„EU-Datenschutzrecht: Die Überprüfung der Richtlinie 95/46/EG und die vorgeschlagene Datenschutz-Grundverordnung“

Peter Hustinx[*]

1. Einführung

Das Konzept des „Datenschutzes“ wurde vor fast vier Jahrzehnten entwickelt, um natürlichen Personen rechtlichen Schutz vor dem unangemessenen Einsatz der Informationstechnologie bei der Verarbeitung sie betreffender Daten zu bieten. Es wurde nicht entwickelt, um die Verarbeitung solcher Informationen zu *verhindern* oder den Einsatz der Informationstechnologie grundsätzlich zu *beschränken*. Es wurde vielmehr erdacht, um Garantien für jegliche Verwendung der Informationstechnologie zur Verarbeitung von Daten über natürliche Personen zu bieten. Grundlage war die früh gewonnene Überzeugung, dass der intensive Einsatz der Informationstechnologie für diesen Zweck weitreichende Auswirkungen auf die Rechte und Interessen natürlicher Personen haben könnte.[1]

Mit anderen Worten: Beim Datenschutz ging es um die Rechte und Interessen natürlicher Personen und, trotz der verwendeten Terminologie, in der Hauptsache nicht um die diese Personen betreffenden Daten. Das Konzept wurde jedenfalls zu einer Zeit entwickelt, in der der allgegenwärtige Einsatz der Informationstechnologie noch in den Kinderschuhen steckte. Heute stellt sich die Lage völlig anders dar, und aufgrund des Internets und mobiler Geräte spüren wir die potenziellen Auswirkungen dieses Einsatzes unmittelbar, zu jeder Minute des Tages, und zwar sowohl in unserem Privatleben als auch im Beruf. Dieser Zustand dürfte sich in Zukunft noch verschärfen. Es ist daher durchaus angebracht, den derzeitigen Stand des EU-Datenschutzrechts in einem Kurs über EU-Recht und Technologie zu betrachten.

Ein weiterer Grund für die Relevanz des EU-Datenschutzrechts liegt darin, dass dessen derzeitiges Hauptinstrument, die Richtlinie 95/46/EG, auch als „Datenschutzrichtlinie“ bekannt, gegenwärtig einer umfassenden Überprüfung unterzogen wird, um sie wirksamer in einer Welt zu machen, in der die Informationstechnologie eine herausragende Rolle in allen

---

[*] Europäischer Datenschutzbeauftragter (2004-2014). Dieser Artikel stützt sich auf einen Kurs, der an der European University Institute's Academy of European Law, 24th Session on European Union Law, 1. bis 13. Juli 2013, gehalten wurde. Er baut ferner auf Material auf, das der Verfasser in den letzten Jahren in zahlreichen Artikeln und Reden verwendet hat, so z. B. P. J. Hustinx, „Gegevensbescherming in de informatiemaatschappij“, in E.J. Numan et al. (ed.), *Massificatie in het privaatrecht* (2010), S. 77-91, und P. Hustinx, „EU Data Protection Law – Current State and Future Perspectives“, Rede auf der Hochrangigen Konferenz: „Ethische Aspekte von Datenschutz und Privatsphäre“, Zentrum für Ethik, Universität Tartu / Datenschutzaufsichtsbehörde, Tallinn, Estland, 9. Januar 2013, abrufbar unter https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-01-09_Speech_Tallinn_DE.pdf (zuletzt aufgerufen am 31. Mai 2014). Der Verfasser dankt C. Docksey für seine Anmerkungen zu einem Entwurf dieses Artikels.

[1] Siehe weiter unten Abschnitt 2.

Bereichen des öffentlichen wie des privaten Lebens spielt. Diese Überprüfung nähert sich der letzten Phase des politischen Entscheidungsprozesses: Das Europäische Parlament und der Rat bereiten die Verhandlungen vor, in denen der künftige EU-Rechtsrahmen für den Datenschutz festgelegt wird, möglicherweise sogar für mehrere Jahrzehnte. Daher ist dies auch der geeignete Augenblick, um eine Bestandsaufnahme des EU-Datenschutzrechts vorzunehmen und sich etwas näher mit einigen Kernfragen zu beschäftigen.[2]

Angesichts des Umfelds der Überprüfung der Richtlinie gewinnt dieses Vorhaben noch weiter an Bedeutung. Abgesehen von dem dynamischen Charakter unseres digitalen Umfelds und dem Wunsch, von diesen Entwicklungen in einer digitalen Agenda zu profitieren, die zum Wirtschaftswachstum beiträgt, haben wir jüngst entdecken müssen, dass dieses Umfeld verletzlicher ist, als die meisten Menschen angenommen haben. Die Enthüllungen über die massive Ausspähung unseres Online-Verhaltens durch die amerikanische *National Security Agency* und andere Nachrichtendienste haben zu Recht Schockwellen um die ganze Welt ausgesandt. Gleichzeitig wurde damit aber auch klar, dass viele Online-Praktiken von Unternehmen, einschließlich einiger der beliebtesten, ebenfalls auf einer umfassenden Überwachung des Verbraucherverhaltens beruhen, und dass die um sich greifende Praxis, „kostenlose" Dienste gegen Überwachung anzubieten, der umfassenden Ausspähung durch andere Akteure Tür und Tor geöffnet hat. Die Überprüfung des EU-Rechtsrahmens für den Datenschutz findet daher in einem Kontext statt, in dem sowohl der Bedarf an einem wirksameren Schutz als auch die Probleme bei der Gewährleistung dieses Schutzes in der Praxis enorm gewachsen sind. Auch wenn es uns nicht gelingt, alle relevanten Fragen zu beantworten, könnte es hilfreich sein, sich mit einigen der Lösungen zu befassen, die derzeit zur Bewältigung dieser Probleme entwickelt werden.

Wir werden uns in diesem Artikel auch mit den Ursprüngen des EU-Datenschutzrechts und den Unterschieden zwischen „Privatsphäre" und „Datenschutz" beschäftigen, die zu seiner Weiterentwicklung beigetragen haben. Es ist notwendig, diese Punkte besser zu verstehen, um die Probleme einordnen zu können, die im Zusammenhang mit dem derzeitigen und dem künftigen Rechtsrahmen möglicherweise auftreten. Zwischen diesen beiden Konzepten bestehen aber auch wichtige Verbindungen. Privatsphäre und Datenschutz oder, genauer gesagt, das Recht auf *Achtung* des Privatlebens und das Recht auf den *Schutz* personenbezogener Daten sind beide recht junge Ausdrucksformen einer universellen Idee mit ziemlich ausgeprägten ethischen Dimensionen, nämlich der Würde, Autonomie und *Einzigartigkeit* jedes Menschen. Sie impliziert auch das Recht jedes Menschen, seine eigene Persönlichkeit zu entwickeln und ein Mitspracherecht in Angelegenheiten zu haben, die sich unmittelbar auf ihn auswirken. Dies erklärt zwei Aspekte, die in diesem Zusammenhang häufig auftauchen, nämlich die Notwendigkeit, unzulässige *Eingriffe* in Privatangelegenheiten zu verhindern, und die Notwendigkeit, natürlichen Personen eine

[2] Siehe weiter unten insbesondere die Abschnitte 5 bis 7.

angemessene *Kontrolle* über sie möglicherweise berührende Angelegenheiten zu gewährleisten.

Privatsphäre und Datenschutz als eigenständiger Rechtsbereich haben sich über die letzten vier Jahrzehnte auf europäischer Ebene entwickelt, zunächst vor allem beim Europarat, später dann im Wesentlichen im Kontext der Europäischen Union. Da die EU jedoch auf den Arbeiten des Europarats aufgebaut hat, werden wir, um ein vollständiges Bild zu erhalten, beide Entwicklungsstränge betrachten. Es lassen sich in diesem Überblick zwei große Linien erkennen: Bei der ersten geht es um die Entwicklung *stärkerer* Rechte in den Bereichen Privatsphäre und Datenschutz als solche, bei der zweiten um die Notwendigkeit, für eine *kohärentere* Anwendung dieser Rechte überall in der EU zu sorgen. Beide streben einen *wirksameren* Schutz in der Praxis und weniger *nicht gerade hilfreiche Vielfalt* in der Ausgestaltung des Schutzes in den Mitgliedstaaten an. Bei beiden Linien werden wir eine schrittweise Entwicklung in verschiedenen Phasen beobachten, in der sich nunmehr zunehmend die Auswirkungen der Charta der Grundrechte bemerkbar machen, sowohl in der Rechtsprechung des Gerichtshofs als auch bei der Überprüfung des bestehenden Rechtsrahmens. Da „Privatsphäre“ und „Datenschutz“ in der Charta als eigenständige Begriffe erwähnt werden, treten Probleme bei der Unterscheidung zwischen ihnen auf.

Dieser Artikel wird die Entwicklung weitgehend in chronologischer Abfolge schildern: Die Ursprünge des Datenschutzes und die Rolle des Europarats werden Gegenstand von Abschnitt 2 sein, die großen Züge der derzeitigen EU-Richtlinie Thema von Abschnitt 3. Nach einem Intermezzo in Abschnitt 4 zu verschiedenen institutionellen Aspekten, einschließlich der Charta und der Auswirkungen des Vertrags von Lissabon, werden wir uns in Abschnitt 5 dem Hintergrund und den wichtigsten Elementen der vorgeschlagenen Datenschutz-Grundverordnung zuwenden. In Abschnitt 6 werden wir auf einige der Hauptfragen eingehen, die im Zuge der Gesetzgebung erörtert werden, und Abschnitt 7 befasst sich mit anderen Fragen, die weiterer Überlegungen und Diskussionen bedürfen. Abschnitt 8 schließlich enthält einige Schlussbemerkungen.

2. Die Ursprünge des Datenschutzes

A. Privatsphäre und Privatleben

Erst nach dem Zweiten Weltkrieg fand das Konzept „Recht auf Privatsphäre“ Eingang in internationales Recht. Dies geschah zunächst in eher schwacher Fassung in Artikel 12 der Allgemeinen Erklärung der Menschenrechte[3], dem zufolge niemand *willkürlichen* Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr ausgesetzt werden darf.

[3] UN-Vollversammlung, Paris 1948.

Ein substanziellerer Schutz folgte in Artikel 8 der Europäischen Menschenrechtskonvention (EMRK)[4], dem zufolge jede Person das Recht auf *Achtung* ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz hat und eine Behörde in die Ausübung dieses Rechts nur eingreifen darf, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft für bestimmte wichtige und legitime Interessen notwendig ist.

Die Erwähnung von „Wohnung" und „Korrespondenz" konnte an verfassungsrechtliche Traditionen in vielen Ländern weltweit, als gemeinsames Erbe einer langen, gelegentlich Jahrhunderte alten Entwicklung, anknüpfen, aber der Fokus auf „Privatsphäre" und „Privatleben" war neu und eine offenkundige Reaktion auf die Ereignisse des Zweiten Weltkriegs.

Der Umfang und die Auswirkungen dieses Schutzes wurden durch den Europäischen Gerichtshof für Menschenrechte in einer Reihe von Urteilen erläutert.[5] In allen diesen Rechtssachen geht der Gerichtshof, um es kurz zu fassen, der Frage nach, ob ein *Eingriff* in das Recht auf Achtung des Privatlebens stattgefunden hat, und wenn ja, ob dieser auf einer *angemessenen*, also eindeutigen, zugänglichen und vorhersehbaren Rechtsgrundlage beruhte, und ob er für die fraglichen legitimen Interessen *notwendig* und verhältnismäßig war.

B. Datenschutz

Zu Beginn der 1970er-Jahre kam der Europarat zu dem Schluss, dass Artikel 8 EMRK vor dem Hintergrund neuer Entwicklungen, insbesondere im Hinblick auf den wachsenden Einsatz von Informationstechnologie, eine Reihe von Schwachstellen aufweise: Es werde nicht ganz klar, was genau unter „Privatleben" zu verstehen sei, es werde dem Schutz vor Eingriffen durch „Behörden" große Bedeutung beigemessen, und es fehle an einem eher proaktiven Ansatz, der auch einen möglichen Missbrauch personenbezogener Daten durch Unternehmen oder andere relevante Organisationen im privaten Sektor erfassen würde.[6]

Daraufhin formulierte das Ministerkomitee zwei Empfehlungen an die Mitgliedstaaten, alle erforderlichen Schritte zu ergreifen, um bestimmten Grundsätzen des Schutzes der Privatsphäre natürlicher Personen im nicht öffentlichen und öffentlichen Sektor Geltung zu verschaffen.[7] Dies fiel mit den ersten Initiativen auf nationaler Ebene in Ländern wie Deutschland und Schweden zusammen.[8]

---

[4] Europarat, Rom 1950.

[5] Siehe z. B. weiter unten Abschnitt 2 Teil D.

[6] Erläuterung zum Übereinkommen Nr. 108 (siehe weiter unten Fußnote 9), Absatz 4.

[7] Entschließung (73) 22 über den Schutz der Privatsphäre natürlicher Personen gegenüber elektronischen Datenbanken im nicht öffentlichen Sektor, und Entschließung (74) 29 über den Schutz der Privatsphäre natürlicher Personen gegenüber elektronischen Datenbanken im öffentlichen Bereich.

[8] Das erste einzelstaatliche Gesetz wurde 1972 in Schweden verabschiedet. Das deutsche Bundesland Hessen nahm das weltweit erste Datenschutzgesetz 1971 an. Auch die Vereinigten Staaten spielten seinerzeit eine führende Rolle mit der Formulierung sogenannter „fair information principles", die großen Einfluss auf die

Die positiven Erfahrungen mit diesen ersten Initiativen waren ein Anreiz für den Europarat, Zeit in die Ausarbeitung eines internationalen Abkommens als ersten rechtsverbindlichen Instruments zu diesem Thema zu investieren. Nach vier Jahren führte dies zur Annahme des Datenschutzübereinkommens, auch bekannt als Übereinkommen Nr. 108[9], das bisher von 46 Staaten ratifiziert worden ist, darunter alle EU-Mitgliedstaaten, die meisten Mitgliedstaaten des Europarats, und ein Nichtmitgliedstaat.[10]

Zweck dieses Übereinkommens ist es gemäß Artikel 1, „im Hoheitsgebiet jeder Vertragspartei für jedermann ungeachtet seiner Staatsangehörigkeit oder seines Wohnortes sicherzustellen, dass seine Rechte und Grundfreiheiten, insbesondere seine Rechte auf einen Persönlichkeitsbereich, bei der automatischen Verarbeitung personenbezogener Daten geschützt werden („Datenschutz“).[11] Der Begriff „personenbezogene Daten“ wird definiert als „alle Daten, die sich auf eine bestimmte oder bestimmbare Person beziehen („Betroffener“).[12]

Der Begriff „Datenschutz“ ist also breiter gefasst als „Schutz der Privatsphäre“, da er sich auch auf andere Grundrechte und -freiheiten sowie alle Arten von Daten bezieht, *unabhängig* davon, ob sie die Privatsphäre betreffen oder nicht. Gleichzeitig ist der Begriff *enger gefasst*, da er sich nur auf die Verarbeitung personenbezogener Daten bezieht und andere Aspekte des Schutzes der Privatsphäre unberücksichtigt bleiben.

