In der erstgenannten Vorschrift heißt es, dass die Geltung der Grundsätze des sicheren Hafens insoweit begrenzt werden kann, „als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss“. Nach der letztgenannten Vorschrift können die Mitgliedstaaten Rechtsvorschriften erlassen, die die Pflichten und Rechte gemäß den Art. 6 Abs. 1, 10, 11 Abs. 1, 12 und 21 der Richtlinie beschränken, sofern eine solche Beschränkung u. a. für die Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten notwendig ist.

195. Wie der Gerichtshof in seinem Urteil IPI[77] ausgeführt hat, geht aus dem Wortlaut von Art. 13 Abs. 1 der Richtlinie 95/46 hervor, dass die Mitgliedstaaten die in dieser Vorschrift genannten Maßnahmen nur vorsehen können, wenn sie notwendig sind. Die „Notwendigkeit“ der Maßnahmen ist somit Voraussetzung für die den Mitgliedstaaten in der genannten Vorschrift eingeräumte Wahlmöglichkeit[78]. Für Verarbeitungen personenbezogener Daten innerhalb der Union sind die in

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

72 — Rn. 48.

73 — Urteil Digital Rights Ireland u. a. (C-293/12 und C-594/12, EU:C:2014:238, Rn. 52 und die dort angeführte Rechtsprechung).

74 — Ebd. (Rn. 53).

75 — Ebd. (Rn. 54 und die dort angeführte Rechtsprechung).

76 — Ebd. (Rn. 55 und die dort angeführte Rechtsprechung).

77 — C-473/12, EU:C:2013:715.

78 — Rn. 32.

Art. 13 der Richtlinie vorgesehenen Grenzen so zu verstehen, dass sie auf das für die Erreichung des verfolgten Ziels unbedingt erforderliche Maß beschränkt sind. Das Gleiche muss meines Erachtens für die in Anhang I Abs. 4 der Entscheidung 2000/520 vorgesehenen Grenzen der Grundsätze des sicheren Hafens gelten.

196. Allerdings wird nicht in allen Sprachfassungen von Anhang I Abs. 4 Buchst. a der Entscheidung 2000/520 das Kriterium der Erforderlichkeit erwähnt. Dies gilt u. a. für die französische Sprachfassung („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"), während es z. B. in der spanischen, der deutschen und der englischen Sprachfassung heißt, dass die eingeführten Beschränkungen zur Erreichung der vorerwähnten Ziele erforderlich sein müssen.

197. Dessen ungeachtet zeigen die vom vorlegenden Gericht sowie von der Kommission in ihren oben genannten Mitteilungen angeführten tatsächlichen Umstände eindeutig, dass die Einführung dieser Beschränkungen in der Praxis nicht auf das zur Erreichung der angestrebten Ziele unbedingt erforderliche Maß beschränkt ist.

198. Insoweit ist darauf hinzuweisen, dass sich der Zugang zu den übermittelten personenbezogenen Daten, über den die amerikanischen Nachrichtendienste verfügen, generell auf alle Personen und alle elektronischen Kommunikationsmittel sowie auf sämtliche übermittelten Daten einschließlich des Inhalts der Kommunikation erstreckt, ohne jede Differenzierung, Beschränkung oder Ausnahme anhand des verfolgten dem Gemeinwohl dienenden Ziels [79].

199. Der Zugang der amerikanischen Nachrichtendienste zu den übermittelten Daten betrifft nämlich umfassend alle Personen, die elektronische Kommunikationsdienste nutzen, ohne dass verlangt wird, dass die betreffenden Personen eine Bedrohung für die nationale Sicherheit darstellen [80].

200. Eine solche massenhafte und ungezielte Überwachung ist naturgemäß unverhältnismäßig und stellt einen ungerechtfertigten Eingriff in die durch die Art. 7 und 8 der Charta garantierten Rechte dar.

