Europäisches Daten- und Persönlichkeitsschutzrecht im Spiegel der Rechtsprechung des EuGHEuropäisches Daten- und Persönlichkeitsschutzrecht **Astrid Epiney**

Astrid Epiney

Dieser Beitrag wurde erstmals wie folgt veröffentlicht:
***Astrid Epiney*, Europäisches Daten- und Persönlichkeitsschutzrecht im Spiegel der Rechtsprechung des EuGH, FS Christoph Vedder, Baden-Baden 2017, 89-111. Es ist möglich, dass die publizierte Version – die allein zitierfähig ist – im Verhältnis zu diesem Manuskript geringfügige Modifikationen enthält.**

I. Einführung

Datenschutzrecht ist durchaus kein neues Thema des Unionsrechts; vielmehr wurde die sog. Datenschutz-Richtlinie (RL 95/46/EG)[1] bereits 1995 erlassen, und auch die Tragweite der hier einschlägigen grundrechtlichen Garantien (Art. 8 EMRK sowie Art. 7, Art. 8 GRC) waren bereits früh Gegenstand auch der Rechtsprechung des EuGH. Nichtsdestotrotz erscheint es nicht übertrieben, davon auszugehen, dass die Frage nach der Reichweite der RL 95/46/EG (die durch die sog. Datenschutz-Grundverordnung – VO (EU) 2016/679[2] – abgelöst werden wird) sowie der Art. 7, Art. 8 GRC in den letzten rund zwei bis drei Jahren auch und gerade aufgrund verschiedener m.E. bedeutender Urteile des EuGH (zu Recht) vermehrt in den Fokus des (auch juristischen) Interesses gerückt ist. Dies sowie der Umstand, dass die grundlegenden Aussagen des Gerichtshofs zur RL 95/46/EG in der Regel auch im Rahmen der Datenschutz-Grundverordnung Bestand haben werden, soll zum Anlass genommen werden, nachfolgend die m.E. wichtigsten jüngeren Urteile des EuGH zur Thematik zusammenzustellen und zu bewerten (II), bevor ein kurzes Fazit (III) gezogen wird. Auf diese Weise soll auch ein gewisser Überblick über die wegweisenden Aussagen des Gerichtshofs und damit die Tragweite der einschlägigen unionsrechtlichen Bestimmungen gegeben werden.

---

[1] RL 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Richtlinie), ABl. 1995 L 281/31.

[2] VO (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. 2016 L 119/1. Zu den mit dieser Verordnung einhergehenden Neuerungen, m.w.N., *Epiney/Kern*, Zu den Neuerungen im Datenschutzrecht der Europäischen Union, in: *Epiney/Nüesch* (Hrsg.), Die Revision des Datenschutzes in Europa und die Schweiz / La révision de la protection des données en Europe et la Suisse, Zürich 2016, 39 ff. S. auch die inzwischen erschienen Kommentare zur VO 2016/679.

II. Zur Entwicklung der jüngeren Rechtsprechung des EuGH im Bereich des Daten- und Persönlichkeitsschutzes

1. Anwendungsbereich der RL 95/46/EG

a) Rs. C-230/14 (Weltimmo)

Um den Anwendungsbereich der RL 95/46/EG und die Kompetenzen der nationalen Kontrollstelle ging es in der Rs. C-230/14.[3] Der Ausgangsfall betraf die Verhängung eines Bußgelds durch die ungarische Kontrollbehörde gegen eine in der Slowakei ansässige Gesellschaft wegen der Verletzung des ungarischen Informationsgesetzes, das Umsetzungsgesetz der RL 95/46/EG. Der Gerichtshof hielt zunächst fest, dass in einer solchen Konstellation nach Art. 4 RL 95/46/EG[4] (auch) das Datenschutzrecht eines anderen Mitgliedstaats (hier Ungarn) als dem, in dem der für die Verarbeitung Verantwortliche eingetragen oder ansässig ist (hier die Slowakei), angewandt werden kann, soweit der für die Verarbeitung Verantwortliche mittels einer festen Einrichtung im Hoheitsgebiet des zuerst genannten Mitgliedstaats eine effektive und tatsächliche Tätigkeit ausübt, in deren Rahmen eine Datenverarbeitung durchgeführt wird. Eine solche Tätigkeit könne im Betreiben von Websites bestehen, die der Vermittlung von Immobilien dienen, die sich in diesem Mitgliedstaat befinden, insbesondere wenn diese Website hauptsächlich auf diesen Mitgliedstaat ausgerichtet ist. Zu berücksichtigen sei ferner, ob der Datenverantwortliche in dem betreffenden Mitgliedstaat über einen Vertreter verfügt, der die Forderungen aus dieser Tätigkeit einziehen und den Verantwortlichen in Verwaltungs- und Gerichtsverfahren vertreten soll. Die Staatsangehörigkeit der von der Datenverarbeitung Betroffenen sei hingegen irrelevant. Soweit die Befugnisse der nationalen Kontrollstelle betroffen sind sei diese zwar befugt, jedwede Beschwerde einer natürlichen Person unabhängig vom anwendbaren Recht zu prüfen; die Sanktionsmöglichkeiten stünden ihr jedoch nur soweit zu, wie auch das nationale Datenschutzrecht anwendbar ist. Andernfalls müsse sie die zuständige Behörde benachrichtigen.

Der Gerichtshof legt damit den räumlichen Anwendungsbereich der RL 95/46/EG (übrigens unter Bezugnahme auf die Zielsetzung der Richtlinie, einen umfassenden Persönlichkeitsschutz zu gewährleisten) weit aus und geht von einem „flexiblen“ Konzept der Niederlassung im Sinne des Art. 4 Abs. 1 lit. a RL 95/46/EG aus, für deren Vorliegen es offenbar auf die konkreten Umstände des Einzelfalls ankommt; ein Ansatz, der in einem späteren Urteil (in dem es um die Geschäftstätigkeit von *Amazon* ging) bestätigt wurde.[5] In diesem Folgeurteil stellte der Gerichtshof zusätzlich klar, dass zwar der Umstand, dass das für die Datenverarbeitung verantwortliche Unternehmen in einem Mitgliedstaat weder über eine Tochtergesellschaft noch über eine Zweigniederlassung verfügt, nicht ausschließe, dass es dort eine Niederlassung im Sinne von Art. 4 Abs. 1 lit. a RL 95/46/EG besitzt; allerdings könne eine Niederlassung nicht allein deshalb bestehen, weil von dem betreffenden Staatsgebiet

---

[3] EuGH, Rs. C-230/14 (Weltimmo/Nemzeti), ECLI:EU:C:2015:639.

[4] Wonach die Mitgliedstaaten die Umsetzungsgesetzgebung auch auf diejenigen Datenverarbeitungen anwenden, die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaates besitzt.