Es sei in diesem Zusammenhang darauf hingewiesen, dass heutzutage viele Tätigkeiten im öffentlichen oder auch privaten Sektor auf die eine oder andere Weise mit der Erhebung und Verarbeitung personenbezogener Daten im Zusammenhang stehen. Das eigentliche Ziel des Übereinkommens besteht daher darin, den Einzelnen (Bürger, Verbraucher, Arbeitnehmer usw.) vor der ungerechtfertigten Erhebung, Speicherung, Verwendung und Weitergabe seiner personenbezogenen Daten zu schützen. Betroffen sein kann auch ihre öffentliche oder nicht öffentliche Teilhabe an sozialen Beziehungen, und es kann um den Schutz der freien Meinungsäußerung sowie um die Verhinderung unfairer Diskriminierung und die Förderung des „Fair Play“ in Prozessen der Entscheidungsfindung gehen. Schließlich strebte das Übereinkommen an, die Achtung des Persönlichkeitsbereichs und des freien Informationsaustausches in Einklang zu bringen.[13]

---

internationale Debatte hatten. Siehe den Bericht „*Records, Computers and the Rights of Citizens”*, US Department of Health, Education and Welfare, 1973, und den 1974 angenommenen *Privacy Act*.

[9] Übereinkommen zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten, Straßburg, 28. Januar 1981, SEV 108.

[10] Im April 2013 ratifizierte Uruguay als erster Nichtmitgliedstaat das Übereinkommen.

[11] Artikel 1.

[12] Artikel 2 Buchstabe a.

[13] Präambel, Absatz 4.

C. Strukturelle Garantien

Das Übereinkommen enthält eine Reihe von Grundsätzen für den Datenschutz, die von den Vertragsparteien in ihr innerstaatliches Recht umgesetzt werden müssen, bevor das Übereinkommen für sie in Kraft tritt.[14] Diese Grundsätze bilden noch immer den Kern jeglicher einzelstaatlicher Rechtsvorschriften in diesem Bereich. Das Übereinkommen besagt: Personenbezogene Daten müssen „nach Treu und Glauben und auf rechtmäßige Weise beschafft sein und verarbeitet werden", „für festgelegte und rechtmäßige Zwecke gespeichert sein und dürfen nicht so verwendet werden, dass es mit diesen Zwecken unvereinbar ist", und sie müssen „so aufbewahrt werden, dass der Betroffene nicht länger identifiziert werden kann, als es die Zwecke, für die sie gespeichert sind, erfordern". Personenbezogene Daten müssen ferner „den Zwecken, für die sie gespeichert sind, entsprechen, dafür erheblich sein und dürfen nicht darüber hinausgehen", und sie müssen „sachlich richtig und wenn nötig auf den neuesten Stand gebracht sein".[15]

Noch strengere Bedingungen sieht das Übereinkommen für „besondere Arten von Daten" vor.[16] Dieser Bestimmung zufolge dürfen „personenbezogene Daten, welche die rassische Herkunft, politische Anschauungen oder religiöse oder andere Überzeugungen erkennen lassen, sowie personenbezogene Daten, welche die Gesundheit oder das Sexualleben betreffen", nur verarbeitet werden, wenn das innerstaatliche Recht einen geeigneten Schutz gewährt. Dasselbe gilt für personenbezogene Daten über Strafurteile.

Weitere Grundsätze des Übereinkommens sind „geeignete Sicherungsmaßnahmen"[17] und „zusätzlicher Schutz für den Betroffenen" wie das Recht auf Auskunft über die eigenen personenbezogenen Daten, das Recht, gegebenenfalls diese Daten berichtigen oder löschen zu lassen, und das Recht auf Rechtsmittel, wenn diese Rechte nicht gewahrt werden.[18] Ursprünglich war das Konzept der „unabhängigen Kontrolle" in dem Übereinkommen nicht enthalten, wurde aber in der Praxis weitgehend angewendet und dem Übereinkommen später im Wege eines Protokolls hinzugefügt.[19]

Um es noch einmal klar zu sagen: Ausgangspunkt des Übereinkommens ist *nicht*, dass die Verarbeitung personenbezogener Daten immer als *Eingriff* in das Recht auf Privatsphäre zu betrachten ist, sondern dass zum Schutz der Privatsphäre sowie anderer Grundrechte und

[14] Artikel 4.
[15] Artikel 5.
[16] Artikel 6.
[17] Artikel 7.
[18] Artikel 8.
[19] Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr, Straßburg, 8. November 2001, siehe insbesondere Artikel 1. Dies war im Wesentlichen auf die einschlägigen Bestimmungen der Richtlinie 95/46/EG zurückzuführen (siehe weiter unten Abschnitt 3 Teil B).

-freiheiten bei jeder Verarbeitung personenbezogener Daten *immer* bestimmte rechtliche Rahmenbedingungen zu beachten sind. Dies kommt beispielsweise in dem Grundsatz zum Ausdruck, dass personenbezogene Daten nur für festgelegte rechtmäßige Zwecke verarbeitet werden dürfen, diesen Zwecken entsprechen müssen und nicht so verwendet werden dürfen, dass es mit diesen Zwecken unvereinbar ist.

Gemäß diesem Ansatz wurden die Schlüsselelemente von Artikel 8 EMRK, etwa der Eingriff in die Ausübung des Rechts auf Privatsphäre nur, soweit gesetzlich vorgesehen und soweit für einen rechtmäßigen Zweck vorgesehen, in einen allgemeineren Kontext übernommen. Ausnahmen von diesen Grundsätzen sind nach dem Übereinkommen nicht zulässig, nur unter ähnlichen Bedingungen wie beim Recht auf Privatsphäre selbst.[20]

Es sollte klar sein, dass dies in der Praxis nur dann gut funktioniert, wenn das im Übereinkommen vorgesehene System von Kontrolle und Gegenkontrolle – bestehend aus materiellen Bedingungen, individuellen Rechten, Verfahrensbestimmungen und unabhängiger Kontrolle – hinreichend flexibel ist, um unterschiedliche Gegebenheiten berücksichtigen zu können, und wenn es pragmatisch und mit gutem Blick für die Interessen der Betroffenen und anderer wichtiger Interessengruppen angewendet wird. Bei diesem Ansatz spielt das in Artikel 8 EMRK angeführte Recht auf Achtung des Privatlebens nach wie vor eine wichtige Rolle im Hintergrund, unter anderem bei der Bestimmung der Rechtmäßigkeit bestimmter, einen größeren Eingriff darstellender Maßnahmen.

Dem Übereinkommen kommt in den meisten Mitgliedstaaten des Europarates bei der Ausgestaltung ihrer Rechtssetzungspolitik große Bedeutung zu. Vor diesem Hintergrund galt das Thema „Datenschutz“ von Anfang an als Frage von großer struktureller Bedeutung für eine moderne Gesellschaft, in der die Verarbeitung personenbezogener Daten eine zunehmend wichtige Rolle spielt. Das Übereinkommen wird derzeit überarbeitet; wir werden später noch darauf zurückkommen.

D. Andere Aspekte

Nach der Annahme des Übereinkommens Nr. 108 spielte der Europarat weiterhin eine wichtige Rolle bei der Ausarbeitung einer Reihe von Empfehlungen durch das Ministerkomitee zur Anwendung des Übereinkommens in verschiedenen Bereichen. Dabei kam es zu wichtigen Klarstellungen einiger Kernbestimmungen.[21] Diese Empfehlungen

[20] Artikel 9.

[21] So wird beispielsweise in der Empfehlung Nr. R (83) 10 zum Schutz personenbezogener Daten für Zwecke der wissenschaftlichen Forschung und Statistik unter Punkt 1.2 das Konzept “personenbezogene Daten” klargestellt, wo es heißt, dass eine Person nicht als „bestimmbar“ gilt, wenn eine Bestimmung einen unverhältnismäßig großen Aufwand an Zeit, Geld oder Arbeitskraft erfordert. Im erläuternden Bericht zum Übereinkommen heißt es eher vage, eine „bestimmbare Person“ sei eine Person, die „leicht zu bestimmen“ sei. Nicht abgedeckt hierdurch ist die „Bestimmung von Personen mit sehr ausgefeilten Methoden” (Nr. 28).

haben den einzelstaatlichen Rechtsvorschriften den Weg bereitet und waren wichtige Eckpunkte für andere internationale Abkommen.[22]

Es war nicht beabsichtigt, dass die Bestimmungen des Übereinkommens unmittelbar anwendbar sein oder der gerichtlichen Kontrolle durch den EMRG unterliegen sollten. Seit 1997 hat der Europäische Gerichtshof für Menschenrechte jedoch in einer Reihe von Rechtssachen geurteilt, dass der Schutz personenbezogener Daten von „grundlegender Bedeutung" ist, damit eine Person das Recht auf Achtung vor dem Privatleben gemäß Artikel 8 EMRK wahrnehmen kann, und hat aus dem Übereinkommen Maßstäbe für die Beantwortung der Frage abgeleitet, inwieweit dieses Recht verletzt wurde.[23] Dies lässt darauf schließen, dass der Gerichtshof zunehmend geneigt ist, die Einhaltung des Übereinkommens, zumindest im Hinblick auf „sensible Daten", vor dem Hintergrund von Artikel 8 EMRK zu bewerten.

Dies führt aber auch zu der Frage, inwieweit die Schwachstellen von Artikel 8 EMRK, die die Annahme des Übereinkommens Nr. 108 zur Folge hatten, noch immer bestehen. Das Konzept „Privatleben" in Artikel 8 ist zwar noch immer nicht ganz klar, doch hat sich sein Anwendungsbereich erheblich erweitert.[24] Gemäß der Rechtsprechung des Gerichtshofs ist es nicht auf „intime" Situationen beschränkt, sondern deckt auch bestimmte Aspekte des beruflichen Lebens und des Verhaltens in der Öffentlichkeit ab, ob nun in der Vergangenheit oder nicht. Auf der anderen Seite betreffen diese Fälle häufig konkrete Situationen, bei denen es um sensible Daten (medizinische oder soziale Dienstleistungen), berechtigte Erwartungen an den Schutz der Privatsphäre (vertrauliche Nutzung des Telefons oder E-Mail am Arbeitsplatz) oder Untersuchungen durch Polizei oder Geheimdienste geht. Bisher hat der Gerichtshof noch nie befunden dass *jede* Verarbeitung personenbezogener Daten – *unabhängig* von ihrer Art oder ihres Kontexts – in den Anwendungsbereich von Artikel 8 EMRK fällt.[25] Das Übereinkommen dient daher lediglich als weitere Quelle von Standards für die Bewertung eines Verhaltens im Anwendungsbereich dieser Bestimmung.

---

[22] Die Empfehlung Nr. (87) 15 über die Nutzung personenbezogener Daten im Polizeibereich diente als Orientierung für das Datenschutzniveau bei Europol (siehe Artikel 14 des Übereinkommens, gestützt auf Artikel K.3 des EU-Vertrags, über die Errichtung eines Europäischen Polizeiamtes (Europol-Übereinkommen) und Erwägungsgrund 14 des derzeitigen Europol-Beschlusses 2009/371/JI des Rates).

[23] Siehe z. B. *Z / Finnland*, Beschwerde 22009/93, EGMR 1997-I, Randnr. 95.

[24] Siehe z. B. *Klass / Deutschland*, EGMR (1978), A-28; *Malone / Vereinigtes Königreich*, EGMR (1984), A-82; *Leander / Schweden*, EGMR (1987), A-116; *Gaskin / Vereinigtes Königreich*, EGMR (1989), A-160; *Niemietz / Deutschland*, EGMR (1992), A-251-B; *Halford / Vereinigtes Königreich*, EGMR 1997-IV; *Amann / Schweiz*, EGMR 2000-II, und *Rotaru / Rumänien*, EGMR 2000-V.

[25] Auch wenn dies mitunter etwas unklar formuliert ist, so z. B. in *Khelili / Schweiz*, 18.10.2011, Beschwerde 16188/07, Randnr. 56: „Die Speicherung von Daten *über das Privatleben der Beschwerdeführerin*, u. a. über ihren Beruf, und deren Aufbewahrung kamen einem Eingriff im Sinne von Artikel 8 gleich, *weil es sich um personenbezogene Daten über eine bestimmte oder bestimmbare natürliche Person handelte*" (Hervorhebung durch uns). Der Fall betraf jedoch die Aufbewahrung von Daten einschließlich der Bezeichnung der Beschwerdeführerin als Prostituierte durch die Polizei über einen langen Zeitraum und ohne faktische Grundlage. Im selben Urteil befand der Gerichtshof ferner, dass die Frage, ob die Aufbewahrung personenbezogener Daten Aspekte des Schutzes des Privatlebens berühre, von dem konkreten Zusammenhang

Der Gerichtshof hat nunmehr in einem Urteil zum Ausdruck gebracht, dass Artikel 8 EMRK positive Verpflichtungen für die Mitgliedstaaten bedeuten könnte und dass diese daher für eine Verletzung der Privatsphäre durch eine private Partei haftbar gemacht werden können.[26] Die Anzahl einschlägiger Rechtssachen ist jedoch noch ziemlich begrenzt und bedeutet keine allgemeine Verpflichtung für die Mitgliedstaaten, den Schutz personenbezogener Daten in horizontalen Beziehungen zu gewährleisten. Das Übereinkommen spielt daher in diesem Zusammenhang auch weiterhin eine sinnvolle ergänzende Rolle.

Nur wenige Jahre nach der Annahme des Übereinkommens Nr. 108 erließ das Bundesverfassungsgericht in Deutschland eine Entscheidung, in der es ein Recht auf „informationelle Selbstbestimmung" als Ausdruck des in Artikel 2 Absatz 1 GG verankerten Rechts auf freie Entfaltung der Persönlichkeit formulierte.[27] Nach diesem Ansatz gilt jede Verarbeitung personenbezogener Daten grundsätzlich als Eingriff in das Recht auf informationelle Selbstbestimmung, sofern die betroffene Person nicht ihre Zustimmung gegeben hat. Diese Entscheidung hat sehr großen Einfluss gehabt, und zwar nicht nur in Deutschland, sondern auch anderswo in Europa. Dieser Ansatz sollte allerdings klar von dem des Übereinkommens Nr. 108 und damit, wie wir noch sehen werden, auch von dem der Richtlinie 95/46/EG und der einschlägigen Bestimmungen der EU-Charta unterschieden werden.

Wenige Monate vor der Annahme des Übereinkommens Nr. 108 verabschiedete die OECD Leitlinien für den Schutz der Privatsphäre, die zwar nicht rechtsverbindlich waren, aber doch auch großen Einfluss hatten, insbesondere in nicht europäischen Ländern wie den Vereinigten Staaten, Kanada, Australien und Japan.[28] Die Leitlinien enthielten eine Reihe grundlegender Prinzipien, die in enger Abstimmung mit dem Europarat aufgestellt worden waren und daher mit den Datenschutzgrundsätzen im Übereinkommen Nr. 108 harmonierten. Im Detail gab es allerdings recht subtile, aber bedeutungsschwere Unterschiede. Der Anwendungsbereich der Leitlinien beschränkte sich auf personenbezogene Daten, „die aufgrund der Art ihrer Verarbeitung oder aufgrund ihrer Art oder des Zusammenhangs, in dem sie verwendet werden, die Privatsphäre und Freiheiten der Person gefährden".[29] Implizit wurde der Begriff „Risiko" hier zu einer *Schwellenwert*-Bedingung für den Schutz, was mit dem grundrechtegestützten Ansatz des Europarates nicht in vollem Umfang vereinbar war. Des

---

abhänge, in dem diese Daten erhoben und gespeichert worden seien, um welche Art von Daten es sich handle, wie sie verarbeitet und verwendet würden und welche Folgen dies haben könne (siehe Randnr. 55).