201. Da weder der Unionsgesetzgeber noch die Mitgliedstaaten Rechtsvorschriften erlassen dürfen, die unter Verstoß gegen die Charta eine massenhafte und ungezielte Überwachung vorsehen, folgt daraus, wie das Parlament in seinen Erklärungen zu Recht festgestellt hat, notwendigerweise, dass bei Drittländern, deren Rechtsvorschriften tatsächlich eine massenhafte und ungezielte Überwachung und Erfassung personenbezogener Daten der Unionsbürger erlauben, erst recht nicht davon ausgegangen werden kann, dass sie ein angemessenes Schutzniveau für derartige Daten gewährleisten.

202. Darüber hinaus ist hervorzuheben, dass die Safe-Harbor-Regelung, so wie sie in der Entscheidung 2000/520 definiert wird, keine geeigneten Garantien zur Verhinderung eines massenhaften und pauschalen Zugriffs auf die übermittelten Daten enthält.

203. Der Gerichtshof hat in seinem Urteil Digital Rights Ireland u. a. [81] insoweit auf die Bedeutung „klare[r] und präzise[r] Regeln zur Tragweite des Eingriffs in die in Art. 7 und Art. 8 der Charta verankerten Grundrechte" hingewiesen [82]. Eine solche Regelung müsse „Bestimmungen [enthalten], die zu gewährleisten vermögen, dass sich der Eingriff tatsächlich auf das absolut Notwendige beschränkt" [83].

79 — Vgl. entsprechend Urteil Digital Rights Ireland u. a. (C-293/12 und C-594/12, EU:C:2014:238, Rn. 57 und die dort angeführte Rechtsprechung).

80 — Ebd. (Rn. 58 und 59).

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

82 — Rn. 65.

83 — Ebd.

Er hat in diesem Urteil darüber hinaus die Notwendigkeit „hinreichende[r], den Anforderungen von Art. 8 der Charta entsprechende[r] Garantien dafür, dass die [personenbezogenen] Daten wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu ihnen und jeder unberechtigten Nutzung geschützt sind“, hervorgehoben [84].

204. Die privaten Schlichtungsmechanismen und die FTC stellen aber aufgrund ihrer auf handelsrechtliche Streitigkeiten beschränkten Rolle keine Mittel dar, um gegen den Zugriff der amerikanischen Nachrichtendienste auf personenbezogene Daten vorzugehen, die aus der Union übermittelt werden.

205. Die Zuständigkeit der FTC umfasst unlautere und irreführende Geschäftspraktiken und erstreckt sich daher nicht auf die Erhebung und Nutzung personenbezogener Daten für nichtgewerbliche Zwecke [85]. Der begrenzte Zuständigkeitsbereich der FTC schränkt das Recht von Privatpersonen auf den Schutz ihrer personenbezogenen Daten ein. Die FTC ist nicht errichtet worden, um, wie es innerhalb der Union bei den nationalen Kontrollstellen der Fall ist, den Schutz des individuellen Rechts auf Achtung der Privatsphäre zu gewährleisten, sondern um für die Verbraucher einen fairen und zuverlässigen Handel zu garantieren, was ihre Einwirkungsbefugnisse auf dem Gebiet des Schutzes personenbezogener Daten *de facto* einschränkt. Die FTC spielt daher keine den in Art. 28 der Richtlinie 95/46 vorgesehenen nationalen Kontrollstellen vergleichbare Rolle.

206. Unionsbürger, deren Daten übermittelt wurden, können sich zur Klärung der Frage, ob das im Besitz ihrer personenbezogenen Daten befindliche Unternehmen gegen die Bedingungen der Selbstzertifizierungsregelung verstößt, an spezialisierte Schiedseinrichtungen mit Sitz in den Vereinigten Staaten wie TRUSTe und BBBOnline wenden. Die private Schiedsgerichtsbarkeit, die von Einrichtungen wie TRUSTe ausgeübt wird, kann sich nicht mit Verstößen anderer Einrichtungen oder Behörden als der selbstzertifizierten Unternehmen gegen das Recht auf den Schutz personenbezogener Daten befassen. Die Schiedseinrichtungen haben keinerlei Zuständigkeit für Entscheidungen über die Rechtmäßigkeit von Handlungen der amerikanischen Sicherheitsbehörden.