[5] EuGH, Rs. C-191/15 (Verein für Konsumenteninformation/Amazon), ECLI:EU:C:2016:612, Rn. 72 ff.

auf die Website des fraglichen Unternehmens zugegriffen werden kann. Ausschlaggebend dürfte letztlich sein, ob eine echte Geschäftstätigkeit spezifisch in dem betreffenden Staat ausgeübt wird und in irgendeiner Form eine spezifische Vertretung vorgesehen ist. Deutlich wird damit auch, dass die Anforderungen hier eher gering angesetzt sind, was im Übrigen nichts daran ändert, dass das flexible Konzept des Gerichtshofs durchaus Abgrenzungsprobleme mit sich bringen dürfte. Jedenfalls ermöglicht es aber einen erleichterten Zugriff auf Unternehmen, die Datenverarbeitungen im bzw. über das Internet vornehmen, und insofern steht das Urteil in der logischen Folge des Urteils in der Rs. C-131/12.[6] Hinzuweisen ist aber auch darauf, dass auf der Grundlage des Urteils davon auszugehen ist, dass zahlreiche Unternehmen neben dem Datenschutzrecht ihres Gesellschaftssitzes auch diejenigen zahlreicher weiterer Mitgliedstaaten zu beachten haben, in denen sie Niederlassungen im Sinne des Urteils betreiben. Dies wird sich jedoch mit dem Inkrafttreten der Datenschutz-Grundverordnung ändern, da diese unmittelbar anwendbares Recht schafft, wobei die in der Rechtsprechung entwickelten Prinzipien jedoch für die Frage nach dem Anwendungsbereich der Durchführungsgesetzgebung der Mitgliedstaaten sowie die Reichweite der Zuständigkeiten der nationalen Kontrollbehörden auch in Zukunft eine Rolle spielen können. Weiter bleiben die durch den Gerichtshof entwickelten Grundsätze in Bezug auf außerhalb der Union ansässige Unternehmen in jeder Beziehung relevant und sind hier auch von großer Bedeutung.

b) Rs. C-212/13 (Rynes)

Nach Art. 3 Abs. 2 RL 95/46/EG findet die Richtlinie (u.a.) keine Anwendung auf Datenverarbeitungen, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird. In der Rs. C-212/13[7] stand die Reichweite dieses Ausnahmetatbestands in Frage, dies im Zusammenhang mit dem Betrieb einer Überwachungskamera, die auch den öffentlichen Raum vor dem durch die Kamera „bewachten“ Haus abdeckte. Nach der wenig überraschenden Feststellung, dass das von einer Kamera aufgezeichnete Bild einer Person als ein personenbezogenes Datum im Sinne der Richtlinie anzusehen sei, schloss der Gerichtshof auf die Nichteinschlägigkeit der Ausnahmebestimmung des Art. 3 Abs. 2 RL 95/46/EG: Denn diese sei schon deshalb eng auszulegen, weil die RL 95/46/EG letztlich auf die effektive Verwirklichung der in Art. 7, Art. 8 GRC garantierten Rechte abziele, ganz abgesehen davon, dass auch der Wortlaut des Art. 3 Abs. 2 RL 95/46/EG, der von Datenverarbeitungen, die „ausschließlich“ im Rahmen persönlicher oder familiärer Tätigkeiten vorgenommen werden, spreche, in diese Richtung gehe. Auf dieser Grundlage müsse die Datenverarbeitung ausschließlich die persönliche oder familiäre Sphäre betreffen, was bei einer Videoüberwachung, die auch öffentlichen Raum umfasst, eben gerade nicht gegeben sei.

c) Rs. C-582/14 (Breyer)

In der Rs. C-582/14[8] hielt der Gerichtshof fest, dass auch eine dynamische IP-Adresse ein personenbezogenes Datum darstellt, dies soweit der Nutzer anhand von

---

[6] EuGH, Rs. C-131/12 (Google Spain und Google Inc.), ECLI:EU:C:2014:541. Zu diesem Urteil unten II.3.

[7] EuGH, Rs. C-212/13 (Rynes), ECLI:EU:C:2014:2428.

[8] *EuGH*, Rs. C-582/14, ECLI:EUC:2016:779 – Breyer.

Zusatzinformationen bestimmbar ist und diese Informationen aus tatsächlicher und rechtlicher Sicht zugänglich sind. Weiter sehe Art. 7 RL 95/46 eine erschöpfende und abschließende Liste derjenigen Fälle vor, in denen eine Verarbeitung personenbezogener Daten als rechtmäßig anzusehen sei, so dass die Mitgliedstaaten weder neue bzw. weitere Zulässigkeitsgründe einführen dürften noch zusätzliche Bedingungen stellen dürften, welche die Tragweite einer der in dieser Bestimmung enthaltenen Grundsätze modifizieren würde.[9] Daher sei es nicht mit der RL 95/46 (Datenschutzrichtlinie) vereinbar, wenn ein Anbieter von Online-Mediendiensten ohne Einwilligung des Nutzers dessen personenbezogene Daten nur verarbeiten darf, um die Inanspruchnahme der Dienstleistungen zu ermöglichen und die Abrechnung sicherzustellen (mit der Folge, dass z.B. eine Verarbeitung zur Gewährleistung der generellen Funktionsfähigkeit eines Online-Mediendienstes nicht zulässig wäre), stehe Art. 7 lit. f RL 95/46 doch einer mitgliedstaatlichen Regelung entgegen, die kategorisch und ganz allgemein die Verarbeitung bestimmter personenbezogener Daten ausschließt, ohne Raum für eine Abwägung der im konkreten Einzelfall einander gegenüberstehenden Rechte und Interessen zu lassen, so dass ein Mitgliedstaat das Ergebnis der Abwägung dieser Rechte und Interessen nicht abschließend vorschreiben dürfe, ohne Raum für ein Ergebnis zu lassen, das aufgrund besonderer Umstände des Einzelfalls anders ausfällt.

2. Datenschutz und staatliche Überwachungsmaßnahmen

In drei bemerkenswerten Urteilen hatte sich der Gerichtshof mit der Zulässigkeit staatlicher Überwachungsmaßnahmen bzw. der Vereinbarkeit gewisser diesbezüglicher Regelungen mit Art. 7, Art. 8 GRC auseinanderzusetzen.[10]

a) Vorratsdatenspeicherung (Rs. C-293/12, Digital Rights Ireland, und Rs. C-203/15 u.a., Tele2Sverige)

In dem von der Großen Kammer gefällten Urteil in der Rs. C-293/12[11] erklärte der EuGH die sog. Vorratsdatenspeicherungs-Richtlinie[12] für ungültig: Die Richtlinie – die die Mitgliedstaaten dazu verpflichtet, dafür zu sorgen, dass die Anbieter von elektronischen Kommunikationsdiensten die Verkehrs- und Standortdaten (nicht die Inhalte) der erfassten Kommunikation während mindestens sechs und höchstens 24 Monaten „auf Vorrat“ zu speichern haben – greife in den Schutzbereich der Art. 7, Art. 8 GRC (Recht auf Privatleben, Recht auf Schutz personenbezogener Daten) ein, erlaube die Gesamtheit der zu speichernden personenbezogenen Daten doch sehr genaue Rückschlüsse auf das Privatleben der Betroffenen. Allerdings sei der Wesensgehalt dieser Grundrechte nicht angetastet, da die Richtlinie nicht die

---

[9] S. insoweit auch schon *EuGH*, verb. Rs. C-468/10, C-469/10, ECLI:EU:C:2011:777 – ASNEF und FECEMD.

[10] S. ansonsten noch EuGH, verb. Rs. C-446/12 bis C-449/12 (Willems u.a.), ECLI:EU:C:2015:238; die Nutzung und Speicherung biometrischer Daten in der VO (EG) 2252/2004 über den biometrischen Pass für die Zwecke der Verordnung fnsplit

[11] EuGH, Rs. C-293/12 (Digital Rights Ireland), ECLI:EU:C:2014:238.

[12] RL 2006/24/EG über die Vorratsspeicherung von Daten, ABl. 2006 L 105/54.