[26] Siehe z. B. *von Hannover / Deutschland*, EGMR 2004-VI, und *K.U. / Finnland*, Beschwerde 2872/02, EGMR 2008-V.

[27] Urteil vom 15. Dezember 1983, BVerfGE 65, 1-71, *Volkszählung*.

[28] OECD, Empfehlung des Rates für Leitlinien für den Schutz der Privatsphäre und den grenzüberschreitenden Verkehr personenbezogener Daten, Paris, 23. September 1980, abrufbar unter: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (zuletzt aufgerufen am 31. Mai 2014).

[29] Leitlinien, Absatz 2.

Weiteren fehlten in den Leitlinien das Erfordernis eines *rechtmäßigen* Zwecks und einer *gesetzlichen* Grundlage für die Verarbeitung personenbezogener Daten ganz generell.[30] Beide Aspekte stehen im Zusammenhang mit Fragen, die in den weltweiten Diskussionen noch immer eine sehr wichtige Rolle spielen.

3. Die Richtlinie 95/46/EG

A. Harmonisierung

Auch wenn der Europarat mit großem Erfolg das Thema „Datenschutz" auf die Tagesordnung gesetzt und die maßgeblichen Elemente eines Rechtsrahmens festgelegt hatte, war er weniger erfolgreich darin, für mehr Kohärenz in seinen Mitgliedstaaten zu sorgen. Einige Mitgliedstaaten haben das Übereinkommen Nr. 108 erst verspätet umgesetzt, und diejenigen, die es umgesetzt haben, gelangten zu unterschiedlichen Ergebnissen, was in einigen Fällen sogar zu Beschränkungen des Datenverkehrs mit anderen Mitgliedstaaten führte.

Aus diesem Grund hatte die Europäische Kommission große Bedenken, dass sich diese fehlende Kohärenz negativ auf die Entwicklung des Binnenmarkts in verschiedenen Bereichen – u. a. den freien Personen- und Dienstleistungsverkehr – auswirken könnte, in denen die Verarbeitung personenbezogener Daten eine zunehmend wichtige Rolle spielen sollte. Ende 1990 legte sie daher einen Vorschlag für eine Richtlinie zur Harmonisierung der nationalen Rechtsvorschriften im Bereich des Datenschutzes im privaten und in weiten Teilen des öffentlichen Sektors vor. [31]

Nach vierjährigen Verhandlungen führte dies zur Annahme der aktuellen Richtlinie 95/46/EG[32], die zweierlei Ziele verfolgt. Erstens verpflichtet sie alle Mitgliedstaaten, die Grundrechte und -freiheiten natürlicher Personen, insbesondere das Recht auf Schutz der Privatsphäre, bei der Verarbeitung personenbezogener Daten, im Einklang mit der Richtlinie zu schützen. Zweitens verpflichtet sie sie, den freien Verkehr personenbezogener Daten zwischen den Mitgliedstaaten aus Gründen, die mit diesem Schutz in Zusammenhang stehen, weder einzuschränken noch zu untersagen.[33] Beide Auflagen stehen in enger Beziehung

---

[30] Siehe Leitlinien, Absatz 7: „Daten sollten *auf rechtmäßige Weise und nach Treu und Glauben* und *gegebenenfalls* mit dem Wissen oder der Einwilligung der betroffenen Person erhoben werden." (Hervorhebung durch uns)

[31] KOM (90) 314 endgültig – SYN 287 und 288, 13. September 1990, S. 4: „Die Vielfalt nationaler Ansätze und das Fehlen eines Schutzsystems auf Gemeinschaftsebene behindern die Vollendung des Binnenmarktes. Werden die Grundrechte betroffener Personen, insbesondere ihr Recht auf Privatsphäre, auf Gemeinschaftsebene nicht gewahrt, könnte der grenzüberschreitende Datenverkehr behindert werden".

[32] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Bearbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, S. 31.

[33] Siehe Erwägungsgründe 7 bis 10 und Artikel 1.

zueinander. Sie zielen darauf ab, in allen Mitgliedstaaten ein gleich hohes Maß an Schutz zu bewirken, um eine ausgewogene Entwicklung des Binnenmarktes zu erreichen.

Damit gründete die Richtlinie auf den im Übereinkommen Nr. 108 des Europarates niedergelegten Grundprinzipien des Datenschutzes.[34] Gleichzeitig konkretisierte sie diese Grundsätze und ergänzte sie durch weitere Anforderungen und Bedingungen. Da in die Richtlinie jedoch allgemein formulierte Konzepte und offene Standards übernommen wurden, verfügten die Mitgliedstaaten bei ihrer Umsetzung immer noch über einen recht breiten Ermessensspielraum.[35] Im Ergebnis hat die Richtlinie zu mehr Kohärenz zwischen Mitgliedstaaten geführt, gewiss aber nicht zu identischen oder vollständig übereinstimmenden Lösungen.

B. Anwendungsbereich und Gegenstand

Die derzeitige Richtlinie hat einen breit gefassten Anwendungsbereich: Sie gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen.[36] Es gibt zwei Ausnahmen: Erstens Verarbeitungen, die nicht in den Anwendungsbereich des Gemeinschafts- bzw. jetzt des Unionsrechts fallen, und auf keinen Fall Verarbeitungen, die die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates oder Strafverfolgung betreffen, und zweitens Verarbeitungen durch eine natürliche Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.[37] Die Definitionen von Begriffen wie „Verarbeitung“ und „personenbezogene Daten“ kommen denen im Übereinkommen Nr. 108 sehr nahe.[38]

Die Richtlinie folgt den im Übereinkommen aufgestellten Grundprinzipien für den Datenschutz, sieht aber sechs Kriterien für die Zulässigkeit der Datenverarbeitung vor, die es im Übereinkommen nicht gibt.[39] Demzufolge dürfen personenbezogene Daten nur verarbeitet werden, wenn die betroffene Person *ohne jeden Zweifel* ihre Einwilligung gegeben hat, wenn die Verarbeitung für die Erfüllung eines Vertrags *erforderlich* ist, dessen Vertragspartei die

[34] Siehe insbesondere Erwägungsgrund 11.
[35] Siehe Erwägungsgrund 9 und Artikel 5.
[36] Artikel 3 Absatz 1.
[37] Artikel 3 Absatz 2.
[38] Artikel 2 Buchstaben a und b. Zum zweiten Thema Näheres in: Artikel 29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, angenommen am 20. Juni 2007 (WP 136), abrufbar unter. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf (zuletzt aufgerufen am 31. Mai 2014).
[39] Artikel 7. Siehe in diesem Zusammenhang Artikel 29-Datenschutzgruppe, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011 (WP 187), und Stellungnahme 6/2014 zum Begriff „legitime Interessen des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG“, angenommen am 9. April 2014 (WP 217), abrufbar unter:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_de.pdf (zuletzt aufgerufen am 31. Mai 2014).
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_de.pdf (zuletzt aufgerufen am 31. Mai 2014).

betroffene Person ist, zur Erfüllung einer rechtlichen Verpflichtung, für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, zur Wahrung lebenswichtiger Interessen der betroffenen Person, oder zur Verwirklichung der berechtigten Interessen des für die Verarbeitung Verantwortlichen, sofern nicht das Interesse der betroffenen Person überwiegt. Hierzu ist eine genaue Prüfung der verschiedenen Phasen der Datenverarbeitung erforderlich und müssen für die Verarbeitung Verantwortliche die Ergebnisse dieser Prüfung zum richtigen Zeitpunkt berücksichtigen.

In der Richtlinie sind ferner die Bedingungen für die Verarbeitung besonderer Kategorien sensibler Daten festgelegt.[40] Ausgangspunkt ist ein *Verbot* mit bestimmten Ausnahmen: entweder die *ausdrückliche* Einwilligung der betroffenen Person oder die Einhaltung spezifischer Bedingungen wie Verarbeitung von Gesundheitsdaten zum Zweck der Gesundheitsvorsorge. Andere Ausnahmen können auf einzelstaatlicher Ebene vorgesehen werden, jedoch nur aus Gründen eines „wichtigen öffentlichen Interesses" und „vorbehaltlich angemessener Garantien". Um sicherzustellen, dass diese Möglichkeit nur eingeschränkt genutzt wird, sieht die Richtlinie eine entsprechende Meldung an die Kommission vor.

Die Richtlinie sieht ferner für den für die Verarbeitung Verantwortlichen die Verpflichtung vor, der betroffenen Person, sofern ihr diese Angaben noch nicht vorliegen, angemessene Informationen über seine Identität, den Zweck der Verarbeitung und andere wichtige Aspekte zukommen zu lassen, sofern diese Informationen unter Berücksichtigung der spezifischen Umstände, unter denen die Daten erhoben werden, „notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten".[41] Wird eine solche Transparenz nicht hergestellt, kann dies bedeuten, dass Daten unrechtmäßig erhoben werden, mit allen entsprechenden Folgen.

Die Richtlinie sieht weiter die Einrichtung von Kontrollstellen vor, die die Einhaltung der einzelstaatlichen Rechtsvorschriften im jeweiligen Hoheitsgebiet überwachen, und die eine Reihe besonderer Aufgaben und Befugnisse haben, die sie „in völliger Unabhängigkeit" wahrnehmen.[42] Je nachdem, wie die Richtlinie in einzelstaatliches Recht umgesetzt wurde, können dazu Vorabkontrolle oder Konsultation[43], die Bearbeitung von Beschwerden, Inspektionen und andere Durchsetzungstätigkeiten gehören. Diese Stellen arbeiten bei der Wahrnehmung ihrer Aufgaben zusammen, und zwar entweder bilateral oder im Rahmen der „Artikel 29-Datenschutzgruppe", die auf EU-Ebene als unabhängiges beratendes Gremium wirkt.[44]

[40] Artikel 8.
[41] Artikel 10 und 11.
[42] Artikel 28.
[43] Artikel 18 bis 20.
[44] Artikel 29 und 30, in denen auch der Europäische Datenschutzbeauftragte als Mitglied dieser Gruppe erwähnt wird.

Der territoriale Anwendungsbereich der Richtlinie erstreckt sich auf die Verarbeitungen personenbezogener Daten, die im Rahmen der Tätigkeiten einer Niederlassung des für die Verarbeitung Verantwortlichen im Hoheitsgebiet eines EU-Mitgliedstaats durchgeführt werden.[45] An welchem Ort die Datenverarbeitung stattfindet, ist in diesem Zusammenhang unerheblich. Dieses Kriterium ist auch für den Anwendungsbereich einzelstaatlichen Rechtsvorschriften innerhalb der EU von Belang. Besitzt der für die Verarbeitung Verantwortliche keine Niederlassung in der EU, findet das Recht des Mitgliedstaats Anwendung, in dem sich die für die Datenverarbeitung verwendeten Mittel befinden.[46]

Darüber hinaus folgt die Richtlinie dem Grundsatz, dass personenbezogene Daten nur an Drittstaaten übermittelt werden dürfen, die ein angemessenes Schutzniveau gewährleisten. Ist ein solcher Schutz nicht gegeben, ist eine Übermittlung nur unter bestimmten Bedingungen zulässig, entweder auf der Grundlage einer Ausnahme oder wenn in Verträgen oder anderen einschlägigen Instrumenten angemessene Garantien gewährleistet wurden.[47]

Diese Bestimmungen stoßen heute auf eine komplexe Wirklichkeit, in der sich – sowohl innerhalb der EU als auch mit Blick auf Drittstaaten – immer häufiger die Frage stellt, welches Recht anwendbar und wer für dessen Einhaltung zuständig ist. Dies wirft auch neue Fragen in Bezug auf das Internet – betreffend die Position von Websites, Suchmaschinen[48], sozialen Netzen und moderner Werbetechnologie – sowie den Datenverkehr innerhalb multinationaler Konzerne, das Outsourcing von Dienstleistungen und Cloud-Computing auf. In der Praxis wird ein angemessener Schutz zunehmend in Form „verbindlicher unternehmensinterner Vorschriften“ gewährleistet, von Verhaltenskodizes, die von Unternehmen unterschrieben werden, den spezifischen Anforderungen genügen und von den zuständigen Kontrollstellen als ausreichend effektiv akzeptiert werden.[49]

---

[45] Artikel 4. Siehe EuGH in der Rechtssache C-131/12, *Google Spain*, 13. Mai 2014, noch nicht veröffentlicht, Randnrn. 55-56. Siehe auch weiter unten Abschnitt 6 Teil D.

[46] Siehe hierzu im Einzelnen Artikel 29-Datenschuzgruppe, Stellungnahme 8/2010 zum anwendbaren Recht, angenommen am 16. Dezember 2010 (WP 179), abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_de.pdf (zuletzt aufgerufen am 31. Mai 2014)

[47] Artikel 25 und 26. Auf dieser Grundlage hat die Europäische Kommission eine Reihe von Drittstaaten mit einem angemessenen Schutzniveau anerkannt und Vertragsklauseln angenommen, die in konkreten Fällen angemessenen Schutz bieten können. Nähere Informationen hierzu auf der Website der Europäischen Kommission und der Artikel 29-Datenschutzgruppe: http://ec.europa.eu/justice/data-protection/index_en.htm (zuletzt aufgerufen am 31. Mai 2014)

[48] Siehe z. B *Google Spain* (Fußnote 45), dem zufolge der Betreiber einer Suchmaschine ein für die Verarbeitung Verantwortlicher ist und die Einhaltung des EU-Datenschutzrechts zu gewährleisten hat (siehe Randnrn. 33 und 38). Siehe auch weiter unten Abschnitt 6 Teil D.

[49] Gemäß Artikel 26 Absatz 2 können sich angemessene Garantien „insbesondere“ aus angemessenen Vertragsklauseln ergeben, sind andere Instrumente jedoch nicht ausgeschlossen. Weitere Informationen zu verbindlichen unternehmensinternen Vorschriften finden sich auf der in Fußnote 44 erwähnten Website.

Die Notwendigkeit, die Achtung vor der Privatsphäre und den freien Datenverkehr miteinander zu vereinbaren, was eines der Ziele des Übereinkommens Nr. 108 ist und auch an den Zielen der Richtlinie deutlich wird, führte letztendlich zu einer besonderen Bestimmung, die von den Mitgliedstaaten verlangt, für die Verarbeitung personenbezogener Daten, die „allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt", insofern potenziell sehr breit gefasste Abweichungen oder Ausnahmen von bestimmten Bestimmungen vorzusehen, als sich dies als notwendig erweist, um das Recht auf Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen.[50]

C. Einschlägige Rechtsprechung

Alle EU-Mitgliedstaaten haben die Richtlinie in einzelstaatliches Recht umgesetzt, auch die neuen Mitgliedstaaten, bei denen die Umsetzung eine Bedingung für den Beitritt darstellte, sowie alle Nicht-EU-Vertragsstaaten des EWR. Mittlerweise hat die Kommission mehrere gerichtliche Klagen wegen nicht ordnungsgemäßer Umsetzung der Richtlinie angestrengt. Die erste Klage richtete sich gegen den Mitgliedstaat mit der längsten Erfahrung in diesem Bereich, nämlich Deutschland. Im März 2010 urteilte der Gerichtshof, die geforderte „vollständige Unabhängigkeit" einer Kontrollstelle bedeute, dass diese frei von *jedem* äußeren Einfluss sein müsse.[51] Diese Auffassung wurde in der jüngeren Vergangenheit in Rechtssachen gegen Österreich und Ungarn bekräftigt und näher erläutert.[52]

Auch zu anderen Aspekten des bestehenden Rechtsrahmens für den Schutz personenbezogener Daten hat der Gerichtshof wichtige Urteile gefällt. In seinen ersten Urteilen zur Richtlinie 95/46/EG befand der Gerichtshof beispielsweise, sie habe einen breiten Anwendungsbereich, der nicht in jedem Einzelfall zwingend mit dem Binnenmarkt verknüpft sei.[53] Somit sei die Richtlinie auch auf Streitfälle im öffentlichen Sektor eines einzelnen Mitgliedstaats oder auf die Website einer Kirche oder einer Stiftung für wohltätige Zwecke anwendbar. Im letztgenannten Fall wurde ferner deutlich, dass die Richtlinie grundsätzlich auch für das Internet gilt, selbst wenn die Verfügbarkeit personenbezogener Daten auf einer Website an sich nicht bedeutet, dass die Bestimmungen über den Datenverkehr mit Drittländern anwendbar sind.[54] Die genauen Konsequenzen dieser Schlussfolgerung sind noch nicht ganz klar.