207. Weder die FTC noch die privaten Schiedseinrichtungen sind daher zur Kontrolle möglicher Verstöße öffentlicher Akteure wie der amerikanischen Sicherheitsbehörden gegen die Grundsätze für den Schutz personenbezogener Daten befugt. Eine solche Befugnis wäre jedoch unerlässlich, um das Recht auf einen effektiven Schutz dieser Daten in vollem Umfang zu gewährleisten. Die Kommission durfte daher beim Erlass der Entscheidung 2000/520 und bei deren Aufrechterhaltung nicht feststellen, dass es für sämtliche in die Vereinigten Staaten übermittelten personenbezogenen Daten einen angemessenen Schutz des durch Art. 8 Abs. 3 der Charta gewährten Rechts gebe, d. h., dass eine unabhängige Stelle eine wirksame Kontrolle über die Einhaltung der Anforderungen in Bezug auf den Schutz und die Sicherheit dieser Daten ausübe.

208. Folglich ist festzustellen, dass es im Rahmen der in der Entscheidung 2000/520 vorgesehenen Safe-Harbor-Regelung keine unabhängige Stelle gibt, die überwachen könnte, dass sich die Umsetzung der Ausnahmen von den Grundsätzen des sicheren Hafens auf das unbedingt erforderliche Maß beschränkt. Wie wir gesehen haben, ist eine solche Überwachung durch eine unabhängige Stelle aus unionsrechtlicher Sicht aber ein wesentlicher Bestandteil der Wahrung des Schutzes der Betroffenen bei der Verarbeitung personenbezogener Daten [86].

209. In diesem Zusammenhang ist die Rolle hervorzuheben, die den nationalen Kontrollstellen in dem innerhalb der Union bestehenden System zum Schutz personenbezogener Daten bei der Überwachung der in Art. 13 der Richtlinie 95/46 vorgesehenen Beschränkungen zukommt. Nach dem Wortlaut von Art. 28 Abs. 4 Unterabs. 2 dieser Richtlinie kann „[j]ede Kontrollstelle … insbesondere von jeder

84 — Ebd. (Rn. 66).

85 — Vgl. hierzu Anhang II, FAQ 11, der Entscheidung 2000/520 unter „Befassung der FTC“ sowie ihre Anhänge III, V und VII.

86 — Vgl. Urteil Digital Rights Ireland u. a. (C-293/12 und C-594/12, EU:C:2014:238, Rn. 68 und die dort angeführte Rechtsprechung).

Person mit dem Antrag befasst werden, die Rechtmäßigkeit einer Verarbeitung zu überprüfen, wenn einzelstaatliche Vorschriften gemäß Artikel 13 Anwendung finden“. Entsprechend hätte der Hinweis auf Grenzen für die Anwendung der Grundsätze des sicheren Hafens in Anhang I Abs. 4 der Entscheidung 2000/520 nach meinem Dafürhalten mit der Schaffung eines durch eine unabhängige, auf den Bereich des Schutzes personenbezogener Daten spezialisierte Stelle gewährleisteten Kontrollmechanismus einhergehen müssen.

210. Die Intervention unabhängiger Kontrollstellen ist nämlich das Herzstück des europäischen Systems zum Schutz personenbezogener Daten. Die Existenz solcher Stellen wurde daher naturgemäß von vornherein als eine der notwendigen Voraussetzungen für die Feststellung der Angemessenheit des von Drittländern gebotenen Schutzniveaus angesehen. Hierbei handelt es sich um eine Voraussetzung dafür, dass Datenübermittlungen aus dem Hoheitsgebiet der Mitgliedstaaten in das Hoheitsgebiet von Drittländern nicht nach Art. 25 der Richtlinie 95/46 untersagt werden [87]. Wie es in dem Diskussionspapier der durch Art. 29 der Richtlinie eingesetzten Arbeitsgruppe heißt, besteht in Europa ein breiter Konsens über die „Notwendigkeit der ‚externen Kontrolle‘ in Form einer unabhängigen Stelle, die Teil eines Systems zur Einhaltung des Datenschutzes ist“ [88].