Kenntnisnahme des Inhalts der Kommunikation gestatte und geeignete Maßnahmen zum Schutz der Daten gegen zufällige oder unrechtmäßige Verluste oder Modifikationen zu ergreifen seien. Der Eingriff – den der Gerichtshof als schwer bezeichnete, gehe es doch um eine stetige Überwachung – könne zwar grundsätzlich durch das Anliegen der Bekämpfung schwerer Kriminalität und damit der öffentlichen Sicherheit gerechtfertigt werden. Jedoch verneinte der Gerichtshof aufgrund einer detaillierten Prüfung die Erforderlichkeit; die Geeignetheit wurde hingegen unproblematisch bejaht, wobei der Gerichtshof hervorhob, hieran ändere auch der Umstand nichts, dass es manche elektronische Kommunikationsweisen gebe, die nicht in den Anwendungsbereich der Richtlinie fallen, da diese jedenfalls einen Beitrag zur Verfolgung des angestrebten Ziels zu leisten vermöge. Bei seiner Prüfung ging der EuGH aufgrund der besonderen Bedeutung des Schutzes personenbezogener Daten für das Grundrecht auf Achtung des Privatlebens sowie des Ausmaßes und der Schwere des mit der RL 2006/24/EG verbundenen Eingriffs in diese Grundrechte davon aus, dass der Gestaltungsspielraum des Unionsgesetzgebers eingeschränkt sei, so dass die Richtlinie einer strikten Kontrolle unterliege. Unter Rückgriff auf die einschlägige Rechtsprechung des EGMR betonte der Gerichtshof sodann, dass ein solch schwerwiegender Eingriff in die Rechte der Art. 7, Art. 8 GRC präzise Regeln für die Tragweite und die Anwendung der fraglichen Maßnahme vorsehen und Mindestanforderungen aufstellen müsse, so dass die Betroffenen über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen, Anforderungen, die im Rahmen automatisierter Verarbeitungen umso bedeutender seien. Diese Vorgaben erfülle die RL 2006/24/EG nicht, da sich ihr Anwendungsbereich generell auf alle Personen und alle elektronischen Kommunikationsmittel sowie sämtliche Verkehrsdaten erstrecke, ohne dass irgendeine Differenzierung, Einschränkung oder Ausnahme in Abhängigkeit von dem Ziel der Kriminalitätsbekämpfung vorgesehen sei. Auch sehe die Richtlinie kein objektives Kriterium vor, das den Zugang der zuständigen nationalen Behörden zu den Daten einschränke, und sie enthalte auch sonst keine materiell- oder verfahrensrechtlichen Voraussetzungen für den Zugang dieser Behörden zu den Daten. Sodann dürfe die Speicherfrist zwischen sechs und 24 Monaten liegen, ohne dass objektive Kriterien formuliert werden, die eine Differenzierung etwa in Abhängigkeit von den Datenkategorien zu gewährleisten vermögen. Schließlich seien auch die Vorgaben in Bezug auf die Datensicherheit nicht hinreichend klar und präzise, zumal sie nicht im Unionsgebiet zu speichern sind, was jedoch aufgrund der Überwachung auf der Grundlage des Unionsrechts notwendig sei.

Das Urteil ist schon deshalb bemerkenswert, weil es eines der wenigen Urteile ist, in denen der Gerichtshof einen Sekundärrechtsakt wegen Verstoßes gegen die Grundrechte für nichtig erklärt. Es überzeugt im Ergebnis und in der Begründung; bemerkenswert ist insbesondere die sehr differenzierte und argumentativ ausführliche Verhältnismäßigkeitsprüfung. Gewünscht hätte man sich jedoch – auch wenn man dem Gerichtshof hier ebenfalls zustimmen mag – eine etwas ausführlichere Stellungnahme zu der Frage, auf welche Weise denn methodisch ermittelt werden soll, unter welchen Voraussetzungen der „Wesensgehalt“ eines Grundrechts angetastet ist, was nach Art. 52 Abs. 1 GRC keinesfalls zulässig ist. Man wird aus den insofern etwas ergebnisorientierten Formulierungen des Gerichtshofs schließen können, dass die durch das jeweilige Grundrecht eingeräumten Rechte jedenfalls nicht vollumfänglich „ausgehebelt“ werden dürfen; aber auch auf dieser Grundlage bleiben selbstverständlich beachtliche Unschärfen, wenn auch Vieles dafür spricht, dass jedenfalls in den Fällen, in denen in Bezug auf einen nicht näher eingegrenzten Personenkreis auf Kommunikationsinhalte zurückgegriffen werden kann, der

Kerngehalt berührt ist.[13] Ebenfalls auslegungsbedürftig sind Aussage und Begründung in Bezug auf die Feststellung, die Grundrechtskonformität der Richtlinie unterliege einer strikten gerichtlichen Kontrolle, so dass der ansonsten häufig eingeräumte Gestaltungsspielraum des Gesetzgebers entsprechend eingeschränkt ist: Zwar vermag diese Aussage im Ergebnis im konkreten Fall durchaus zu überzeugen; fraglich ist jedoch, unter welchen Voraussetzungen denn jeweils eine solche strikte Kontrolle durchzuführen ist. Der Gerichtshof stellt hier auf die Bedeutung der in Frage stehenden Grundrechte sowie die Schwere des Eingriffs ab; aufgeworfen wird damit die Frage, ob diese Kriterien kumulativ zu verstehen sind (wofür die Formulierung des Gerichtshofs sprechen dürfte), wobei aber die besondere Bedeutung eines Grundrechts wohl auch für sich allein ein Kriterium für eine zumindest etwas strengere Prüfung darstellen könnte. Daran anschließend fragt es sich, welche Grundrechte denn von besonderer Bedeutung sind; vieles könnte hier dafür sprechen, an ihren Bezug zur in Art. 1 GRC garantierten Menschenwürde anzuknüpfen. Schließlich ist darauf hinzuweisen, dass der Gerichtshof, wenn er an mehreren Stellen die fehlende Präzision gewisser Regelungen moniert, offenbar davon ausgeht, dass die Richtlinie selbst bereits so ausgestaltet sein muss, dass sie den Anforderungen an die Schranken für den Grundrechtseingriff entspricht; es soll also nicht genügen, dass sie es den Mitgliedstaaten nicht verwehrt, die Richtlinie so umzusetzen, dass die EU-Grundrechte – die bei der Umsetzung von Richtlinien unbestrittenerweise zu beachten sind – nicht verletzt werden. Dieser Ansatz steht in einem gewissen Gegensatz zu anderen Urteilen des Gerichtshofs, in denen er darauf hinweist, ein Verstoß gegen die EU-Grundrechte könne deshalb nicht festgestellt werden, weil der Sekundärrechtsakt einen Gestaltungsspielraum lasse und die Mitgliedstaaten diesen dann eben so zu nutzen hätten, dass die EU-Grundrechte beachtet werden;[14] es war schon immer unklar, warum dann nicht gleich das Sekundärrecht so formuliert werden muss, zumal derartige Spielräume eine gewisse Rechtsunsicherheit mit sich bringen und es nicht klar ist, warum Gestaltungsspielräume so ausgestaltet werden, dass eine Verletzung von Grundrechten möglich ist. Insofern ist der in dem angezeigten Urteil vertretene Ansatz sehr zu begrüßen, wobei zu hoffen ist, dass er sich nicht nur auf die Fälle „strikter“ Kontrolle durch den Gerichtshof beschränkt.

Auch in der Rs. C-203/15[15] ging es um die Vorratsdatenspeicherung, dies jedoch in Bezug auf eine mitgliedstaatliche Vorschrift. Im Anschluss an sein Urteil in der Rs. C-293/12 hielt der *Gerichtshof* fest, es stehe nicht mit Art. 15 Abs. 1 RL 2002/58 (Datenschutzrichtlinie im Bereich der elektronischen Kommunikation[16]) in Einklang, zum Zweck der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten vorzusehen. Denn eine solche Maßnahme genüge nicht den Anforderungen der Verhältnismäßigkeit, wobei der Gerichtshof auf seine Erwägungen in der Rs. C-293/12 zur RL 2006/24 zurückgreift (da die in Frage stehende nationale Regelung im Wesentlichen derjenigen entspreche, die in der RL 2006/24 verankert war); letztlich war somit auch hier die „Pauschalität“

---

[13] In diesem Sinne dann auch die nachfolgende Rechtsprechung; vgl. EuGH, Rs. C-362/14 (Schrems), ECLI:EU:C:2015:650. S. noch unten II.2.b).