[50] Artikel 9.
[51] Rechtssache C-518/07, *Kommission / Deutschland*, [2010] Slg. I-01885, Randnr. 30.
[52] Rechtssache C-614/10, *Kommission / Österreich*, 16. Oktober 2012, und Rechtssache C-288/12, *Kommission / Ungarn*, 8. April 2014, beide noch nicht veröffentlicht.
[53] Verbundene Rechtssachen C-465/00, C-138/01 und C-139/01, *Österreichischer Rundfunk*, [2003] Slg. I-04989, Randnrn. 41-43, und Rechtssache C-101/01, *Bodil Lindqvist*, [2003] Slg. I-12971, Randnrn. 39-41.
[54] *Bodil Lindqvist*, Randnrn. 24-27 und 56-71.

Ist die Richtlinie auf einen Bereich innerhalb des Anwendungsbereichs von Artikel 8 EMRK anwendbar, ist sie im Einklang mit dieser Bestimmung auszulegen.[55] In diesem Zusammenhang hat der Gerichtshof zwischen Verarbeitungstätigkeiten unterschieden, die Artikel 8 EMRK möglicherweise verletzen oder nicht verletzen. Der erste Fall bezog sich auf eine einzelstaatliche Rechtsvorschrift, der zufolge Arbeitgeber verpflichtet sind, einer staatlichen Stelle bestimmte Lohndaten vorzulegen. Die Verarbeitung derselben Daten durch den Arbeitgeber für Beschäftigungszwecke warf keine Grundsatzfragen auf, sofern die Datenschutzvorschriften eingehalten wurden.[56] Dies fügt sich in die bereits erwähnte Unterscheidung zwischen „Privatsphäre" und „Datenschutz" im Verlauf der Rechtsentwicklung ein.

Die Ausnahme für Datenverarbeitungen im Zusammenhang mit öffentlicher Sicherheit und strafrechtlicher Verfolgung wurde vom Gerichtshof in einem größeren Fall angewandt, in dem es um die Übermittlung von Fluggastdaten an die USA zu Grenzschutzzwecken nach den terroristischen Attentaten am 11. September 2001 ging.[57] In anderen Rechtssachen vertrat der Gerichtshof die Auffassung, dass die Ausnahme für die Verarbeitung personenbezogener Daten durch eine natürliche Person im Rahmen ausschließlich persönlicher oder familiärer Tätigkeiten nur für Tätigkeiten gilt, die zum Privat- oder Familienleben von Einzelpersonen gehören, was offensichtlich nicht der Fall ist, wenn personenbezogene Daten einer unbegrenzten oder unbeschränkten Zahl von Personen zugänglich gemacht werden.[58] In einer dieser Rechtssachen befand der Gerichtshof ferner, dass die Ausnahme für journalistische Tätigkeiten weit ausgelegt werden sollte, damit sie alle Tätigkeiten umfasst, die allein das Ziel verfolgen, der Öffentlichkeit Informationen, Meinungen oder Ideen näherzubringen.[59]

In einer Rechtssache, in der es um die Kriterien für die Rechtmäßigkeit von Datenverarbeitungen ging, vertrat der Gerichtshof die Auffassung, Spanien habe Artikel 7 Buchstabe f der Richtlinie nicht korrekt umgesetzt, da es verlange, dass – in Abwesenheit der Einwilligung der betroffenen Person – alle verarbeiteten Daten in öffentlich zugänglichen Quellen erscheinen sollen.[60] Der Gerichtshof war ferner der Meinung, Artikel 7 Buchstabe f gelte unmittelbar.[61] Durch das Urteil wird der Ermessensspielraum der Mitgliedstaaten bei der Umsetzung von Artikel 7 Buchstabe f eingeengt. So dürfen sie insbesondere die schmale Grenze zwischen Spezifikation oder Klarstellung auf der einen Seite und Vorgabe weiterer

[55] *Österreichischer Rundfunk*, Randnrn. 68-72.
[56] *Österreichischer Rundfunk*, Randnrn. 73-74.
[57] Verbundene Rechtssachen C-317/04 und C-318/04, *PNR*, [2006] Slg. I-04721, Randnrn. 56-59 und 67-69. Eine kritische Würdigung dieses Urteils in: C. Docksey, „The European Court of Justice and the Decade of Surveillance", in H. Hijmans und H. Kranenborg (Hrsg.), *Data Protection Anno 2014: How to Restore Trust?* (2014), Punkte 97-111.
[58] *Bodil Lindqvist*, Randnrn. 46-47, und Rechtssache C-73/07, *Satamedia*, [2008] Slg. I-09831, Randnrn. 43-44.
[59] *Satamedia*, Randnrn. 56 und 61.
[60] Verbundene Rechtssachen C-468/10 und C-469/10, *ASNEF*, [2011] Slg. I-12181, Randnrn. 32-39 und 49.
[61] *ASNEF*, Randnrn. 51-54.

Anforderungen auf der anderen Seite, die den Anwendungsbereich von Artikel 7 Buchstabe f ändern würden, nicht überschreiten.

In einer Rechtssache, in der es um den Geltungsbereich des Rechts auf Auskunft über automatisierte Einwohnerakten in den Niederlanden ging, entschied der Gerichtshof, die Mitgliedstaaten hätten ein Recht auf Auskunft über frühere Verarbeitungen zu gewährleisten, insbesondere über die Empfänger personenbezogener Daten und den Inhalt von in der Vergangenheit weitergegebenen Daten. Es ist Sache der Mitgliedstaaten, eine Frist für die Aufbewahrung dieser Informationen festzulegen und einen Zugang zu dieser Information vorzusehen und dabei für einen gerechten Ausgleich zwischen dem Interesse der betroffenen Person am Schutz ihrer Privatsphäre auf der einen Seite und der Belastung, die die Pflicht zur Aufbewahrung der betreffenden Information für den für die Verarbeitung Verantwortlichen darstellt, auf der anderen Seite zu sorgen. Eine Regelung jedoch, die die Aufbewahrung von Informationen auf die Dauer eines Jahres begrenzt, während die Basisdaten viel länger aufbewahrt werden, stellt keinen gerechten Ausgleich zwischen dem hier in Rede stehenden Interesse und der fraglichen Verpflichtung dar, es sei denn, eine längere Aufbewahrung den für die Verarbeitung Verantwortlichen über Gebühr belasten würde.[62] Dieses Urteil zeugt von einem scharfen Verständnis der zentralen Rolle des Rechts der betroffenen Person auf Auskunft und des komplexen Umfelds, in dem dieses Recht mitunter auszuüben ist.

4. Institutionelle Aspekte

A. Andere Instrumente

Bisher haben wir uns ausschließlich mit der Richtlinie 95/46/EG befasst, doch ist sie nicht das einzige wichtige Instrument des EU-Datenschutzrechts. Kurz erwähnt werden sollten zumindest drei weitere Kategorien von Instrumenten, nämlich Rechtsakte, in denen die Vorschriften für einen bestimmten Bereich niedergelegt sind, Rechtsakte, die die Vorschriften auf die EU-Ebene anwenden, und Rechtsakte, die ihre Anwendung im Bereich der Strafverfolgung regeln. Ein Beispiel für die erste Kategorie ist die Richtlinie 2002/58/EG über Privatsphäre und elektronische Kommunikation, die das Anliegen der Richtlinie 95/46/EG im Bereich öffentlich verfügbarer elektronischer Kommunikationsdienste und öffentlicher Kommunikationsnetze verdeutlichte.[63] Sie befasst sich mit Fragen, die von der Sicherheit und Vertraulichkeit der Kommunikation bis zur Speicherung und Verwendung von Verkehrs- und Standortdaten und zu unerbetenen Mitteilungen reichen, und zwar unabhängig von der eingesetzten Technologie. Obwohl die Richtlinie damit auch für das Internet gilt, tut sie dies doch nur in ihrem eigenen Geltungsbereich. Einige wichtige Datenverarbeitungen im

[62] Rechtssache C-553/07, *Rijkeboer*, [2009] Slg. I-03889, Randnrn. 56-70.

[63] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.7.2002, S. 37. Siehe insbesondere Artikel 1 zu Geltungsbereich und Zielsetzung der Richtlinie.

Zusammenhang mit Websites fallen nach wie vor in den Geltungsbereich der Richtlinie 95/46/EG.[64]

Ein Beispiel für die zweite Kategorie ist die Verordnung (EG) Nr. 45/2001, mit der die Richtlinie 95/46/EG und die Richtlinie 97/66/EG, die Vorgängerin der Richtlinie 2002/58/EG, für Organe und Einrichtungen der EU umgesetzt wurde.[65] Artikel 286 des EG-Vertrags – das 1997 als Teil des Vertrags von Amsterdam verabschiedet wurde - sah vor, dass „Rechtsakte der Gemeinschaft" über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und den freien Verkehr solcher Daten auch auf EU-Ebene gelten sollten und bildete die Rechtsgrundlage für die Errichtung einer unabhängigen Kontrollinstanz. Ohne eine solche spezifische Rechtsgrundlage wäre dies nicht möglich gewesen. Die Verordnung (EG) Nr. 45/2001 stellt in einem Instrument ein komplettes Regelwerk dar und sieht die Funktion des Europäischen Datenschutzbeauftragten mit einer Reihe von Aufgaben und Befugnissen vor, die sich auf die in der Richtlinie 95/46/EG aufgeführten stützen.[66]

Der Fall der dritten Kategorie ist etwas anders gelagert. Bisher galt unser Augenmerk hauptsächlich der Rechtsgrundlage für den Binnenmarkt in dem, was früher als „erster Pfeiler" der EU bezeichnet wurde. Diese galt natürlich nicht für die anderen Pfeiler wie die Gemeinsame Außen- und Sicherheitspolitik („zweiter Pfeiler") und die polizeiliche und justizielle Zusammenarbeit in Strafsachen („dritter Pfeiler"), die beide 1992 mit dem Vertrag von Maastricht eingeführt wurden. Im Vertrag von Amsterdam wurden einige dieser zum dritten Pfeiler gehörenden Bereiche (wie Einwanderung, Asyl und Grenzkontrolle) in den ersten Pfeiler übertragen, weshalb diese Bereiche nunmehr in den Geltungsbereich der Richtlinie 95/46/EG fielen. Vor diesem Hintergrund wurden einige Verordnungen mit erheblicher Bedeutung für den Datenschutz angenommen.[67]

Dessen ungeachtet enthielten die Bestimmungen des EU-Vertrags zum dritten Pfeiler einige spezifische Rechtsgrundlagen für Datenschutzrechtsvorschriften. Der Ansatz hierbei war,

---

[64] Siehe z. B. *Lindqvist* und *Google Spain*.

[65] Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8 vom 12.1.2001, S. 1.

[66] Siehe Artikel 41-48 über den EDSB. Auf diese Bestimmungen hat der Gerichtshof in seinem Urteilen Bezug genommen, wenn es um die Unabhängigkeit von Kontrollstellen ging (siehe Fußnoten 51 und 52 und insbesondere *Kommission / Deutschland*, Randnrn. 26-28).

[67] z. B. die Verordnung (EG) Nr. 2725/2000 des Rates vom 11. Dezember 2000 über die Einrichtung von „Eurodac" für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens, ABl. L 316 vom 15.12.2000, S. 1, (siehe insbesondere die Erwägungsgründe 15-17), und die Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung), ABl. L 218 vom 13.8.2008, S. 60 (siehe insbesondere die Erwägungsgründe 17-20, in denen auch eine koordinierte Kontrolle durch nationale Datenschutzbehörden und den EDSB erwähnt wird).

dass gemeinsames Handeln im Bereich der polizeilichen oder justiziellen Zusammenarbeit in Strafsachen angemessenen Garantien für den Schutz personenbezogener Daten unterliegen sollte und dass gemeinsame Datenschutzstandards auch einen Beitrag zur Effizienz und Rechtmäßigkeit der Zusammenarbeit leisten könnten.[68] Die Folge waren eine Reihe von Beschlüssen zu konkreten Themen einschließlich Eurojust und Europol[69] sowie 2008 der Rahmenbeschluss 2008/977/JI des Rates mit allgemeinen Vorschriften über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden.[70] Inhaltlich lehnten sich diese Vorschriften an die Richtlinie 95/46/EG und das Übereinkommen Nr. 108 des Europarats an, doch war das Schutzniveau vom Geltungsbereich und Inhalt her deutlich niedriger.[71] Der Geltungsbereich des Beschlusses umfasst nur Fälle, in denen personenbezogene Daten an andere Mitgliedstaaten übermittelt oder ihnen zur Verfügung gestellt werden, und somit, anders als der der Richtlinie 95/46/EG, keine „inländischen" Verarbeitungen.[72]

B. Charta der Grundrechte

Grundrechte, wie sie durch die EMRK garantiert werden oder wie sie sich aus den Mitgliedstaaten gemeinsamen verfassungsrechtlichen Traditionen ergeben, wurden vom Europäischen Gerichtshof lange Zeit als allgemeine Grundsätze des EU-Rechts anerkannt und angewandt. Im Juni 1999 beschloss dessen ungeachtet der Europäische Rat, es sei an der Zeit, eine Charta der Grundrechte der EU auszuarbeiten, um „die überragende Bedeutung der Grundrechte und ihre Tragweite für die Unionsbürger sichtbar zu verankern".[73] Das Ergebnis war, dass im Dezember 2000 auf dem Europäischen Gipfel von Nizza die Charta der

[68] Siehe Artikel 30 und 31 EUV vor dem Inkrafttreten des Vertrags von Lissabon.

[69] Beschluss 2009/426/JI des Rates vom 16. Dezember 2008 zur Stärkung von Eurojust und zur Änderung des Beschlusses 2002/187/JI des Rates über die Errichtung von Eurojust zur Verstärkung der Bekämpfung der schweren Kriminalität, ABl. L 138 vom 4.6.2009, S. 14, und Beschluss 2009/371/JI des Rates vom 6. April 2009 über die Errichtung des Europäischen Polizeiamts (Europol), ABl. L 121 vom 15.5.2009, S. 37.

[70] Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. L 350 vom 30.12.2008, S. 60.

[71] Siehe die Einschätzung durch die Kommission selber in der Erklärung des Bedarfs an einem Ersatz des Beschlusses (Fußnoten 124, 128 und 133).

[72] Siehe insbesondere Erwägungsgrund 7 und Artikel 1.