211. Ferner ist festzustellen, dass der FISC Unionsbürgern, deren personenbezogene Daten in die Vereinigten Staaten übermittelt werden, keinen effektiven gerichtlichen Rechtsschutz bietet. Die Schutzmechanismen gegen die Überwachung durch Regierungsstellen im Rahmen von Section 702 des Foreign Intelligence Surveillance Act of 1978 gelten nämlich nur für Bürger der Vereinigten Staaten und für ausländische Bürger, die rechtmäßig und dauerhaft in den Vereinigten Staaten ansässig sind. Wie die Kommission selbst festgestellt hat, ließe sich die Aufsicht über die amerikanischen Datenerhebungsprogramme durch eine Stärkung der Rolle des FISC sowie durch die Einführung von Rechtsmitteln für natürliche Personen verbessern. Mit diesen Mechanismen könnte die Verarbeitung für nationale Sicherheitsbelange unbedeutender personenbezogener Daten von Unionsbürgern eingeschränkt werden [89].

212. Darüber hinaus hat die Kommission selbst ausgeführt, dass die Unionsbürger keine Möglichkeit haben, Auskunft über ihre im Rahmen der amerikanischen Überwachungsprogramme erhobenen und weiterverarbeiteten Daten sowie deren Berichtigung oder Löschung zu erwirken und dass auch keine administrativen oder gerichtlichen Rechtsbehelfe zur Verfügung stehen [90].

213. Schließlich ist zu erwähnen, dass bei der Anwendung der amerikanischen Vorschriften über den Schutz des Privatlebens zwischen Bürgern der Vereinigten Staaten und ausländischen Bürgern differenziert werden kann [91].

214. Aus dem Vorstehenden folgt, dass die Entscheidung 2000/520 keine klaren und präzisen Regeln zur Tragweite des Eingriffs in die Grundrechte vorsieht, die in den Art. 7 und 8 der Charta verankert sind. Somit ist festzustellen, dass diese Entscheidung und ihre Anwendung einen weitreichenden und besonders gravierenden Eingriff in diese Grundrechte darstellen, ohne dass ein solcher Eingriff durch Bestimmungen eingegrenzt würde, die zu gewährleisten vermögen, dass er sich tatsächlich auf das absolut Notwendige beschränkt.

87 — Vgl. Poullet, Y., „L’autorité de contrôle: ‚vues‘ de Bruxelles“, *Revue française d’administration publique*, Nr. 89, Januar-März 1999, S. 69, speziell S. 71.

88 — Vgl. S. 7 der in Fn. 56 erwähnten Arbeitsunterlage WP 12 der Kommission.

89 — S. 10 der in Fn. 2 angeführten Mitteilung der Kommission.

90 — Abschnitt 7.2, S. 19, der in Fn. 58 angeführten Mitteilung der Kommission.

91 — Vgl. zu dieser Frage Kuner, C., „Foreign Nationals and Data Protection Law: A Transatlantic Analysis“, *Data Protection Anno 2014: How To Restore Trust*? Intersentia, Cambridge, 2014, S. 213, speziell S. 216 und 217.

215. Mit dem Erlass der Entscheidung 2000/520 und ihrer anschließenden Aufrechterhaltung hat die Kommission daher die durch die Wahrung des Grundsatzes der Verhältnismäßigkeit im Hinblick auf die Art. 7, 8 und 52 Abs. 1 der Charta gebotenen Grenzen überschritten. Hinzu kommt die Feststellung eines ungerechtfertigten Eingriffs in das durch Art. 47 der Charta geschützte Recht der Unionsbürger auf einen wirksamen Rechtsbehelf.

216. Diese Entscheidung ist infolgedessen für ungültig zu erklären, da aufgrund der vorstehend beschriebenen Grundrechtsverstöße nicht davon ausgegangen werden kann, dass die mit ihr eingeführte Safe-Harbor-Regelung ein angemessenes Schutzniveau für die im Rahmen dieser Regelung aus der Union in die Vereinigten Staaten übermittelten personenbezogenen Daten gewährleistet.