[14] Vgl. EuGH, Rs. C-540/03 (Parlament/Rat), ECLI:EU:C:2006:429.

[15] *EuGH*, verb. Rs. C-203/15, C-658/15, ECLI:EU:C:2016:970 – Tele2 Sverige (Große Kammer).

[16] ABl. 2002 L 201, 37.

der Pflicht zur Vorratsdatenspeicherung entscheidend. Ebensowenig sei es mit Art. 15 Abs. 1 RL 2002/58 vereinbar, wenn der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten nicht ausschließlich auf die Zwecke der Bekämpfung schwerer Straftaten beschränkt wird, der Zugang keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird und nicht gewährleistet ist, dass die betreffenden Daten im Gebiet der Union auf Vorrat zu speichern sind. Dabei seien bei der Regelung des Zugangs der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten nicht nur die in Art. 15 Abs. 1 RL 2002/58 genannten Zwecke zu beachten, sondern es seien auch materiell- und verfahrensrechtliche Voraussetzungen bezüglich dieses Zugangs zu regeln, womit ein allgemeiner Zugang gerade nicht in Einklang stehe.

Der Gerichtshof legt Art. 15 Abs. 1 RL 2002/58 im Lichte der Art. 7, 8, 52 I GRCh aus und nimmt eine ausführliche Prüfung der Grundrechtskonformität der in Frage stehenden nationalen Maßnahmen vor. Dabei hebt er auch hervor, dass eine Pflicht zur Vorratsdatenspeicherung zur Bekämpfung schwerer Straftaten zulässig sein könne, wenn sie hinsichtlich der Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsdatenspeicherung auf das absolut Notwendig beschränkt ist; dabei wird durchaus ein gewisser Spielraum eingeräumt, so wenn auf die Objektivität der Kriterien (die auch ein bestimmtes geographisches Gebiet betreffen können) hingewiesen wird.

b) Rs. C-362/14 (Schrems)

In der sog. *Safe-Harbor*-Entscheidung[17] stellte die Kommission fest, dass eine Datenübermittlung in die USA nach den Grundsätzen des sog. *Safe Harbor* (wonach diejenigen Organisationen in den USA, an welche die Daten übermittelt werden, sich zur Einhaltung einer Reihe von datenschutzrechtlichen Grundsätzen verpflichten) ein angemessenes Schutzniveau übermittelter personenbezogener Daten gewährleiste und die danach erfolgende grenzüberschreitende Datenübermittlung daher den Anforderungen der RL 95/46/EG entspreche. In der von der Großen Kammer entschiedenen Rs. C-362/14[18] (erklärte der EuGH diese Entscheidung für ungültig, wobei er sich auch zu den Befugnissen der nationalen Kontrollstellen in diesem Zusammenhang äußerte:

- Falls eine Person – wie im Ausgangsfall – geltend macht, ein Drittstaat, in den ihre persönlichen Daten übermittelt werden, gewährleiste kein angemessenes Schutzniveau im Sinne der RL 95/46/EG, sei die zuständige nationale Kontrollstelle im Sinne des Art. 28 RL 95/46/EG befugt, die Eingabe dieser Person auch dann zu prüfen, wenn die Kommission in einer Entscheidung gemäß Art. 25 Abs. 6 RL 95/46/EG festgestellt hatte, dass (ggf. unter bestimmten Voraussetzungen) in dem jeweiligen Drittstaat ein angemessenes Schutzniveau gewährleistet sei. Ausgangspunkt für die diesbezügliche sehr ausführliche Begründung des Gerichtshof ist die Feststellung, die RL 95/46/EG sei im Lichte der Grundrechtecharta

---

[17] Entscheidung 2000/520 gemäß der RL 95/46/EG über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ gewährleisteten Schutzes, ABl. 2000 L 215/7.

[18] EuGH, Rs. C-362/14 (Schrems), ECLI:EU:C:2015:650. Der Ausgangsfall betraf die Klage eines österreichischen Staatsbürgers gegen *Facebook Ireland*, mittels derer er die Übermittlung seiner Daten in die USA unterbinden lassen wollte.

auszulegen, wobei Art. 7, Art. 8 GRC sowie die Richtlinie nicht nur einen wirksamen und umfassenden Schutz, sondern auch ein hohes Schutzniveau gewährleisten sollten. Die nationalen Kontrollstellen sollten in völliger Unabhängigkeit die wirksame und zuverlässige Kontrolle der Einhaltung der datenschutzrechtlichen Vorschriften gewährleisten und verfügten zu diesem Zweck über eine große Bandbreite von Befugnissen, die in Art. 28 Abs. 3 RL 95/46/EG in nicht abschließender Weise aufgezählt seien. Diese Befugnisse bezögen sich auch auf die Übermittlung personenbezogener Daten in einen Drittstaat, stelle diese Übermittlung doch nach Art. 2 lit. b RL 95/46/EG eine im Hoheitsgebiet des betreffenden Mitgliedstaats vorgenommene Datenbearbeitung dar. Die Kontrollstellen seien daher auch zur Prüfung befugt, ob bei einer Übermittlung personenbezogener Daten in einen Drittstaat die in der RL 95/46/EG aufgestellten Anforderungen eingehalten werden. Zwar könne die Feststellung, ob ein Drittstaat über ein angemessenes Schutzniveau (die Voraussetzung für eine zulässige Datenübermittlung in einen Drittstaat) verfügt sowohl von den Mitgliedstaaten als auch von der Kommission getroffen werden, und die Kommission könne auf der Grundlage des Art. 25 Abs. 6 RL 95/46/EG eine Entscheidung erlassen, welche die Angemessenheit des Schutzniveaus in einem Mitgliedstaat feststellt. Da eine solche Entscheidung die mitgliedstaatlichen Behörden binde (Art. 288 Abs. 4 AEUV), dürften diese (und damit auch die nationalen Kontrollstellen) – solange die Entscheidung der Kommission nicht vom EuGH für ungültig erklärt wurde – zwar keine dieser Entscheidung zuwiderlaufenden Maßnahmen ergreifen (wie etwa die Feststellung, im Gegensatz zur Entscheidung der Kommission, das Schutzniveau sei nicht angemessen); dies ändere jedoch nichts daran, dass die nationalen Kontrollstelen sich mit entsprechenden Eingaben der Betroffenen befassen dürften, ganz abgesehen davon, dass eine solche Entscheidung der Kommission die Zuständigkeit der Kontrollstellen nach der Richtlinie weder beseitigen noch einschränken könne. Es liefe daher dem durch die RL 95/46/EG geschaffenen System sowie dem Zweck der Art. 25, Art. 28 RL 95/46/EG zuwider, wenn sich eine nationale Kontrollstelle nicht mit der Eingabe einer Person befassen dürfe, welche die Übermittlung ihrer Daten in einen Drittstaat, die Gegenstand einer Kommissionsentscheidung ist, betrifft. Aufgrund einer solchen Eingabe müssten die Kontrollstellen prüfen können, ob bei der Datenübermittlung die in der Richtlinie formulierten Anforderungen gewahrt werden. Macht eine natürliche Person dies geltend, so sei eine solche Eingabe letztlich dahingehend zu verstehen, dass sie die Frage der Vereinbarkeit der einschlägigen Kommissionsentscheidung mit den Vorgaben der Richtlinie betrifft. Da es jedoch allein Sache des EuGH sei, Unionsrechtsakte für ungültig zu erklären, müsse die entsprechende Frage vor ein nationales Gericht gebracht werden können (je nach Ansicht der Kontrollstelle entweder von dem Betroffenen oder von der Kontrollstelle), das dann den EuGH anzurufen hat.