[73] Europäischer Rat von Köln, 3./4. Juni 1999, Schlussfolgerungen des Vorsitzes, Punkte 44 und 45 sowie Anhang IV. Zur Ausarbeitung der Charta wurde ein Konvent aus 15 Vertretern der Staats- und Regierungschefs, 30 Vertretern der nationalen Parlamente, 16 Vertretern des Europäischen Parlaments und einem Vertreter der Kommission einberufen, dessen Vorsitz Roman Herzog übernahm, früherer Präsident der Bundesrepublik Deutschland und des Bundesverfassungsgerichts.

Grundrechte der Europäischen Union verkündet wurde, die ursprünglich nur als politisches Dokument geplant war.[74]

Eine der Neuerungen der Charta bestand darin, dass sie *zusätzlich* zum Recht auf Achtung des Privatlebens in einer eigenen Bestimmung die ausdrückliche Anerkennung des Rechts auf den Schutz personenbezogener Daten enthielt. Artikel 7 „*Achtung des Privat- und Familienlebens*" besagt: „Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation". Artikel 8 „*Schutz personenbezogener Daten*" sieht in Absatz 1 vor: „Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten". Absatz 2 besagt: „Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden", und „Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken". Absatz 3 lautet: „Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht".

Gemäß den Erläuterungen entsprechen die in Artikel 7 der Charta garantierten Rechte denen, die in Artikel 8 EMRK garantiert werden.[75] Beide sind typische Beispiele für klassische Grundrechte, bei denen ein *Eingriff* nur unter strengen Bedingungen erfolgen darf. Der einzige Unterschied zwischen ihnen liegt in der Tatsache, dass Artikel 52 der Charta eine eher allgemeine Ausnahmeklausel enthält.

Der Erläuterung zu Artikel 8 ist zu entnehmen, dass er sich auf Artikel 286 EGV und die Richtlinie 95/46/EG sowie auf Artikel 8 EMRK und das Übereinkommen Nr. 108 des Europarats stützt. Weiter heißt es dort: „Das Recht auf den Schutz personenbezogener Daten ist zu den in der oben genannten Richtlinie niedergelegten Bedingungen auszuüben und kann

[74] Charta der Grundrechte der Europäischen Union, ABl. C 364 vom 18.12.2000, S. 1. Die Charta wurde feierlich vom Europäischen Parlament, dem Rat und der Kommission verkündet, die sich dazu verpflichteten, die Charta bei ihren Tätigkeiten zu wahren. Die Präambel unterstreicht, dass die Charta auf „*gemeinsamen Werten*" beruht, und „bekräftigt ... die Rechte, die sich vor allem aus den gemeinsamen Verfassungstraditionen und den *gemeinsamen* internationalen Verpflichtungen *der Mitgliedstaaten*, aus der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten, ... sowie aus der Rechtsprechung des Gerichtshofs der Europäischen Union und des Europäischen Gerichtshofs für Menschenrechte ergeben" (Hervorhebung durch uns).

[75] Erläuterungen zur Charta der Grundrechte der Europäischen Union, Dokument CONVENT 49 vom 11.10.2000, Erläuterung zu Artikel 7. Das Präsidium des Konvents arbeitete diese Erläuterungen zu allen Artikeln der Charta aus. Sie sollten die Bestimmungen der Charta erklären, enthielten Angaben zu den Quellen und zum Geltungsbereich der einzelnen in der Charta aufgeführten Rechte. Ursprünglich hatten sie keinerlei rechtlichen Wert und wurden allein zu Informationszwecken veröffentlicht. Mit Artikel 6 Absatz 1 dritter Unterabsatz EUV hat sich ihr Status jedoch geändert. Eine leicht überarbeitete Fassung wurde im ABl. C 303 vom 14.12.2007, S. 17 und in der Präambel der endgültigen Fassung der Charta im ABl. C 303 vom 14.12.2007, S. 1 veröffentlicht. Siehe ferner spätere Veröffentlichungen der Charta im ABl. C 83 vom 30.3.2010, S. 389 und ABl. C 326 vom 26.10.2012, S. 391.

durch die in Artikel 52 der Charta festgelegten Bedingungen eingeschränkt werden".[76] Daraus ergeben sich Fragen nach der Art des neuen Rechts und seinen Elementen, wie sie in Artikel 8 niedergelegt sind, und nach der Unterscheidung zwischen Bedingungen für die „Ausübung" des Rechts gemäß der Richtlinie 95/46/EG und Bedingungen für die „Einschränkung" des Rechts gemäß Artikel 52.

Wie bereits gesagt, wurde das Recht auf den Schutz personenbezogener Daten vom Europarat erdacht und im Übereinkommen Nr. 108 geregelt, um einen *proaktiven* Schutz der Rechte und Freiheiten natürlicher Personen bei jeglicher Verarbeitung personenbezogener Daten unabhängig davon vorzusehen, ob eine solche Verarbeitung einen Eingriff in das Recht auf Achtung des Privatlebens darstellt oder nicht. Es war als ein System von Kontrollen und Gegenkontrollen gedacht, das natürlichen Personen einen *strukturellen* Schutz in einer Vielzahl von Situationen sowohl im öffentlichen als auch im privaten Sektor bietet.

Die Richtlinie 95/46/EG hat das Übereinkommen Nr. 108 als Ausgangspunkt für die Harmonisierung der Datenschutzgesetze in der EU genommen und auf verschiedene Weise spezifiziert.[77] Dabei wurden die wesentlichen Grundsätze des Datenschutzes, die Pflichten von für die Verarbeitung Verantwortlichen und das Erfordernis einer unabhängigen Aufsicht zu den zentralen strukturellen Elementen des Datenschutzes. Am Wesen des Datenschutzes als einem System von Kontrollen und Gegenkontrollen für den Schutz in allen Situationen, in denen personenbezogene Daten verarbeitet werden, wurde jedoch nicht gerüttelt. Anders ausgedrückt: Artikel 7 und 8 haben nicht den gleichen Charakter und müssen deutlich voneinander unterschieden werden.[78]

Der Konvent, der die Charta vor ihrer Annahme beim Gipfel in Nizza ausarbeitete, erwog auch die Aufnahme eines Rechts auf informationelle Selbstbestimmung in Artikel 8, verwarf diesen Gedanken jedoch. Stattdessen beschloss er die Aufnahme eines Rechts auf den Schutz personenbezogener Daten, um die Kernelemente der Richtlinie 95/46/EG zu erhalten, wie es kurz in der Erläuterung heißt.[79] Die in Artikel 8 Absatz 2 und 3 verankerten Elemente wie

[76] Siehe Fußnote 75, Erläuterung zu Artikel 8. In die überarbeitete Fassung ist ein Verweis auf Artikel 16 AEUV und die Verordnung (EG) Nr. 45/2001 eingefügt worden, sie besagt nunmehr, „[die] genannte Richtlinie und Verordnung enthalten Bedingungen und Beschränkungen für die Wahrnehmung des Rechts auf den Schutz personenbezogener Daten". Der Verweis auf Artikel 52 wurde gestrichen.

[77] Siehe weiter oben Abschnitt 3 Teile A und B.

[78] Diese Position geht weiter als die Analyse von J. Kokott und Ch. Sobotta, „The distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR", in H. Hijmans und H. Kranenborg (Hrsg.), *Data Protection Anno 2014: How to Restore Trust?* (2014). Punkte 83-95, und eine frühere Fassung in *International Data Privacy Law*, 2013, Vol. 3, Nr. 4, Punkte 222-228.

[79] Siehe Fußnote 76. Es sei darauf hingewiesen, dass die Artikel 29-Datenschutzgruppe indirekt in die Arbeit des Konvents eingebunden war. Ihr stellvertretender Vorsitzender (1998-2000) bzw. Vorsitzender (2000-2004), Professor Stefano Rodota, war auch Mitglied des Konvents. In einer frühen Phase nahm die Datenschutzgruppe eine Empfehlung dahin gehend an, ein Grundrecht auf Datenschutz in die Charta aufzunehmen (siehe Empfehlung 4/99 über die Aufnahme des Grundrechts auf Datenschutz in den Europäischen Grundrechtskatalog, angenommen am 7. September 1999 (WP 26), abrufbar unter:

Verarbeitung nach Treu und Glauben, Zweckbindung, Auskunfts- und Berichtigungsrecht und unabhängige Kontrolle entsprechen somit den Kerngrundsätzen der Richtlinie 95/46/EG. Dies deutet darauf hin, dass eine „Einschränkung" des Rechts auf Datenschutz nur gegeben ist, wenn diese Kernelemente des Datenschutzes nicht gewahrt werden. Die Richtlinie 95/46/EG und das Übereinkommen Nr. 108 sehen bereits gewisse Ausnahmen von diesen grundlegenden Prinzipien vor, sofern sie aus berechtigten Gründen erforderlich sind. Im derzeitigen Rechtsrahmen wird also bereits zwischen Bedingungen für die „Ausübung" und Bedingungen für die „Einschränkung" des Rechts auf Datenschutz unterschieden.

Außerdem kann nicht ausgeschlossen werden, dass der Gerichtshof noch andere Elemente des Datenschutzes findet, die noch nicht ihren Ausdruck in Artikel 8 Absatz 2 und 3 gefunden haben, aber in der Richtlinie 95/46/EG vorhanden sind und als implizit in Artikel 8 Absatz 1 der Charta geregelt betrachtet werden können. Solche Elemente können auch zur Stärkung der bereits explizit geregelten Elemente beitragen und die Wirkung des in Artikel 8 Absatz 1 zum Ausdruck gebrachten allgemeinen Rechts verstärken.[80]

Das bedeutet auf jeden Fall, dass der *Geltungsbereich* von Artikel 8 – alle Verarbeitungen personenbezogener Daten – nicht mit der Frage verwechselt werden sollte, ob es einen *Eingriff* in das in Artikel 8 verankerte Grundrecht gegeben hat. Ein Eingriff in Artikel 8 resultiert nicht allein aus der Tatsache, dass personenbezogene Daten verarbeitet werden. Von einem solchen Eingriff kann nur die Rede sein, wenn eines oder mehrere der Hauptbestandteile des Rechts auf Datenschutz, wie das Erfordernis einer „gesetzlich geregelten legitimen Grundlage" oder der „unabhängigen Kontrolle", nicht geachtet wurden. Jede Einschränkung des Rechts sollte aus der Perspektive von Artikel 52 behandelt und nicht im Licht der Anforderung in Artikel 8 Absatz 2 einer gesetzlich geregelten legitimen Grundlage betrachtet werden. Diese Anforderung ist keine Ausnahmeklausel, sondern ein Element des Rechts auf Datenschutz selbst. Es mag sein, dass sich die Verfasser der Charta dieser Tatsache nicht in vollem Umfang bewusst waren, doch steht die Erläuterung voll im Einklang mit dem hier vorgetragenen Ansatz.[81]

---

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp26_de.pdf). Schließlich muss der Vorsitzende des Konvents als früherer Präsident des Bundesverfassungsgerichts das Recht auf „informationelle Selbstbestimmung" unterstrichen haben (siehe Fußnote 73).

[80] Ein Beispiel könnte der Grundsatz der „Zweckbindung" sein, der in Artikel 8 Absatz 2 nur teilweise zum Ausdruck kommt („für festgelegte Zwecke … verarbeitet"), in der Praxis jedoch eine zentrale Rolle spielt. Siehe hierzu im Einzelnen Artikel 29-Datenschuzgruppe, Stellungnahme 3/2013 zum Grundsatz der Zweckbindung, angenommen am 2. April 2013 (WP 203), abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (zuletzt aufgerufen am 31. Mai 2014)

[81] Siehe ferner die geringfügigen Unterschiede zwischen der ursprünglichen und der revidierten Fassung der Erläuterung zu Artikel 8, auf die bereits in Fußnote 76 hingewiesen wurde.

C. Auswirkungen des Vertrags von Lissabon

Das Inkrafttreten des Vertrags von Lissabon hatte erhebliche Auswirkungen auf die weitere Entwicklung des EU-Datenschutzrechts.

Erstens erhielt die Charta in Artikel 6 Absatz 1 des Vertrags über die Europäische Union (EUV) die gleiche Rechtsgültigkeit wie die Verträge. Sie wurde also ein rechtsverbindliches Instrument, und zwar nicht nur für die Organe und Einrichtungen der EU, sondern auch für die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich des EU-Rechts fallen.[82] Das Recht auf Datenschutz wurde ferner in Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) im Teil über die allgemeinen Grundsätze der EU ausdrücklich erwähnt.[83] Das bedeutet, dass einige der Hauptelemente der Richtlinie 95/46/EG nunmehr die Ebene des EU-Primärrechts erreicht haben. Wie wir später sehen werden, ist dies auch für die derzeit laufende Reform von Belang.[84]

Zweitens bietet Artikel 16 Absatz 2 AEUV jetzt eine allgemeine Rechtsgrundlage für den Erlass von Vorschriften im ordentlichen Gesetzgebungsverfahren durch das Europäische Parlament und den Rat „über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten“ durch Organe und Einrichtungen der EU sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen. Schließlich unterstreicht Artikel 16 Absatz 2 ebenso wie Artikel 8 Absatz 3 der Charta auch, dass die Einhaltung dieser Vorschriften von unabhängigen Stellen überwacht wird.[85]

Die Formulierungen im Haupttext erinnern an den Wortlaut der Richtlinie 95/46/EG, doch geht der Anwendungsbereich dieser neuen Rechtsgrundlage, die als Verpflichtung formuliert ist, in der Wirklichkeit weit über den Binnenmarkt hinaus und deckt im Prinzip alle Politikbereiche der EU ab.[86] Der Begriff „Vorschriften“ räumt die Möglichkeit ein, Richtlinien oder unmittelbar geltende Verordnungen zu erlassen, und die Entscheidung zwischen diesen beiden Formen dürfte nunmehr eine eher politische sein. In einem späteren

[82] Siehe Artikel 6 Absätze 1 und 2 EUV und Artikel 51 der Charta. Siehe auch weiter unten Abschnitt 4 Teil D zur einschlägigen Rechtsprechung.

[83] Artikel 16 Absatz 1 AEUV: „Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten“.

[84] Siehe weiter unten insbesondere in Abschnitt 7 Teil A.

[85] Die geringfügige sprachliche Abweichung von Artikel 8 Absatz 3 der Charta („Stelle“ oder „Behörden“) scheint aber keine Folgen zu haben.