217. In Anbetracht der festgestellten Verstöße gegen Grundrechte der Unionsbürger hätte die Kommission die Anwendung der Entscheidung 2000/520 meines Erachtens aussetzen müssen.

218. Diese Entscheidung gilt unbefristet. Die vorliegende Rechtssache zeigt jedoch, dass die Angemessenheit des von einem Drittland gebotenen Schutzniveaus im Lauf der Zeit aufgrund von Änderungen sowohl der tatsächlichen als auch der rechtlichen Umstände, auf denen die Entscheidung beruhte, einer Entwicklung unterliegen kann.

219. Es ist darauf hinzuweisen, dass die Entscheidung 2000/520 selbst Vorschriften enthält, die der Kommission die Möglichkeit geben, sie den Umständen anzupassen.

220. So heißt es im neunten Erwägungsgrund dieser Entscheidung: „Der durch die Grundsätze und die FAQ geschaffene ‚sichere Hafen' wird möglicherweise im Licht der Erfahrungen mit Entwicklungen beim Datenschutz in einem Umfeld, in dem die Technik die Übermittlung und Verarbeitung personenbezogener Daten immer einfacher macht, und im Licht von Berichten der für die Durchsetzung zuständigen Behörden über die Anwendung gegebenenfalls überprüft werden müssen."

221. Weiter heißt es in Art. 3 Abs. 4 der Entscheidung: „Ergeben die Informationen nach den Absätzen 1, 2 und 3, dass eine der für die Einhaltung der entsprechend den FAQ umgesetzten Grundsätze in den Vereinigten Staaten verantwortlichen Einrichtungen ihrer Aufgabe nicht wirkungsvoll nachkommt, so informiert die Kommission das Handelsministerium der USA und schlägt, wenn nötig, … im Hinblick auf eine Aufhebung, Aussetzung oder Beschränkung des Geltungsbereichs dieser Entscheidung entsprechende Maßnahmen vor."

222. Nach Art. 4 Abs. 1 der Entscheidung 2000/520 kann diese darüber hinaus „jederzeit im Licht der Erfahrungen mit ihrer Anwendung angepasst werden und/oder dann, wenn das durch die Grundsätze und die FAQ gewährte Schutzniveau in die Rechtsvorschriften der USA übernommen wird. In jedem Fall nimmt die Kommission drei Jahre, nachdem sie die Mitgliedstaaten von dieser Entscheidung in Kenntnis gesetzt hat, anhand der verfügbaren Informationen eine Bewertung ihrer Umsetzung vor und unterrichtet den nach Artikel 31 der Richtlinie [95/46] eingesetzten Ausschuss über sämtliche relevanten Feststellungen, einschließlich aller Erkenntnisse, die die Beurteilung der Vereinbarung in Artikel 1 als zur Gewährleistung des Datenschutzes angemessen im Sinne von Artikel 25 der Richtlinie [95/46] berühren könnten …" In Art. 4 Abs. 2 der Entscheidung 2000/520 heißt es: „Die Kommission legt erforderlichenfalls gemäß dem Verfahren nach Artikel 31 der Richtlinie Vorschläge für Maßnahmen vor."

223. Die Kommission hat in ihren Erklärungen festgestellt, dass „eine hohe Wahrscheinlichkeit [besteht], dass der Beitritt zu den Grundsätzen des sicheren Hafens auf eine Weise eingeschränkt worden ist, die den eng umschriebenen Bedingungen für die Ausnahme zugunsten der nationalen Sicherheit nicht genügt"[92]. Sie weist insoweit darauf hin, dass „[d]ie fraglichen Enthüllungen … einen

92 — Rn. 44.