- Vor dem Hintergrund der angestellten Erwägungen prüfte der Gerichtshof die Gültigkeit der Entscheidung der Kommission und verneinte ihre Vereinbarkeit mit der RL 95/46/EG, da auch die sog. *Safe-Harbor*-Grundsätze kein angemessenes Datenschutzniveau zu gewährleisten vermögen. Denn obwohl die RL 95/46/EG nicht im Einzelnen definiere, was als angemessenes Schutzniveau zu gelten hat, ergebe sich doch aus dem Wortlaut und dem Sinn und Zweck der Vorschriften, dass es um eine Art „Garantie“ eines solchen Schutzes gehen müsse und dass auch im Falle der Übermittlung in einen Drittstaat ein hohes Schutzniveau zu gewährleisten sei, das zwar nicht identisch mit demjenigen der RL 95/46/EG sein müsse, jedoch einen gleichwertigen Schutz bieten müsse. Jeder andere Ansatz verkenne die Zielsetzung der RL 95/46/EG und führe zu zahlreichen Umgehungsmöglichkeiten. Im Übrigen müsse es – wie sich aus dem Wortlaut der RL 95/46/EG ergebe – die Rechtsordnung des Drittstaates sein, die ein solches angemessenes Schutzniveau gewährleistet, wobei die Mittel im Vergleich zu denjenigen, die in der Union herangezogen werden, anders ausgestaltet sein können, was jedoch nichts daran ändere,

dass sie in der Praxis im Hinblick auf die Gewährleistung eines gleichwertigen Schutzes wirksam sein müssten. Die Kommission sei vor diesem Hintergrund zur inhaltlichen Prüfung der einschlägigen Regeln in dem betreffenden Drittstaat sowie der zur Gewährleistung der Einhaltung dieser Regeln dienenden Praxis verpflichtet. Überdies sei in regelmäßigen Abständen zu prüfen, ob die Feststellung der Angemessenheit des Schutzniveaus nach wie vor gerechtfertigt ist, wobei eine solche Prüfung jedenfalls dann vorzunehmen sei, wenn Anhaltspunkte bestehen, die daran Zweifel wecken könnten. Die gerichtliche Überprüfung sei angesichts der Bedeutung der in Frage stehenden Grundrechte im Fall der Übermittlung personenbezogener Daten in Drittstaaten strikt auszugestalten und der Wertungsspielraum der Kommission entsprechend beschränkt. Ausgehend von diesen Grundsätzen erklärte der Gerichtshof die Entscheidung der Kommission für ungültig, da in den USA kein angemessenes Schutzniveau gewährleistet sei. Hauptgrund für diesen Schluss – den der EuGH auf der Grundlage einer detaillierten Analyse des Konzepts des *Safe Harbor* entwickelte – war einerseits der Umstand, dass die Selbstzertifizierung (auf der das Konzept des *Safe Harbor* beruht und das vom EuGH grundsätzlich durchaus als zulässiges Konzept angesehen wird) nicht einhergehe mit in der innerstaatlichen Rechtsordnung vorgesehenen (staatlichen) Maßnahmen, die die Einhaltung der datenschutzrechtlichen Grundsätze verlangen und gewährleisten. Andererseits könnten die grundsätzlich einzuhaltenden datenschutzrechtlichen Prinzipien allgemein eingeschränkt werden, sofern dies durch Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen begründet ist, so dass diesen Erfordernissen zudem sehr generellen Charakters letztlich Vorrang vor den datenschutzrechtlichen Grundsätzen eingeräumt werde; Anhaltspunkte für Begrenzungen von Eingriffen in die Grundrechte der Betroffenen seien nicht zu erkennen, ganz abgesehen davon, dass kein wirksamer gerichtlicher Rechtsschutz gegen Eingriffe vorgesehen sei. Insgesamt gebe es daher weder präzise Regeln über die Zulässigkeit eines Eingriffs in Art. 7, Art. 8 GRC noch sei der Grundsatz der Verhältnismäßigkeit gewahrt, und im Übrigen verletze eine Regelung, die es gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des Art. 7 GRC. Darüber hinaus schränke die Entscheidung die Befugnisse der nationalen Kontrollstellen ein, da sie ihnen die Möglichkeit nimmt, Maßnahmen zu ergreifen, um die Einhaltung der Vorgaben für die grenzüberschreitende Datenübermittlung für den Fall zu gewährleisten, dass eine Entscheidung der Kommission das Bestehen eines angemessenen Schutzniveaus festgestellt hatte.

Das Urteil des EuGH impliziert, dass Datenübermittlungen in die USA jedenfalls solange nicht zulässig sind, wie die erwähnten gesetzlich vorgesehenen Befugnisse der Sicherheitsbehörden bestehen, es sei denn, die Datenübermittlungen könnten aus anderen Gründen (insbesondere *Binding Corporate Rules*, Standardvertragsklauseln oder Einwilligungen) zulässig sein; beim derzeitigen Stand der Dinge ist jedoch ungeklärt, ob und ggf. inwieweit gewisse der Erwägungen des Gerichtshofs *mutatis mutandis* auch für diese weiteren Rechtsgrundlagen einer Datenübermittlung Anwendung finden könnten (was insbesondere für die beiden erstgenannten in Frage kommt, denn letztlich wird ja das Fehlen der Gewährleistung eines angemessenen Schutzes im nationalen Recht moniert). Darüber hinaus ist aus grundsätzlicher Sicht hervorzuheben, dass der Gerichtshof in überzeugender Weise davon ausgeht, dass die jeweilige innerstaatliche Rechtsordnung das angemessene Schutzniveau gewährleisten muss, an das übrigens eher hohe Anforderungen gestellt werden. Das Erfordernis der effektiven Einhaltung auch in der Praxis dürfte im Übrigen nicht immer einfach zu erfüllen sein; man wird hier wohl auf gewisse Plausibilitätserwägungen zurückgreifen dürfen. In der öffentlichen Diskussion bislang eher weniger beachtet sind die Ausführungen des Gerichtshofs zu den Kompetenzen der nationalen Aufsichtsbehörden, die nicht durch eine Entscheidung der Kommission beschnitten

werden dürfen, eine wichtige Feststellung im Hinblick auf den Schutz der Rechte Einzelner und die effektive Beachtung des Datenschutzrechts. Interessant ist in diesem Zusammenhang, dass der Gerichtshof zwar davon spricht, die Aufsichtsbehörde dürfe entsprechende Eingaben Einzelner prüfen; diese Formulierung geht jedoch wohl auf die Formulierung der Vorlagefrage zurück: Denn im Falle einer Eingabe eines Einzelnen besteht nach Art. 28 RL 95/46/EG wohl eine Pflicht der nationalen Kontrollstelle, die Eingabe auch zu behandeln. Schließlich impliziert der Ansatz des Gerichtshofs, dass eine Regelung, die es Behörden generell gestattet, auf die Inhalte elektronischer Kommunikation zurückzugreifen, den Wesensgehalt des Art. 7 GRC beeinträchtigt, die Unzulässigkeit solcher Vorschriften, so dass der entsprechende Grundrechtseingriff damit auch nicht rechtfertigungsfähig ist.

Inzwischen hat die Union mit den Vereinigten Staaten ein neues Abkommen ausgehandelt, das Datenübermittlungen in die USA erlaubt (sog. „Privacy Shield"),[19] wobei fraglich ist, ob dieses einer wohl zu erwartenden gerichtlichen Überprüfung durch den EuGH standhalten wird, sind die vom Gerichtshof formulierten Anforderungen doch sehr streng ausgestaltet (was übrigens nicht mit Blick auf eine angebliche Extraterritorialität kritisiert werden kann, geht es doch um eine Datenverarbeitung in der Union, nämlich die Übermittlung in Drittstaaten).