[86] Artikel 39 EUV enthält eine spezifische Rechtsgrundlage für die Gemeinsame Außen- und Sicherheitspolitik, der zufolge der Rat alle relevanten Vorschriften über den Datenschutz ohne Mitwirkung des Parlaments erlässt. In der Erklärung Nr. 20 heißt es, dass immer dann, wenn „Bestimmungen über den Schutz personenbezogener Daten, die auf der Grundlage von Artikel 16 zu erlassen sind, direkte Auswirkungen auf die nationale Sicherheit haben könnten, dieser Umstand gebührend zu berücksichtigen ist”. In der Erklärung 21 heißt es ferner, „dass es sich aufgrund des spezifischen Charakters der Bereiche justizielle Zusammenarbeit in Strafsachen und polizeiliche Zusammenarbeit als erforderlich erweisen könnte, in diesen Bereichen spezifische … Vorschriften über den Schutz personenbezogener Daten und den freien Datenverkehr zu erlassen.“

Schritt werden wir der Frage nachgehen, wie viel Ermessensspielraum dem Gesetzgeber nach Artikel 16 Absatz 2 AEUV im Lichte der Charta zur Verfügung steht.[87]

Drittens und in einem viel weiteren Sinne hat der Vertrag von Lissabon auch die institutionelle Struktur der EU umgeformt.[88] Er beseitigte weitgehend die alte Pfeilerstruktur und führte die bewährte Gemeinschaftsmethode für die Entscheidungsfindung auch in Bereichen ein, in denen im Rat Einstimmigkeit gängige Praxis war und das Parlament eine lediglich beratende Funktion hatte. Stattdessen bekam nunmehr die Kommission ihre übliche Rolle als Initiatorin neuer Rechtsvorschriften, die von Parlament und Rat im Mitentscheidungsverfahren anzunehmen sind, wobei je nach Thema diese beiden Organe mit Mehrheiten entscheiden. Nach Ablauf eines Übergangszeitraums sollte bei der Durchsetzung von EU-Rechtsvorschriften auch der Gerichtshof in der Lage sein, seine Rechtsprechungsbefugnisse in vollem Umfang auszuüben, und die Kommission ihre Aufgabe als Hüterin der Verträge wahrnehmen.[89]

Dies bedeutete ferner, dass Datenschutzvorschriften im früheren dritten Pfeiler, die vom Rat allein beschlossen worden waren – mitunter noch kurz vor dem Inkrafttreten des Vertrags von Lissabon[90] –, durch Vorschriften zu ersetzen sein würden, die gemäß Artikel 16 Absatz 2 AEUV von Rat und Parlament im Mitentscheidungsverfahren anzunehmen waren. Dies hat zu dem dynamischen Umfeld der derzeitigen Überprüfung des EU-Rechtsrahmens für den Datenschutz beigetragen.

D. Einschlägige Rechtsprechung

Mittlerweile spielt die Charta eine immer wichtigere Rolle in der Rechtsprechung des Gerichtshofs. Nach Auffassung des Gerichtshofs gilt die Charta immer für die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich des EU-Rechts fallen.[91] Durch das einzelstaatliche Recht dürfen in diesen Fällen weder das Schutzniveau der Charta noch der Vorrang, die Einheit und die Wirksamkeit des Unionsrechts beeinträchtigt werden.[92] Dies kann sogar bedeuten, dass eine einzelstaatliche Verfassungsbestimmung nicht mehr anwendbar ist.[93] Es bedeutet jedoch auch, dass die Charta im Anwendungsbereich des EU-Datenschutzrechts sowohl für den Gesetzgeber als auch in einer späteren Phase in vollem Umfang gilt.

---

[87] Siehe weiter unten Abschnitt 7 Teil A.

[88] Dieser Absatz enthält eine knappe Zusammenfassung der wichtigsten für unseren Kontext belangreichen Änderungen in den Verträgen.

[89] Der Übergangszeitraum endet am 1. Dezember 2014 (siehe Artikel 10 des Protokolls Nr. 36 über die Übergangsbestimmungen, Anhang zum Vertrag von Lissabon).

[90] Siehe z. B. die in den Fußnoten 69 und 70 erwähnten Beschlüsse des Rates.

[91] Rechtssache C-617/10, *Åkerberg Fransson*, 26. Februar 2013, Randnr. 17-21, noch nicht veröffentlicht.

[92] Rechtssache C-399/11, *Melloni*, 26. Februar 2013, Randnrn. 59-60, noch nicht veröffentlicht, und *Åkerberg Fransson*, Randnr. 29.

[93] *Melloni*, Randnr. 64.

Bezüglich des Erfordernisses der „vollständigen Unabhängigkeit“ einer Kontrollstelle erging das erste Urteil wenige Monate nach dem Inkrafttreten des Vertrags von Lissabon, doch erwähnte der Gerichtshof hierin die Charta nicht.[94] In drei danach entschiedenen Rechtssachen unterstrich er jedoch das Erfordernis einer unabhängigen Kontrolle als ein „wesentliches Element“ der Wahrung des Schutzes personenbezogener Daten, das sich aus Artikel 8 Absatz 3 der Charta und Artikel 16 Absatz 2 AEUV ergibt.[95] Es muss somit davon ausgegangen werden, dass sich der Gerichtshof nunmehr auch zur Bedeutung dieser Bestimmungen des Primärrechts geäußert hat.

In den letzten Jahren urteilte der Gerichtshof zweimal, Bestimmungen des EU-Rechts seien aufgrund eines unbegründeten Eingriffs in Artikel 7 und 8 der Charta ungültig. Im November 2010 geschah dies im Zusammenhang mit Bestimmungen über die Veröffentlichung von Angaben zu Empfängern landwirtschaftlicher Beihilfen auf einer Website.[96] Im April 2014 ging es um die vorgeschriebene Speicherung von Kommunikationsdaten für Strafverfolgungszwecke vor dem Hintergrund der Richtlinie 2006/24/EG.[97] In einer dritten Rechtssache entschied der Gerichtshof hingegen im Oktober 2013, eine Verpflichtung zur Bereitstellung von Fingerabdrücken zwecks Speicherung in einem Reisepass sei gültig.[98] In allen diesen Rechtssachen ging es um Vorabentscheidungsersuchen einzelstaatlicher Gerichte zur Gültigkeit von EU-Rechtsvorschriften.

Zwar sind die Entscheidungen in diesen drei Rechtssachen im Ergebnis stichhaltig und überzeugend, doch zeugen sie auch von einer Neigung des Gerichtshofs, Artikel 7 und 8 der Charta „als Paket“ zu betrachten. Dieser Ansatz trägt jedoch den erheblichen Unterschieden im Wesen dieser beiden Bestimmungen nicht Rechnung und verhindert möglicherweise, dass das Potenzial von Artikel 8 voll ausgeschöpft wird.[99]

Die erste der drei Rechtssachen ging auf deutsche Landwirte zurück, die gegen die Veröffentlichung ihrer Kontaktdaten und der pro Jahr erhaltenen Agrarbeihilfen geklagt hatten. Nach Auffassung des vorlegenden Gerichts stellte die Pflicht zur Veröffentlichung dieser Daten auf einer Website einen Eingriff in das Grundrecht auf Schutz der

[94] *Kommission / Deutschland*, siehe Fußnote 51.
[95] *Kommission / Österreich*, Randnrn. 36-37 und *Kommission / Ungarn*, Randnrn. 47-48 (siehe zu beiden Fußnote 52) sowie *Digital Rights Ireland* (siehe Fußnote 97), Randnr. 68.
[96] Verbundene Rechtssachen C-92/09 und C-93/09, *Volker und Markus Schecke GbR und Hartmut Eifert / Land Hessen*, [2010] Slg. I-11063.
[97] Verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland und Seitlinger*, 8. April 2014, noch nicht veröffentlicht.
[98] Rechtssache C-291/12, *Michael Schwarz / Stadt Bochum*, 17. Oktober 2013, noch nicht veröffentlicht. Im Gegensatz zu *Schecke* und *Digital Rights Ireland* wurde dieses Urteil nicht von der Großen Kammer erlassen.
[99] Für eine kritische Analyse siehe ferner H. Kranenborg, Commentary on Article 8, in S. Peers *et al*. (eds.), *The EU Charter of Fundamental Rights: a Commentary* (2014, 223), 229-231 und 260-262.

personenbezogenen Daten dar, der nicht gerechtfertigt sei. Es nahm insoweit im Wesentlichen auf Artikel 8 EMRK Bezug.[100]

Nach Ansicht des Gerichtshofs war seit dem Inkrafttreten des Vertrags von Lissabon die Gültigkeit der Bestimmung im Licht der Charta zu prüfen.[101] Ferner merkte er an, das in Artikel 8 der Charta niedergelegte Recht auf den Schutz personenbezogener Daten stehe in engem Zusammenhang mit dem in Artikel 7 der Charta verankerten Recht auf Achtung des Privatlebens, könne jedoch keine uneingeschränkte Geltung beanspruchen. Dies ergebe sich aus Artikel 8 Absatz 2, dem zufolge die Verarbeitung personenbezogener Daten erlaubt ist, sofern bestimmte Voraussetzungen erfüllt sind, sowie aus Artikel 52 Absatz 1 der Charta, der Einschränkungen der Ausübung der Rechte wie derjenigen zulässt, die in ihren Artikeln 7 und 8 verankert sind, sofern diese Einschränkungen gesetzlich vorgesehen sind, den Wesensgehalt dieser Recht und Freiheiten achten und unter Wahrung des Grundsatzes der Verhältnismäßigkeit erforderlich sind sowie dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen. Ferner müssten diese Einschränkungen denen entsprechen, die im Rahmen von Artikel 8 EMRK geduldet werden.[102]

Der Gerichtshof prüfte dann die Frage, ob die einschlägigen Bestimmungen des EU-Rechts zu einer Verletzung der durch die Artikel 7 und 8 der Charta zuerkannten Rechte führen und ob eine solche Verletzung gegebenenfalls im Hinblick auf Artikel 52 der Charta gerechtfertigt ist. Im Hinblick auf die erste Frage kam der Gerichtshof unter Bezugnahme auf die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zu Artikel 8 EMRK sowie seine eigene Auffassung in *Österreichischer Rundfunk* zu dem Schluss, die Veröffentlichung genauer Daten zu den Einkünften auf einer Website stelle einen Eingriff in das Privatleben im Sinne des Artikel 7 der Charta dar.[103] Im Übrigen stelle die Veröffentlichung eine Verarbeitung personenbezogener Daten im Sinne von Artikel 8 Absatz 2 der Charta dar, und die Landwirte hätten keine Einwilligung in die Veröffentlichung gegeben, sodass auch ein Eingriff in das Recht auf den Schutz personenbezogener Daten gemäß Artikel 8 der Charta stattgefunden habe.[104] Im Hinblick auf die zweite Frage befand der Gerichtshof im Wesentlichen, der Eingriff sei nicht gerechtfertigt gewesen, da kein echter Beweis dafür vorläge, dass der Gesetzgeber nach weniger in die Privatsphäre eindringenden Alternativen gesucht habe.[105]

[100] *Schecke*, Randnrn. 30-31 und 44.
[101] *Schecke*, Randnrn. 45-46.
[102] *Schecke*, Randnrn. 47-52.
[103] *Schecke*, Randnrn. 56-59.
[104] *Schecke*, Randnrn. 60-64.
[105] *Schecke*, Randnrn. 81-86.

Diese letzte Schlussfolgerung kommt einem deutlichen Signal bezüglich der Notwendigkeit einer starken empirischen Basis für alle in die Privatsphäre eindringenden Maßnahmen gleich. Der Schluss, die Veröffentlichung habe einen Verstoß sowohl gegen Artikel 7 wie auch Artikel 8 der Charta dargestellt, überzeugt allerdings nicht ganz. Die fehlende Einwilligung war auf jeden Fall für Artikel 7 belangreicher als für Artikel 8, auch wenn in Artikel 8 Absatz 2 ausdrücklich die Einwilligung als *ein Beispiel* einer legitimen Grundlage für die Verarbeitung personenbezogener Daten erwähnt wird. Das Problem ist, dass eine gültige Einwilligung wahrscheinlich den Befund einer Verletzung von Artikel 7 verhindert hätte, der Gerichtshof jedoch der zweiten in Artikel 8 Absatz 2 aufgeführten Option, nämlich „auf einer sonstigen gesetzlich geregelten legitimen Grundlage" keinerlei Beachtung geschenkt hat. Dann hätte er nämlich festgestellt, dass die Antwort auf die Frage, ob diese Option angewandt werden kann, nur von seiner Analyse von Artikel 7 abhängen konnte, und nicht gleichzeitig von Artikel 8. Denn die Tatsache, dass die Veröffentlichung eine Verarbeitung personenbezogener Daten im Sinne von Artikel 8 Absatz 2 war, machte aus ihr noch keine Verletzung von Artikel 8 in Abwesenheit nur einer von mehreren anderen Optionen für Legitimität. Es steht jedoch fest, dass schon die Tatsache, dass die Veröffentlichung ein ungerechtfertigter Eingriff in Artikel 7 war, auch ein Beweis dafür war, dass sie den Anforderungen von Artikel 8 Absatz 2 nicht entsprach, und das hätte der Gerichtshof vielleicht auch sagen sollen.

Noch expliziter und weitreichender ist der Ansatz, den der Gerichtshof in seinem bereits erwähnten zweiten Urteil gewählt hat, in dem es um die Speicherung von Fingerabdrücken in einem Reisepass ging. In dieser Rechtssache hatte ein deutscher Staatsangehöriger die Abnahme seiner Fingerabdrücke verweigert und die Gültigkeit der einschlägigen Bestimmungen mit dem Argument angefochten, sie verletzten die in Artikel 7 und 8 der Charta verankerten Rechte.[106]

Hierauf ging der Gerichtshof mit einer „gemeinsamen" Betrachtung der besagten Artikel ein und führte aus, jede Verarbeitung personenbezogener Daten durch Dritte könne grundsätzlich einen Eingriff in diese Rechte darstellen.[107] Mit diesem Ausgangspunkt scheint der weit gefasste Anwendungsbereich von Artikel 8 – der grundsätzlich alle Verarbeitungen personenbezogener Daten umfasst – mit der inhaltlichen Frage verwechselt worden zu sein, ob ein Eingriff in Artikel 7 oder Artikel 8 vorliegt. Aus der Tatsache, dass die Erfassung der Fingerabdrücke einer Person und ihre Speicherung in einem Reisepass als Verarbeitung personenbezogener Daten betrachtet werden kann, hat der Gerichtshof darüber hinaus geschlossen, dass die Erfassung und Speicherung von Fingerabdrücken auf der Grundlage der

[106] *Schwarz*, Randnr. 12.
[107] *Schwarz*, Randnrn. 23-25.

einschlägigen Bestimmungen einen Eingriff in die Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten darstellten.[108]

In seiner Analyse der Rechtfertigung dieses „zweifachen Eingriffs" merkt der Gerichtshof zunächst an, dass sich Personen der Verarbeitung ihrer Fingerabdrücke nicht frei widersetzen können und dass somit nicht davon ausgegangen werden kann, dass Personen, die einen Reisepass beantragen, in eine solche Verarbeitung eingewilligt haben.[109] Der Gerichtshof befasst sich anschließend mit der Rechtfertigung der Verarbeitung der Fingerabdrücke „auf einer sonstigen gesetzlich geregelten legitimen Grundlage". Nach einer inhaltlichen Analyse vor dem Hintergrund von Artikel 52 Absatz 1 der Charta kommt der Gerichtshof zu dem Schluss, dass dies auf die einschlägigen Bestimmungen mit Blick auf sowohl Artikel 7 als auch Artikel 8 der Charta zutrifft.[110]

Es fällt auf, dass sich diese Analyse praktisch ausschließlich mit der Verarbeitung personenbezogener Daten und den Bedingungen von Artikel 8 und Artikel 52 Absatz 1 der Charta beschäftigt hat. Ein überzeugenderer, anderer Ansatz hätte darin bestanden, dass der Gerichtshof – in voller Übereinstimmung mit der Rechtsprechung des Menschenrechtsgerichtshofs[111] – befindet, dass die Erfassung und Speicherung von Fingerabdrücken einen Eingriff in das Recht auf Wahrung des Privatlebens in Artikel 7 darstellte, aber gemäß den Kriterien von Artikel 52 Absatz 1 gerechtfertigt war. Stattdessen sah der Gerichtshof einen Eingriff in Artikel 8, noch bevor er überprüft hatte, ob es eine „sonstige gesetzlich geregelte legitime Grundlage" gab. Paradoxerweise war der Schluss, die einschlägigen Bestimmungen seien tatsächlich gültig, nur eine Bestätigung der Tatsache, dass die Feststellung eines Verstoßes gegen Artikel 8 verfrüht war.