Grad an massenhafter und unterschiedsloser Überwachung offenbart [haben], der weder mit dem in dieser Ausnahme vorgesehenen Erforderlichkeitskriterium noch – allgemeiner – mit dem in Art. 8 der Charta verankerten Recht auf den Schutz personenbezogener Daten vereinbar ist“ [93]. Die Kommission hat darüber hinaus selbst festgestellt, dass sich „[a]ngesichts der Reichweite [der] Überwachungsprogramme und der Ungleichbehandlung der [Unionsbürger] … die Frage nach dem Schutzniveau [stellt], das durch die Safe-Harbor-Regelung geboten wird“ [94].

224. Überdies hat die Kommission in der mündlichen Verhandlung ausdrücklich anerkannt, dass die Entscheidung 2000/520, so wie sie gegenwärtig angewandt werde, keine Garantie dafür biete, dass das Recht der Unionsbürger auf den Schutz ihrer Daten gewährleistet werde. Diese Feststellung könne jedoch nicht zur Ungültigkeit der Entscheidung führen. Es sei zwar richtig, dass sie angesichts neuer Umstände handeln müsse, doch habe sie mit der Aufnahme von Verhandlungen mit den Vereinigten Staaten zur Reform der Safe-Harbor-Regelung geeignete und verhältnismäßige Maßnahmen ergriffen.

225. Diese Ansicht teile ich nicht. In der Zwischenzeit müssen Übermittlungen personenbezogener Daten in die Vereinigten Staaten nämlich auf Initiative der nationalen Kontrollstellen oder im Anschluss an bei ihnen eingelegte Beschwerden ausgesetzt werden können.

226. Darüber hinaus hätte die Kommission die Anwendung der Entscheidung 2000/520 angesichts solcher Feststellungen nach meinem Dafürhalten aussetzen müssen. Das mit der Richtlinie 95/46 und mit Art. 8 der Charta verfolgte Ziel des Schutzes personenbezogener Daten erlegt nämlich nicht nur den Mitgliedstaaten Verpflichtungen auf, sondern auch den Unionsorganen, wie sich aus Art. 51 Abs. 1 der Charta ergibt.

227. Bei ihrer Beurteilung des von einem Drittland gebotenen Schutzniveaus muss die Kommission nicht nur die innerstaatlichen Rechtsvorschriften und die internationalen Verpflichtungen dieses Drittlands prüfen, sondern auch die Art und Weise, in der der Schutz personenbezogener Daten in der Praxis gewährleistet wird. Offenbart die Prüfung der Praxis Funktionsstörungen, muss die Kommission reagieren und ihre Entscheidung gegebenenfalls unverzüglich aussetzen und/oder anpassen.

228. Wie sich aus meinen vorstehenden Ausführungen ergibt, besteht die Verpflichtung der Mitgliedstaaten hauptsächlich darin, durch Maßnahmen ihrer nationalen Kontrollstellen die Einhaltung der Bestimmungen der Richtlinie 95/46 zu gewährleisten.

229. Die Verpflichtung der Kommission besteht darin, die Anwendung einer von ihr auf der Grundlage von Art. 25 Abs. 6 dieser Richtlinie erlassenen Entscheidung im Fall erwiesener Verstöße des betreffenden Drittlands auszusetzen, während sie Verhandlungen mit dem Drittland führt, um die Verstöße abzustellen.

230. Wie bereits ausgeführt, hat eine von der Kommission auf der Grundlage der genannten Vorschrift erlassene Entscheidung die Feststellung zum Gegenstand, dass ein Drittland ein angemessenes Schutzniveau für die in dieses Land übermittelten personenbezogenen Daten „gewährleistet“. Der im Präsens konjugierte Begriff „gewährleistet“ impliziert, dass eine solche Entscheidung, um aufrechterhalten werden zu können, ein Drittland betreffen muss, das nach dem Erlass der erwähnten Entscheidung weiterhin ein solches angemessenes Schutzniveau garantiert.

231. Im 57. Erwägungsgrund der Richtlinie 95/46 heißt es: „Bietet … ein Drittland kein angemessenes Schutzniveau, so ist die Übermittlung personenbezogener Daten in dieses Land zu untersagen.“

93 — Ebd.

94 — Vgl. S. 5 der in Fn. 2 angeführten Mitteilung der Kommission.