3. Das „Recht auf Vergessenwerden"

Ebenfalls das Recht auf Schutz personenbezogener Daten – wenn auch in seiner Konkretisierung in der RL 95/46/EG (Datenschutz-Richtlinie)[20] – war Gegenstand der von der Großen Kammer entschiedenen Rs. C-131/12.[21] Auf der Grundlage der Bejahung der Eröffnung des Anwendungsbereichs der RL 95/46/EG, da die Tätigkeit einer Suchmaschine als Datenverarbeitung im Sinne der RL 95/46/EG anzusehen sei und diese auch im Rahmen der Niederlassung von *Google* in Spanien ausgeübt werde (so dass der räumliche Anwendungsbereich der RL 95/46/EG betroffen sei), nahm der Gerichtshof in erster Linie zur rechtlichen Tragweite der Art. 12 lit. b, Art. 14 Abs. 1 lit. a RL 95/46/EG Stellung: Diese Bestimmungen seien so auszulegen, dass ein von der Datenbearbeitung durch die Suchmaschine Betroffener (dessen Personendaten also im Rahmen der Suche angezeigt werden) verlangen kann, dass der Suchmaschinenbetreiber prüft, ob die betroffene Person ein Recht darauf hat, dass ihr Name nicht mehr durch die Ergebnisliste erfasst wird, zumindest nicht in Bezug auf bestimmte personenbezogene Informationen. Irrelevant sei dabei, ob dem Betroffenen durch die Anzeige ein Schaden entsteht. Art. 7, Art. 8 GRC räumten den Betroffenen ein Recht ein, dass bestimmte sie betreffende Informationen nicht mehr auf der Ergebnisliste angezeigt werden, so dass diese Rechte grundsätzlich sowohl gegenüber dem wirtschaftlichen Interesse des Suchmaschinenbetreibers als auch dem Interesse der breiten Öffentlichkeit am Zugang zu solchen Informationen überwögen, letzteres unter dem Vorbehalt, dass nicht besondere Gründe (z.B. die

---

[19] Vgl. hierzu z.B. *v. Lewinski*, Privacy Shield – Notdeich nach dem Pearl Harbor für die transatlantischen Datentransfers, EuR 2016, 405 ff.; *Weiss,* Nach dem Ende von Safe Harbor: Das EU-U.S.-Privacy Shield, RDV 2016, 135 ff.

[20] ABl. 1995 L 281/31.

[21] EuGH, Rs. C-131/12 (Google Spain und Google Inc.), ECLI:EU:C:2014:541.

Rolle der Person im öffentlichen Leben) ein anderes Abwägungsergebnis nahelegen. Auf dieser Grundlage und in Anbetracht des Umstandes, dass Suchmaschinen einen besonders leichten Zugang zu den relevanten Informationen ermöglichen, sei der Suchmaschinenbetreiber verpflichtet, bei Vorliegen der skizzierten Voraussetzungen die Ergebnisliste entsprechend zu verändern, dies auch soweit die Information noch auf den entsprechenden Internetseiten zu finden ist und diese Veröffentlichung rechtmäßig ist.

Das Urteil überzeugt im Ergebnis und in der Begründung und ist in erster Linie aus folgenden Gründen bemerkenswert:

- Erstens dürfte ihm der auch in anderen Bereichen relevante Grundsatz zu entnehmen sein, dass der grundrechtliche Anspruch darauf, dass bestimmte personenbezogene Daten nicht mehr (in einer bestimmten Art und Weise) der Öffentlichkeit zugänglich gemacht werden dürfen, schwerer wiegt als ebenfalls implizierte wirtschaftliche Interessen. Die Schwierigkeit in diesem Zusammenhang wird regelmäßig darin liegen, festzustellen, ob tatsächlich ein „Löschungsanspruch“ besteht, wobei es die Ausführungen des Gerichtshofs nahelegen, dass grundsätzlich bereits aufgrund der Verknüpfungsmöglichkeiten und der damit einhergehenden Eingriffe in die Persönlichkeitsrechte der Betroffenen ein derartiger Löschungsanspruch besteht.

- Zweitens, und damit in engem Zusammenhang stehend, gilt dies auch in reinen Privatrechtsverhältnissen, womit der Gerichtshof im Ergebnis von einer Drittwirkung der genannten Grundrechte ausgeht, wobei diese Drittwirkung jedoch auf der Einräumung der entsprechenden Rechte in der RL 95/46/EG beruhen dürfte, seien diese doch im Lichte der Grundrechte auszulegen.

- Drittens ist die Differenzierung zwischen einer Veröffentlichung von Personendaten auf „irgendeiner“ Webseite und ihrer Zugänglichkeit über eine Suchmaschine und die strengeren Anforderungen an letztere angesichts der Rolle von Suchmaschinen für die Auffindbarkeit von Informationen in jeder Beziehung überzeugend und wohl auch auf andere Formen „differenzierter“ Information übertragbar.

- Schließlich – und dies dürfte in der bisherigen Diskussion über das Urteil meist übersehen werden – geht das Urteil davon aus, dass Suchmaschinenbetreiber selbst als Datenverarbeiter im Sinne der Richtlinie anzusehen sind, dies mit der Folge, dass ihre Datenverarbeitung als solche den Rechtmäßigkeitsanforderungen der Richtlinie – die im Sinne der Grundrechtecharta auszulegen sind – entsprechen muss. Für diese muss daher einer der in Art. 7 RL 95/46/EG aufgeführten (abschließend zu verstehenden) Erlaubnistatbestände vorliegen, wobei für Suchmaschinen in aller Regel im Wesentlichen die Erforderlichkeit der Erfüllung einer Aufgabe, die im öffentlichen Interesse liegt (nämlich die Zurverfügungstellung von Informationen), in Frage kommt. Dies ist aber in jedem Fall zu prüfen, so dass Suchmaschinenbetreiber an sich nicht erst auf Antrag, sondern von sich aus von der Anzeige bestimmter Personendaten absehen müssten, wenn kein überwiegendes öffentliches Interesse anzunehmen ist. Zumindest aber ist davon auszugehen, dass im Falle eines entsprechenden Antrags der Betroffenen deren Interesse regelmäßig (Ausnahmen sind im Falle von Personen des öffentlichen Lebens denkbar) überwiegt.

4. Zulässigkeit der Bekanntgabe von Personendaten

Um die Auslegung diverser Bestimmungen der RL 95/46/EG ging es in der Rs. C-201/14,[22] dies im Zusammenhang mit der Übermittlung der Einkünfte von Selbständigen durch die Steuerverwaltung an die Nationale Kasse der Krankenversicherungen, mit der Folge, dass von den Selbständigen rückständige Krankenversicherungsbeiträge eingefordert wurden. Der Gerichtshof erachtete diese Datenübermittlung als nicht mit der RL 95/46/EG in Einklang stehend: Denn die Verpflichtung, Daten nach Treu und Glauben zu verarbeiten, impliziere eine Pflicht der Verwaltungsbehörde, die Betroffenen davon zu unterrichten, dass die personenbezogenen Daten an eine andere Verwaltungsbehörde weitergeleitet werden, um von dieser in ihrer Eigenschaft als deren Empfänger verarbeitet zu werden; eine solche Unterrichtung habe im Ausgangsfall offenbar nicht stattgefunden. Zudem seien die sich aus Art. 11 RL 95/46/EG ergebenden Informationspflichten nicht eingehalten worden. Art. 13 RL 95/46/EG (der gewisse Ausnahmen von den Verpflichtungen der Richtlinie vorsieht) könne schon deshalb nicht zum Zuge kommen, weil die betreffende Übermittlung nicht durch Rechtsvorschriften vorgesehen war. Nicht ganz klar wird aus dem Urteil, ob bereits allein die Verletzung der Informationspflicht aus Art. 10, Art. 11 RL 95/46/EG quasi „automatisch“ einen Verstoß gegen Treu und Glauben und damit die Rechtswidrigkeit der Verarbeitung nach sich zieht. Da eine Information dann nicht zu erfolgen hat, wenn eine Verarbeitung gesetzlich vorgesehen ist und geeignete Garantien bestehen, spricht Vieles für die Bejahung dieser Frage.