In der dritten erwähnten Rechtssache, in der es um die Verpflichtung zur Speicherung von Kommunikationsdaten für Strafverfolgungszwecke ging, sollte der Gerichtshof die Gültigkeit der Richtlinie über die Vorratsdatenspeicherung[112] vor dem Hintergrund von Artikel 7 und 8 der Charta prüfen. In dieser Rechtssache hob der Gerichtshof deutlich stärker auf Artikel 7 über das Recht auf Achtung des Privatlebens ab und stellte fest, der Eingriff in dieses Recht sei „von großem Ausmaß" und „besonders schwerwiegend" gewesen und könne nicht

[108] *Schwarz*, Randnrn. 26-30.
[109] *Schwarz*, Randnr. 32.
[110] *Schwarz*, Randnrn. 33-34 und 63.
[111] Siehe z. B. *S and Marper / Vereinigtes Königreich*, Beschwerden 30562/04 und 30566/04, EGMR 2008-V, Randnrn. 78-86.
[112] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. L 105 vom 13.4.2006, S. 54.

gerechtfertigt werden.[113] Allerdings erwähnte er in diesem Zusammenhang auch Artikel 8 über das Recht auf den Schutz personenbezogener Daten.

In seinen Vorbemerkungen stellte der Gerichtshof fest: „Eine solche Vorratsspeicherung der Daten fällt zudem unter Artikel 8 der Charta, weil sie eine Verarbeitung personenbezogener Daten im Sinne dieses Artikels darstellt und deshalb zwangsläufig die ihm zu entnehmenden Erfordernisse des Datenschutzes erfüllen muss".[114] Der Gerichtshof führte weiter aus: „Zwar werfen die Vorabentscheidungsersuchen in den vorliegenden Rechtssachen insbesondere die grundsätzliche Frage auf, ob die Daten der Teilnehmer und der registrierten Benutzer im Hinblick auf Artikel 7 der Charta auf Vorrat gespeichert werden dürfen, doch betreffen sie auch die Frage, ob die Richtlinie 2006/24 den in Artikel 8 der Charta aufgestellten Erfordernissen des Schutzes personenbezogener Daten genügt".[115] Beide Ausführungen geben korrekt eine besondere Sicht der Funktion von Artikel 8 wieder: Er wird als Quelle von *Anforderungen* an die Verarbeitung personenbezogener Daten innerhalb seines Anwendungsbereichs gesehen. Einige Absätze weiter unten stellt der Gerichtshof jedoch plötzlich fest: „Desgleichen greift die Richtlinie 2006/24 in das durch Artikel 8 der Charta garantierte Grundrecht auf den Schutz personenbezogener Daten ein, da sie eine Verarbeitung personenbezogener Daten vorsieht".[116]

Diese letzte Bemerkung ist mit den beiden vorherigen Erklärungen und mit dem unterschiedlichen Wesen von Artikel 7 und 8 nicht vereinbar. Erneut kommt der Gerichtshof zu dem Schluss, es habe einen Eingriff in Artikel 8 gegeben, ohne vorher zu überprüfen, ob „die ihm zu entnehmenden Erfordernisse des Datenschutzes" erfüllt sind. Artikel 8 erlaubt nämlich die Verarbeitung personenbezogener Daten, sofern den dort formulierten Anforderungen Genüge getan wird. Im vorliegenden Fall wäre die Antwort gewesen, dass die „gesetzlich geregelte legitime Grundlage" zwar fehlte, diese Schlussfolgerung aber erst nach einer Analyse der möglichen Rechtfertigung des Eingriffs gezogen werden konnte. Das Urteil des Gerichtshofs macht in jedem Fall überdeutlich klar, dass eine solche Rechtfertigung fehlte.

Die drei Rechtssachen zeigen daher, dass der Gerichtshof wohl noch immer mit der richtigen Funktion von Artikel 8 der Charta kämpft. In den Rechtssachen, in denen es um die Unabhängigkeit von Kontrollstellen ging, lag diese Funktion auf der Hand. Es fehlte ein „wesentliches Element" des Schutzes personenbezogener Daten in Artikel 8 Absatz 3.[117] Ähnlich hätte auch ein Eingriff in Artikel 8 vorliegen können, wenn einem oder mehreren der

[113] *Digital Rights Ireland*, Randnrn. 37 und 70.
[114] *Digital Rights Ireland*, Randnr. 29.
[115] *Digital Rights Ireland*, Randnr. 30.
[116] *Digital Rights Ireland*, Randnr. 36.
[117] Siehe die Verweise in den Fußnoten 94 und 95. In diesem Fällen wurde jedoch ein „Eingriff" in Artikel 8 Absatz 3 der Charta nicht ausdrücklich erwähnt.

anderen wesentlichen Elemente dieses Artikels – wie Verarbeitung nach Treu und Glauben, Zweckbindung, Recht auf Auskunft und Berichtigung – nicht Rechnung getragen würde. Ob eine solche Beschränkung dann gerechtfertigt ist, hängt von einer Prüfung im Lichte von Artikel 52 ab.

5. Die Überprüfung der Richtlinie 95/46/EG

A. Warum diese Überprüfung?

Gemäß Artikel 33 der Richtlinie 95/46/EG legt die Kommission regelmäßig einen Bericht über die Durchführung der Richtlinie vor und fügt ihm gegebenenfalls geeignete Änderungsvorschläge bei.

Der erste Bericht wurde nach einer ausführlichen offenen Überprüfung im Mai 2003 veröffentlicht.[118] In diesem Bericht wurde auf eine Reihe von Problemen hingewiesen, unter anderem auf erhebliche Unterschiede zwischen den Mitgliedstaaten entweder aufgrund nicht korrekter Umsetzung oder unterschiedlicher politischer Entscheidungen innerhalb des von der Richtlinie gebotenen Spielraums. Da jedoch nur wenige praktische Erfahrungen mit der Richtlinie vorlagen, war es nach Meinung der Kommission für Änderungen noch zu früh. Sie entschied sich vielmehr für ein Arbeitsprogramm für eine bessere Umsetzung mit verschiedenen Aufgaben für Kommission, Mitgliedstaaten, Kontrollstellen und andere interessierte Parteien. In dem Bericht wurde ferner die Artikel 29-Datenschutzgruppe aufgefordert, eine bessere Durchsetzung und gemeinsame Untersuchungen in relevanten Sektoren zu fördern.

In einem zweiten Bericht, der im März 2007 im Nachgang zum Arbeitsprogramm [119] erstellt wurde, erwähnte die Kommission, einige der Probleme bestünden nach wie vor, stellten aber für den Binnenmarkt kein echtes Hindernis dar. Da die von der Richtlinie angebotenen rechtlichen Lösungen noch immer angemessen waren und auch auf neue Technologien angewandt werden konnten, vertrat die Kommission erneut die Auffassung, es sei für Änderungen zu früh, und forderte alle Akteure auf, ihre Anstrengungen im Rahmen des Arbeitsprogramms zu verstärken. Im Juli 2007 stimmte der Europäische

[118] Erster Bericht über die Durchführung der Datenschutzrichtlinie (95/46/EG), 15. Mai 2003, KOM(2003) 265 endgültig. Siehe auch den sehr aufschlussreichen technischen Anhang: „Analyse und Folgenabschätzung der Umsetzung der Richtlinie 95/46/EG in den Mitgliedstaaten“. Beide Dokumente sind abrufbar unter: http://ec.europa.eu/justice/data-protection/document/transposition/index_de.htm (zuletzt abgerufen am 31. Mai 2014).

[119] Mitteilung der Kommission an das Europäische Parlament und den Rat – Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie, 7. März 2007, KOM(2007) 87 endgültig, abrufbar unter: http://ec.europa.eu/justice/data-protection/law/follow-up-work-programme/index_de.htm (zuletzt aufgerufen am 31. Mai 2014).

Datenschutzbeauftragte zu, es sei noch nicht an der Zeit, die Richtlinie zu ändern, vertrat aber auch die Auffassung, Änderungen seien unvermeidlich und sollten gut vorbereitet werden.[120]

Leicht widerstrebend begann die Kommission kurze Zeit später mit den Vorbereitungen. Im Mai 2009 leitete sie eine öffentliche Konsultation zu der Frage ein, ob eine Änderung des Rechtsrahmens für den Datenschutz erforderlich sei.[121] Auf diesen Aufruf gingen zahlreiche Reaktionen der verschiedensten Akteure ein, unter anderem ein wichtiger Beitrag der Artikel 29-Datenschutzgruppe mit dem Titel „Die Zukunft des Datenschutzes".[122] Zeitlich fiel dies mit dem Inkrafttreten des Vertrags von Lissabon im Dezember 2009, der eine neue horizontale Rechtsgrundlage für den Datenschutz einführte, sowie mit der Ernennung einer neuen Kommission zusammen, die den Menschenrechten einen höheren Stellenwert einräumte.[123]

Im November 2010 veröffentlichte die Kommission den Entwurf eines „Gesamtkonzepts für den Datenschutz in der EU", das sie auf dieser neuen Rechtsgrundlage aufbauen wollte.[124] Ziele dieses Ansatzes waren „Stärkung der Rechte des Einzelnen", „Stärkung der Binnenmarktdimension", „Bessere Durchsetzung der Datenschutzvorschriften" sowie „Die globale Dimension des Datenschutzes". Vorschläge für einen neuen Rahmen wurden für 2011 erwartet.[125] Als Zweites sollte die Kommission prüfen, ob andere Rechtsinstrumente an diesen neuen Rahmen angepasst werden müssen, darunter auch die Verordnung (EG) Nr. 45/2001, die für Organe und Einrichtungen der EU gilt.[126] Im Januar 2011 äußerte der Europäische Datenschutzbeauftragte Unterstützung für die großen Ziele der Mitteilung, forderte jedoch in einer ganzen Reihe von Punkten einen ehrgeizigeren Ansatz.[127]

---

[120] Stellungnahme des EDSB vom 25. Juli 2007 zur Mitteilung der Kommission an das Europäische Parlament und den Rat „Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie", ABl. C 255 vom 27.10.2007, S. 1.

[121] Informationen hierzu unter: http://ec.europa.eu/justice/newsroom/data-protection/opinion/090501_de.htm (zuletzt aufgerufen am 31. Mai 2014).

[122] Artikel 29-Datenschutzgruppe und Arbeitsgruppe Polizei und Justiz, „Die Zukunft des Datenschutzes", Gemeinsamer Beitrag zu der Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf den Schutz personenbezogener Daten, angenommen am 1. Dezember 2009 (WP 168), abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_de.pdf

[123] Für Viviane Reding, Vizepräsidentin der Kommission und zuständig für Justiz, Grundrechte und Bürgerschaft, stand der Datenschutz weit oben auf ihrer Prioritätenliste.

[124] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: „Gesamtkonzept für den Datenschutz in der Europäischen Union", KOM(2010) 609 endgültig. Siehe ferner V. Reding, „The upcoming data protection reform for the European Union", *International Data Privacy Law*, 2011, Vol. 1, Nr. 1, Punkte 3-5.

[125] KOM(2010) 609 endgültig, S. 18.

[126] a.a.O., S. 18f.

[127] Stellungnahme des EDSB vom 14. Januar 2011 zur Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: „Gesamtkonzept für den Datenschutz in der Europäischen Union", ABl. C 181/01 vom 22.6.2011, S. 1.

B. Die Kernelemente der Überprüfung

Im Januar 2012, also nur etwas später als angekündigt, legte die Kommission ein Paket von Vorschlägen zur Aktualisierung und Modernisierung des derzeitigen EU-Rechtsrahmens vor.[128] Seitdem ist dieses Paket sowohl innerhalb als auch außerhalb des Europäischen Parlaments und des Rates intensiv diskutiert worden und die Überprüfung nähert sich allmählich der letzten Phase des politischen Entscheidungsprozesses, nämlich den Verhandlungen zwischen Parlament und Rat über die ersten greifbaren Ergebnisse.[129]

Bevor wir uns mit dem Thema inhaltlich näher beschäftigen, sollte vielleicht kurz zusammengefasst werden, warum die derzeitige Überarbeitung überhaupt stattfindet. Hierfür gibt es im Wesentlichen drei Gründe. Der erste ist, dass das aktuelle Regelwerk – genauer gesagt die Richtlinie 95/46/EG, sein Kernbestandteil – auf den neuesten Stand gebracht werden muss. „Auf den neuesten Stand bringen" bedeutet in diesem Fall in erster Linie, dafür zu sorgen, dass sie in der Praxis weiterhin *wirksam* bleibt. Als die Richtlinie angenommen wurde, steckte das Internet noch in den Kinderschuhen; heutzutage leben wir in einer Welt, in der Datenverarbeitung allgegenwärtig ist, in der wir deshalb also auch bessere Garantien brauchen, die in der Praxis gute Ergebnisse zeitigen. Die Herausforderungen durch neue Technologien und die Globalisierung erfordern fantasievolle Innovationen, um einen wirksameren Schutz zu gewährleisten.

Der zweite Grund ist, dass das aktuelle Regelwerk zwar zu einer gewissen Harmonisierung geführt hat, aber auch zu wachsender *Vielfalt* und *Komplexität*, allein aufgrund der Tatsache, dass es sich um eine Richtlinie handelt, die aufgrund ihrer rechtlichen Natur in einzelstaatliches Recht umgesetzt werden muss, und wir es nun mit 28 mitunter sehr unterschiedlichen Ausformungen derselben Grundprinzipien zu tun haben. Dies ist ganz offensichtlich zu viel Vielfalt und führt nicht nur zu unnötigen Kosten, sondern auch zu einem Verlust an Effizienz. Der erste Bericht über die Durchführung der Richtlinie sprach von einer Reihe von Unterschieden beim Geltungsbereich und den Begriffsbestimmungen in den einzelstaatlichen Rechtsvorschriften, aber auch in der Praxis bei der Anwendung und

[128] Siehe die Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen mit dem Titel: „Der Schutz der Privatsphäre in einer vernetzten Welt – Ein europäischer Datenschutzrahmen für das 21. Jahrhundert", COM(2012) 9 final. Siehe ferner: V. Reding, „The European data protection framework for the twenty-first century", *International Data Privacy Law*, 2012, Vol. 2, Nr. 3, S. 119-129, und C. Kuner, „The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law", Bloomberg BNA *Privacy and Security Law Report*, 11 PVLR 215, 02/06/2012, S. 1-15.

[129] Im März 2014 nahm das Europäische Parlament in erster Lesung mit jeweils überwältigender Mehrheit seine Stellungnahmen zur vorgeschlagenen Verordnung bzw. vorgeschlagenen Richtlinie an. Die Diskussionen im Rat sind noch nicht so weit fortgeschritten. Der Rat verfolgt zu verschiedenen Themen eine „partielle allgemeine Ausrichtung" und dürfte einen allgemeinen Standpunkt wohl bis Ende 2014 formuliert haben. Im Juni 2014 nahm er eine „partielle allgemeine Ausrichtung" zum territorialen Geltungsbereich und zu Kapitel V der Verordnung über die Übermittlung personenbezogener Daten in Drittstaaten oder an internationale Organisationen an.

Durchsetzung.[130] Die Bemühungen um eine Verringerung dieser Unterschiede waren offensichtlich nicht hinreichend erfolgreich. Gleichzeitig ist als Ergebnis des technologischen Wandels und der Globalisierung der Bedarf an harmonisierten Vorschriften gestiegen. Mit anderen Worten: Wir brauchen mehr Harmonisierung und müssen das System nicht nur stärken und in der Praxis wirksamer machen, sondern auch *kohärenter*. Dies sollte zu einem Abbau *nicht hilfreicher* Vielfalt und Komplexität führen.