232. Art. 25 Abs. 4 der Richtlinie 95/46 sieht vor: „Stellt die Kommission nach dem Verfahren des Artikels 31 Absatz 2 fest, dass ein Drittland kein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels aufweist, so treffen die Mitgliedstaaten die erforderlichen Maßnahmen, damit keine gleichartige Datenübermittlung in das Drittland erfolgt.“ Darüber hinaus bestimmt Art. 25 Abs. 5 dieser Richtlinie: „Zum geeigneten Zeitpunkt leitet die Kommission Verhandlungen ein, um Abhilfe für die gemäß Absatz 4 festgestellte Lage zu schaffen.“

233. Aus der letztgenannten Vorschrift ergibt sich, dass die mit einem Drittland aufgenommenen Verhandlungen in dem durch Art. 25 der Richtlinie 95/46 geschaffenen System darauf abzielen, das nach dem Verfahren des Art. 31 Abs. 2 dieser Richtlinie festgestellte Fehlen eines angemessenen Schutzniveaus zu beheben. In dem uns beschäftigenden Fall hat die Kommission nicht im Einklang mit diesem Verfahren förmlich festgestellt, dass die Safe-Harbor-Regelung kein angemessenes Schutzniveau mehr gewährleistete. Wenn sie gleichwohl beschloss, Verhandlungen mit den Vereinigten Staaten aufzunehmen, lag dies gerade an ihrer zuvor gewonnenen Überzeugung, dass das von diesem Drittland gewährleistete Schutzniveau nicht mehr angemessen sei.

234. Trotz ihrer Kenntnis von Funktionsstörungen bei der Anwendung der Entscheidung 2000/520 hat die Kommission diese weder ausgesetzt noch angepasst, was zur Fortsetzung des Verstoßes gegen die Grundrechte der Personen führte, deren personenbezogene Daten im Rahmen der Safe-Harbor-Regelung übermittelt wurden und weiterhin übermittelt werden.

235. Der Gerichtshof hat – wenn auch in anderem Zusammenhang – aber bereits entschieden, dass es der Kommission obliegt, für eine Anpassung der Regelung an die neuen Gegebenheiten zu sorgen [95].

236. Eine solche Untätigkeit der Kommission, die unmittelbar in die durch die Art. 7, 8 und 47 der Charta geschützten Grundrechte eingreift, stellt meines Erachtens einen zusätzlichen Grund dafür dar, die Entscheidung 2000/520 im Rahmen des vorliegenden Vorabentscheidungsersuchens für ungültig zu erklären [96].

III – **Ergebnis**

237. Nach alledem schlage ich dem Gerichtshof vor, die Fragen des High Court wie folgt zu beantworten:

Art. 28 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist im Licht der Art. 7 und 8 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass die Existenz einer von der Europäischen Kommission auf der Grundlage von Art. 25 Abs. 6 der Richtlinie 95/46 erlassenen Entscheidung eine nationale Kontrollstelle nicht daran hindert, eine Beschwerde zu untersuchen, mit der geltend gemacht wird, ein Drittland gewährleiste kein angemessenes Schutzniveau für übermittelte personenbezogene Daten, und die Übermittlung dieser Daten gegebenenfalls auszusetzen.

Die Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ist ungültig.

95 — Vgl. in diesem Sinne Urteil Agrarproduktion Staebelow (C-504/04, EU:C:2006:30, Rn. 40).

96 — Zwar hat der Gerichtshof in seinem Urteil T. Port (C-68/95, EU:C:1996:452) entschieden, dass „der Vertrag … keine Möglichkeit für ein nationales Gericht vor[sieht], den Gerichtshof im Wege der Vorlage zu ersuchen, durch Vorabentscheidung die Untätigkeit eines Organs festzustellen“ (Rn. 53), doch hat er in seinem Urteil Ten Kate Holding Musselkanaal u. a. (C-511/03, EU:C:2005:625, Rn. 29) offenbar eine positivere Haltung zu dieser Möglichkeit eingenommen.