5. Unabhängigkeit der nationalen Kontrollstellen

Der Gerichtshof hatte sich bereits in einem Urteil aus dem Jahr 2010 (Rs. C-518/07)[23] mit den genauen Anforderungen an die Unabhängigkeit der nach Art. 28 RL 95/46/EG einzurichtenden datenschutzrechtlichen Aufsichtsbehörden („Kontrollstellen“) auseinanderzusetzen: Der Gerichtshof formulierte hier zunächst einige grundsätzliche Aussagen zum Erfordernis der Unabhängigkeit, zur Rolle der Kontrollstelle und zu ihrem Verhältnis zur Stellung des Europäischen Datenschutzbeauftragten:

- Ausgehend vom Wortlaut des Art. 28 Abs. 1 RL 95/46/EG, wonach die Kontrollstelle in „völliger Unabhängigkeit“ agieren müsse, hielt der EuGH zunächst fest, dass nichts in dieser Wendung darauf hindeute, dass sich dieses durch das Adjektiv „völlig“ verstärkte Unabhängigkeitserfordernis nur auf das Verhältnis zwischen den Kontrollstellen und den ihrer Kontrolle unterstellten Einrichtungen beziehe, so dass die Kontrollstelle frei von jeglicher Einflussnahme von außerhalb, sei sie nun unmittelbar oder mittelbar, sein müsse.

- Zweitens sei die Rolle der Kontrollstellen im Zusammenhang mit der Zielsetzung der Richtlinie zu sehen: Diese solle den freien Verkehr personenbezogener Daten im Binnenmarkt fördern, was jedoch das aus Art. 8 EMRK fließende Recht auf Achtung der Privatsphäre beeinträchtigen könne, so dass die Richtlinie auch das Ziel der Gewährleistung eines hohen Datenschutzniveaus verfolge. Die Kontrollstellen seien nun die Hüter dieses Grundrechts, und ihre Tätigkeit solle die betroffenen Personen stärker schützen, so dass die

[22] EuGH, Rs. C-201/14 (Bara u.a.), ECLI:EU:C:2015:638.

[23] EuGH, Rs. C-518/07 (Kommission/Deutschland), ECLI:EU:C:2010:125.

Kontrollstellen bei der Wahrnehmung ihrer Aufgaben objektiv und unparteiisch vorgehen müssten. Hierzu müssten sie aber vor jeglicher Einflussnahme von außen sicher sein.

- Drittens sei der Begriff „völlige Unabhängigkeit“ in Art. 28 Abs. 1 RL 95/46/EG ebenso wie in Art. 44 Abs. 1 VO (EG) 45/2001[24] (der die Stellung des Europäischen Datenschutzbeauftragten regelt und ebenfalls den Begriff der „völligen Unabhängigkeit“ verwendet) auszulegen.

Ausgehend von diesen Grundsätzen erachtete der Gerichtshof die staatliche Aufsicht über gewisse Kontrollstellen der deutschen Bundesländer als nicht mit diesen Vorgaben in Einklang stehend: Denn diese ermögliche es der Regierung des betreffenden Landes oder einer Stelle der ihr untergeordneten Verwaltung, auf Entscheidungen der Kontrollstellen unmittelbar oder mittelbar Einfluss zu nehmen bzw. diese Entscheidungen sogar aufzuheben oder zu ersetzen. Damit sei das Erfordernis der Unabhängigkeit jedoch gerade nicht erfüllt. Hieran ändere auch der Umstand nichts, dass die staatliche Aufsicht nur sicherstellen soll, dass das Agieren der Kontrollstellen den geltenden rechtlichen Vorgaben entspricht und demnach nicht darauf abzielt, diese Stellen zu zwingen, politische Zielsetzungen zu verfolgen, die datenschutzrechtlichen Anliegen zuwiderlaufen. Denn es lasse sich gerade nicht ausschließen, dass die Aufsichtsstellen mitunter nicht zu einem objektiven Vorgehen in der Lage sind, könnten sie doch in bestimmten Situationen (so z.B. wenn es um eine Kooperation von öffentlichen und privaten Stellen oder um öffentliche Aufträge geht oder wenn wirtschaftliche Interessen zur Debatte stehen) ein Interesse an der Nichteinhaltung datenschutzrechtlicher Vorgaben haben. Darüber hinaus reiche die bloße Gefahr einer politischen Einflussnahme der Aufsichtsbehörden auf die Entscheidungen der Kontrollstellen aus, um deren unabhängige Wahrnehmung ihrer Aufgaben zu beeinträchtigen. Denn die Kontrollstellen könnten in einer Art „vorauseilenden Gehorsams“ Rücksicht auf die Entscheidungspraxis der Aufsichtsstelle nehmen, ganz abgesehen davon, dass es die Rolle der Kontrollstellen als Hüter des Rechts erfordere, dass ihre Entscheidungen, also sie selbst, über jeglichen Verdacht der Parteilichkeit erhaben sind.

Im Wesentlichen bestätigt wurde dieses Urteil in der die Rechtslage in Österreich betreffenden Rs. C-614/10,[25] in welcher der Gerichtshof zusätzlich noch betonte, eine funktionelle Unabhängigkeit (im Sinne einer fehlenden Bindung an Weisungen) sei zwar eine notwendige, aber keine hinreichende Bedingung für die geforderte Unabhängigkeit. Vielmehr müsse auch jede Form der mittelbaren Einflussnahme, die zur Steuerung der Entscheidungen der Kontrollstelle geeignet wäre, ausgeschlossen sein. Eine solche Gefahr der mittelbaren Einflussnahme liege jedoch vor, wenn ein geschäftsführendes Mitglied der Kontrollstelle dem „normalen“ Dienstverhältnis für Bundesbeamte unterliegt, da mit diesem eine Reihe zumindest indirekter Einflussmöglichkeiten bzw. Gefahren der mittelbaren Einflussnahme verbunden sei, ganz abgesehen davon, dass auf diese Weise auch der Anschein der Parteilichkeit entstehen könne. Ebensowenig stehe die Eingliederung der Kontrollstelle in das Bundeskanzleramt mit den Anforderungen der Unabhängigkeit in Einklang, sei hiermit doch eine Dienstaufsicht über die angestellten Personen verbunden, und schließlich

---

[24] VO (EG) 45/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. 2001 L 8/1.

[25] EuGH, Rs. C-614/10 (Kommission/Österreich), ECLI:EU:C:2012:631.

sei auch das Recht des Bundeskanzlers, sich jederzeit über alle Gegenstände der Geschäftsführung zu unterrichten, geeignet, die Kontrollstelle einer mittelbaren Einflussnahme durch diesen auszusetzen.

Auch in der Rs. C-288/12[26] ging es – wenn auch in einer anders gelagerten Konstellation – um die genauen Anforderungen an die Unabhängigkeit der Aufsichtsbehörden, dies im Zusammenhang mit der vorzeitigen (also vor Ablauf der ursprünglich beschlossenen Amtsdauer) Beendigung des Mandats der Kontrollstelle. Der Gerichtshof (Große Kammer) schloss auf einen Verstoß gegen die Vorgaben der Richtlinie: Denn das Erfordernis der Unabhängigkeit sei dahin zu verstehen, dass die Kontrollstelle ihre Aufgaben ohne jegliche äußere Einflussnahme wahrnehmen können muss, wobei bereits die bloße Gefahr einer politischen Einflussnahme auf die Entscheidungen der Kontrollen ausreiche, um deren unabhängige Wahrnehmung ihrer Aufgaben in Frage zu stellen. Denn daraus könne ein „vorauseilender Gehorsam“ dieser Stellen im Verhältnis zu den politischen Entscheidungsträgern entstehen und im Übrigen müssten die Stellen auch über jeden Verdacht der Parteilichkeit erhaben sein. Wenn nun das Mandat einer Kontrollstelle vor seinem ursprünglich vorgesehenen Ablauf beendet werden könnte, ohne die von den anwendbaren Rechtsvorschriften zu diesem Zweck im Voraus festgelegten Grundsätze und Garantien zu beachten, könnte eben gerade eine solche Gefahr der Einflussnahme bestehen, da die Drohung einer solchen vorzeitigen Beendigung zu einer Form des Gehorsams dieser Stelle gegenüber den politisch Verantwortlichen führen könne, die mit dem Unabhängigkeitsgebot nicht vereinbar sei. Insbesondere könne die Entscheidung über die Modifikation des institutionellen Modells nicht die vorzeitige Beendigung der Amtszeit rechtfertigen; eine solche Modifikation – die den Mitgliedstaaten im Rahmen der Vorgaben der Richtlinie freistehe – sei unter Beachtung der Amtszeiten vorzunehmen.

Insgesamt fasst der Gerichtshof – ausgehend von den Zielsetzungen der Richtlinie – die Anforderungen an die Unabhängigkeit der Kontrollstellen denkbar streng, wobei insbesondere zwei Gesichtspunkte von Bedeutung sein dürften: Zum einen wird jegliche Einflussnahme auf die Kontrollstelle von „außen“ als Beeinträchtigung ihrer Unabhängigkeit gesehen, unabhängig davon, ob diese den zu kontrollierenden Personen bzw. Einrichtungen zuzurechnen ist oder nicht. Dies bedeutet insbesondere auch, dass die Kontrollstellen – gleichgültig, ob sie nun Private oder staatliche Stellen zu kontrollieren haben – denselben (strengen) Anforderungen an die Unabhängigkeit zu genügen haben. Zum anderen genügt die Gefahr – wobei man hier, da der Gerichtshof hervorhebt, dass die Kontrollstellen als Hüter des Rechts über „jeden Verdacht der Parteilichkeit“ erhaben sein müssten, „der Anschein“ präzisierend hinzufügen kann, geht es doch letztlich um eine Art abstrakte Gefährdung – einer solchen Einflussnahme, unabhängig davon, ob es zu einer solchen kommt oder gekommen ist.

Letztlich müssen die Kontrollstellen damit eine richterähnliche Unabhängigkeit genießen, ein ebenso zwingender wie überzeugender Ansatz vor dem Hintergrund des Konzepts und der Kompetenzen der Kontrollstellen, so wie sie in der RL 95/46/EG verankert sind: Denn die Richtlinie geht davon aus, dass es aufgrund der besonderen Charakteristika des Datenschutzes bzw. des Datenschutzrechts nicht ausreicht, dass – wie in vielen anderen Rechtsgebieten – die staatlichen Behörden beauftragt sind, die

[26] EuGH, Rs. C-288/12 (Kommission/Ungarn), ECLI:EU:C:2014:237.

Gesetze durchzuführen und ihre Einhaltung zu kontrollieren bzw. sicherzustellen. Gerade weil zahlreiche Gefährdungen der Privatsphäre der Rechtsunterworfenen auch von staatlichen Behörden ausgehen können bzw. diese in verschiedener Hinsicht in Aktivitäten Privater involviert sein können und weil die Einzelnen aus verschiedenen Gründen bei der Wahrnehmung ihrer Rechte auf Schwierigkeiten stoßen bzw. stoßen können (etwa weil ihnen die Datenverarbeitung verborgen geblieben ist oder weil das „Machtgefälle" zwischen Betroffenen und Datenverarbeitern mitunter sehr groß ist), erachtete man eine im Verhältnis zu den Gerichten zusätzliche Kontrollebene für notwendig. Soll diese nun Sinn machen, so muss sie tatsächlich völlig unabhängig sein, da man ja sonst auch (zumindest für die Kontrolle der Privaten) eine staatliche Stelle hätte vorsehen können.[27]

III. Fazit

Versucht man aus der Gesamtheit der in diesem Beitrag besprochenen jüngeren Urteile des Gerichtshofs ein kurzes Fazit zu ziehen bzw. über die jeweils konkret aufgeworfenen Fragen hinausgehende Grundsätze zu formulieren, so scheinen folgende Aspekte von besonderer Bedeutung zu sein:

- Grundsätzlich wird im Rahmen der Prüfung der Vereinbarkeit von Unionsrechtsakten mit Art. 7, Art. 8 GRC eine sehr hohe Kontrolldichte angelegt. Dem Gestaltungsspielraum des Unionsgesetzgebers werden auf diese Weise entsprechend enge Grenzen gesteckt.

- Der Gerichtshof wendet die allgemeinen datenschutzrechtlichen Grundsätze sowie die grundrechtlichen Vorgaben konsequent auch auf Fallgestaltungen an, bei denen dies auf gewisse Schwierigkeiten stößt (wie im Rahmen der Datenverarbeitung im Internet) und macht sie auf diese Weise auch für eher neue Fragestellungen fruchtbar. Dass es hier mitunter in der Rechtsdurchsetzung zu Problemen kommen kann, ist nicht zu verkennen, jedoch per se kein Grund, das Recht nicht anzuwenden; im Gegenteil: Möglicherweise ist das Schutzbedürfnis der Betroffenen hier gerade besonders groß.

- Von besonderer Bedeutung ist auch der in der gesamten Rechtsprechung zum Ausdruck kommende sehr hohe Stellenwert, der dem Grundrechtsschutz eingeräumt wird. Dies impliziert auch, dass der grundrechtlich garantierte Persönlichkeitsschutz der Verfolgung durchaus legitimer öffentlicher oder privater Interessen Grenzen setzt, so dass diese „nicht um jeden Preis" verfolgt werden dürfen. Insofern wohnt den Grundrechten ein gewisser „Absolutheitsanspruch" inne, was übrigens nicht nur für die Gewährleistung des Kerngehalts der Grundrechte, sondern auch für die übrigen Anforderungen gilt.

- Gleichzeitig ist nicht zu verkennen, dass auch die datenschutz- bzw. grundrechtlichen Vorgaben eine Verfolgung wichtiger (insbesondere öffentlicher) Interessen keineswegs verunmöglichen. Nur sind in diesem Zusammenhang eben die auch in diesem Beitrag anhand der Rechtsprechung des EuGH erörterten Vorgaben bzw. Schranken zu beachten. Freilich schränken diese die Gestaltungsfreiheit des Gesetzgebers ein und führen möglicherweise zu einer gewissen „Ineffizienz". Diese ist aber der Preis für ein

---

[27] Vgl. im Übrigen im Einzelnen zu den Implikationen des Ansatzes des EuGH und damit gesamthaft zu den Anforderungen an die Unabhängigkeit der Kontrollstellen *Epiney*, Zu den Anforderungen an die Unabhängigkeit der Kontrollstellen im Bereich des Datenschutzes, Aktuelle Juristische Praxis 2010, 659 ff.

rechtsstaatliches System, dessen Grundprinzipien auch und gerade bei der Verfolgung bedeutender öffentlicher Interessen Sorge zu tragen ist.

Es lohnt sich m.E., sich diese Zusammenhänge immer wieder in Erinnerung zu rufen: Denn mitunter schlägt im Zuge emotionaler Diskussionen aufgrund bestimmter aktueller Ereignisse das Pendel in der politischen und manchmal auch rechtlichen Diskussion über Sinn und Unsinn von Datenschutz ohne nähere Reflexion der einschlägigen Rechtsprinzipien – die immerhin ein Kernelement jeden rechtsstaatlichen Gemeinwesens bilden – in die eine oder andere Richtung aus. Deutlich wird damit auch, dass eine nähere Analyse auch der Rechtsprechung des EuGH in diesem Zusammenhang zu einer Rationalisierung der entsprechenden Debatten beitragen kann.