Der dritte Grund hat mit dem neuen institutionellen Rahmen der EU zu tun. Wie wir bereits gesehen haben, legt der Vertrag von Lissabon großes Gewicht auf die Grundrechte und hier vor allem auf das Recht auf Datenschutz. So enthält unter anderem Artikel 8 der Grundrechte-Charta eine Datenschutzbestimmung und Artikel 16 AEUV eine neue horizontale Rechtsgrundlage für einen umfassenden Schutz in *allen* Politikbereichen der EU, unabhängig davon, ob es um den Binnenmarkt, Strafverfolgung oder irgendeinen anderen Bereich im öffentlichen Sektor geht.[131]

Bei der derzeitigen Überarbeitung geht es also um einen stärkeren, wirksameren, kohärenteren und *umfassenderen* Schutz personenbezogener Daten. Der Begriff „umfassend" wurde auch von der Kommission in ihrer Strategie für die Reform verwendet, wenngleich viel allgemeiner: Sie sprach von einem Gesamt-„Konzept" für verschiedene Phasen.[132]

Das von der Kommission im Januar 2012 vorgelegte Paket von Vorschlägen umfasst zwei Hauptbestandteile: einen Vorschlag für eine allgemeine Datenschutzverordnung (Datenschutz-Grundverordnung), die an die Stelle der jetzigen Richtlinie 95/46/EG für den privaten Sektor und den Großteil des öffentlichen Sektors in den Mitgliedstaaten treten soll, und einen Vorschlag für eine Richtlinie als Ersatz für den derzeitigen Rahmenbeschluss 2008/977/JI des Rates für den Bereich Strafverfolgung.[133]

Der Vorschlag für eine Verordnung wurde als ein „riesiger Schritt vorwärts"[134] in Richtung eines wirksameren und kohärenteren EU-weiten Schutzes personenbezogener Daten begrüßt, erforderte aber noch einige Klarstellungen und Verbesserungen bei einer Reihe wichtiger Einzelheiten. Auf diese Punkte wurde in der detaillierten Stellungnahme des EDSB vom

[130] Siehe insbesondere den in Fußnote 118 erwähnten Anhang.
[131] Siehe weiter oben Abschnitt 4 Teil C.
[132] Siehe Fußnote 124.
[133] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), COM(2012) 11 final, und
Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, COM(2012) 10 final.
[134] Siehe die Pressemitteilung des EDSB, 25. Januar 2012, abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2012/EDPS-2012-02_EC_DP_Proposal_DE.pdf (zuletzt aufgerufen am 31. Mai 2014)

März 2012 eingegangen.[135] Der Umstand, dass die vorgeschlagene Verordnung in allen Mitgliedstaaten unmittelbar verbindlich sein wird, machte eine hinreichende Klarheit ihrer Bestimmungen umso wichtiger.

Die Struktur des Pakets – eine Verordnung und eine Richtlinie – machte jedoch auch deutlich, dass es mit dem umfassenden Charakter haperte. Und hier ließ sich in der Tat eine der Hauptschwachstellen des Pakets ausmachen. Das Schutzniveau in der vorgeschlagenen Richtlinie liegt deutlich unter dem der vorgeschlagenen Verordnung.[136] Dieses Problem kann auf verschiedenen Ebenen angegangen werden: Die Option einer Verordnung, die auch den Bereich der Strafverfolgung abdeckt, ging den meisten Mitgliedstaaten offensichtlich zu weit, selbst wenn sie angemessene Einschränkungen und Ausnahmen enthielte. Die zweite Option, eine Richtlinie mit dem gleichen Inhalt wie die Verordnung, aber vorbehaltlich der erforderlichen Einschränkungen und Ausnahmen und mit mehr Spielraum für die innerstaatliche Umsetzung, war durchaus vorstellbar. Dennoch hat die Kommission gerade dies nicht vorgeschlagen. Die sich daraus ergebenden Diskrepanzen können unabhängig voneinander betrachtet werden, doch nimmt der Datenaustausch zwischen öffentlichen und privaten Stellen, z. B. Strafverfolgungsbehörden und Banken, Telefon- und Reiseanbietern usw. ständig zu, und ein Mangel an Ausgewogenheit und Kohärenz wird schwerwiegende praktische Folgen in einem größeren Bereich haben. Es sei ferner darauf hingewiesen, dass verwandte Bereich wie Steuern, Zoll und Grenzkontrollen bereits in den Anwendungsbereich der Richtlinie 95/46/EG fallen und daher auch von der vorgeschlagenen Verordnung abgedeckt würden.

Mit Blick auf die Verordnung sind einige allgemeine Dinge zu bedenken. Erstens: Trotz aller Neuerungen herrscht weitgehend *Kontinuität*. Alle vertrauten grundlegenden Konzepte und Grundsätze werden vorbehaltlich einiger Klarstellungen und geringfügiger Änderungen im Detail auch weiterhin bestehen. Ein Beispiel für die Neuerungen ist eine stärkere Betonung[137] der „Datenminimierung“, sprich „nicht mehr Daten als unbedingt erforderlich“ oder „der beste Schutz besteht, wenn so wenig Daten wie möglich verarbeitet werden“. Ein weiteres Beispiel ist die ausdrückliche Anerkennung des „Datenschutzes durch Technik“, kurz: „Berücksichtigung des Datenschutzes von Anfang an“, als allgemeinem Grundsatz.[138] .

---

[135] Stellungnahme des EDSB vom 7. März 2012 zum Datenschutzreformpaket, abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_DE.pdf (zuletzt aufgerufen am 31. Mai 2014).
Siehe ferner die Zusammenfassung im ABl. C 192 vom 30.6.2012, S. 7 sowie die Pressemitteilung, abrufbar unter:
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2012/EDPS-2012-07_DPReform_package_DE.pdf (zuletzt aufgerufen am 31. Mai 2014).

[136] Siehe Stellungnahme des EDSB (Fußnote 135), Punkte 49-74.

[137] Artikel 5 Buchstabe c.

[138] Artikel 23 über „Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen“.

Weiterhin erfolgt eine begrüßenswerte Klarstellung von „Einwilligung“: *Wenn* sie benötigt wird, muss sie ausdrücklich gegeben worden und belastbar sein.[139]

Bei den tatsächlichen Neuerungen geht es in der Hauptsache darum, „den Datenschutz in der Praxis wirksamer zu gestalten“. Wie wir noch sehen werden, beinhaltet dies eine starke Betonung der Umsetzung von Grundsätzen und der Durchsetzung von Rechten und Pflichten, um sicherzustellen, dass der Schutz bei Bedarf in der Praxis auch besteht. Gleichzeitig strebt die Verordnung aber auch Vereinfachung und Kostensenkung an. Ein gutes Beispiel hierfür ist, dass die Pflicht zur Meldung von Datenverarbeitungen bei einer Datenschutzbehörde abgeschafft wurde. Eine Meldung wird nur noch in Situationen verlangt, die besondere Risiken beinhalten.[140] Ferner sieht die vorgeschlagene Verordnung eine zentrale Anlaufstelle für Unternehmen mit Niederlassungen in mehreren Mitgliedstaaten vor. Dies beinhaltet die Einführung einer federführenden Datenschutzbehörde, die eng mit anderen beteiligten zuständigen Behörden zusammenarbeiten soll.[141]

Eine unmittelbar bindende Verordnung bedeutet natürlich auch viel stärkere Harmonisierung – im Prinzip ein einziger in allen Mitgliedstaaten anzuwendender Rechtsakt – und mehr Kohärenz. Allein dies hat für in mehreren Mitgliedstaaten tätige Unternehmen auch in erheblichem Umfang Vereinfachung und Kostensenkungen zur Folge. Gleichzeitig dürfte dies aber auch politische Probleme aufwerfen, denn es geht zu Lasten der Wahrnehmungen und Präferenzen in den Mitgliedstaaten dazu, welches der beste Ansatz beim Datenschutz ist. Eher auf Detailebene stehen die Fragen im Raum, wie genau die Beziehungen zwischen der Verordnung und dem innerstaatlichen Recht aussehen sollen und wie die zentrale Anlaufstelle genau funktionieren soll. Wir werden auf diese Fragen später noch einmal zurückkommen.[142]

C. Datenschutz-Grundverordnung

Es ist nun an der Zeit, einen etwas genaueren Blick auf die Hauptelemente der vorgeschlagenen Datenschutz-Grundverordnung zu werfen. Da es sich hierbei um ein sehr umfangreiches und eher kompliziertes Dokument handelt, sollte man es aus verschiedenen Blickwinkeln betrachten und sich mit seinem Anwendungsbereich, den inhaltlichen Kernpunkten und schließlich den internationalen Dimensionen der Verordnung beschäftigen.

Allgemeiner Anwendungsbereich

Der sachliche Anwendungsbereich der Verordnung ist dem Anwendungsbereich der derzeitigen Richtlinie sehr ähnlich: Sie gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung

[139] Artikel 4 Absatz 8 und Artikel 7.
[140] Artikel 33 und 34.
[141] Artikel 51 Absatz 2.
[142] Siehe weiter unten Abschnitt 6 Teile A und C.

personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen; ausgenommen sind einige Situationen, die inhaltlich mit den in der Richtlinie aufgeführten übereinstimmen.[143] Unter diese Ausnahmen fällt allerdings auch die Verarbeitung personenbezogener Daten durch Organe und Einrichtungen der EU. Auch wenn dies als technische Ausnahme gedacht war, der zu einem späteren Zeitpunkt ein eigener Vorschlag folgen sollte, hat es doch vollkommen zu Recht die Frage aufgeworfen, weshalb eigentlich die EU-Ebene erst in einem zweiten Schritt bedacht werden sollte.[144]

Auf jeden Fall sollte unterstrichen werden, dass die Verordnung einen allgemeinen Anwendungsbereich hat: Sie gilt für den privaten wie den öffentlichen Sektor.[145] Dies entspricht voll und ganz der Situation nach der derzeitigen Richtlinie. Die Möglichkeit einer systematischen Unterscheidung in dieser Richtlinie zwischen öffentlichem und privatem Sektor wurde seinerzeit ausdrücklich erwogen, dann aber verworfen.[146] Eine solche Vorgehensweise hat sich in der Praxis recht gut bewährt, da einige ihrer Bestimmungen – insbesondere die zur Rechtmäßigkeit der Verarbeitung, in denen von „öffentlichen Aufgaben" die Rede ist – offensichtlich eher für öffentliche Einrichtungen von Belang sind, und andere Bestimmungen – in denen es um „Verträge" oder „legitime Interessen" geht – eher für Akteure des privaten Sektors von Bedeutung sind.[147]

Der Gerichtshof hat bestätigt, dass die derzeitige Richtlinie auch auf den öffentlichen Sektor eines Mitgliedstaats anzuwenden ist.[148] Er unterstrich aber auch, dass einzelstaatliches Recht nur dann als Rechtsgrundlage für eine Verarbeitung dienen kann, wenn es im Einklang mit den Grundrechten steht.[149] Diese Haltung wird durch die Tatsache verstärkt, dass Artikel 8 der Charta nunmehr das Recht auf den Schutz personenbezogener Daten explizit anerkennt und dass Artikel 16 AEUV eine ausdrückliche horizontale Rechtsgrundlage für die Annahme von Vorschriften für den Schutz personenbezogener Daten sowohl auf EU-Ebene als auch in den Mitgliedstaaten im Rahmen von Tätigkeiten vorsieht, die in den Anwendungsbereich des EU-Rechts fallen, und zwar unabhängig davon, ob es hier um den privaten oder den öffentlichen Sektor geht.

---

[143] Artikel 2.

[144] Artikel 2 Absatz 2 Buchstabe b. Sowohl das Parlament als auch der Rat haben mit einer Streichung der Ausnahme gedroht, sollte die Kommission nicht einen eigenen, vollständig kohärenten Vorschlag vorlegen.

[145] Artikel 2 und alle anderen allgemeinen Bestimmungen unterscheiden nicht zwischen öffentlichem und privatem Sektor.

[146] Im ersten Vorschlag der Kommission für die Richtlinie (siehe Fußnote 31) war eine systematische Unterscheidung vorgesehen; er wurde allerdings später durch einen überarbeiteten Vorschlag mit einem eher allgemeinen Anwendungsbereich ersetzt.

[147] Siehe Artikel 7 Buchstaben b, e und f der Richtlinie 95/46/EG.

[148] *Österreichischer Rundfunk*, Randnr. 47 (Fußnote 53). Siehe ferner: Rechtssache C-524/06, *Huber*, [2008] Slg. I-09705 und *Rijkeboer* (Fußnote 62).

[149] *Österreichischer Rundfunk*, Randnrn. 68-72.

Es ist damit eine sehr viel gründlichere Analyse des Verhältnisses zwischen EU-Recht und einzelstaatlichem Recht auf der Grundlage der vorgeschlagenen Verordnung erforderlich. Es trügt der Eindruck, die Verordnung werde einfach an die Stelle der einschlägigen nationalen Rechtsvorschriften treten. Dies hängt auch davon ab, wie die Verordnung selbst mit dieser Beziehung umgeht. Es gibt unterschiedliche Wege, auf denen einzelstaatliches und Unionsrecht nebeneinander existieren und in Wechselwirkung miteinander stehen werden. So wird die Verordnung beispielsweise auf einzelstaatlichen Rechtsvorschriften aufbauen, die die Grundrechte umfassend wahren.[150]

Darüber hinaus sollte sorgfältig geprüft werden, ob – und wenn ja, wo und wie – die Verordnung mehr Spielraum für eine nähere Spezifizierung ihrer Bestimmungen im einzelstaatlichen Recht lassen sollte. Es wäre allerdings nicht sinnvoll, eine Aufspaltung der Verordnung in zwei verschiedene Instrumente in Erwägung zu ziehen, eines für den öffentlichen Sektor und eines für den privaten oder kommerziellen Sektor. Ganz im Gegenteil: Eine solche Änderung hätte verhängnisvolle Auswirkungen sowohl auf die Wirksamkeit als auch auf die Kohärenz des neuen Regelwerks, insbesondere für Dienstleistungen, die an der Trennlinie zwischen den beiden Bereichen bzw. über diese Trennlinie hinaus erbracht werden. Die Unterscheidung sähe in verschiedenen Mitgliedstaaten vermutlich auch unterschiedlich aus und würde damit leicht zu neuen Unterschieden führen und den Binnenmarkt in grenzüberschreitenden Situationen untergraben.

Inhaltlich stärkt die Verordnung die Rollen der wichtigsten Akteure, also der einzelnen Person (betroffene Person), der verantwortlichen Organisation (für die Verarbeitung Verantwortlicher) und der Aufsichtsbehörden. Daraus ergeben sich drei verschiedene Perspektiven, die zusammen genommen einen stärkeren Datenschutz ausmachen.

Nutzerkontrolle

Die erste Perspektive kann als eine Aufwertung der Kontrolle betroffener Personen über die Verarbeitung der sie betreffenden personenbezogenen Daten betrachtet werden. Ganz ohne Zweifel besteht ein wichtiges *objektives* Ziel des Datenschutzrechts darin, für betroffene Personen eine wirksame Kontrolle zu gewährleisten, auch wenn dies nicht das Gleiche ist wie die Befürwortung des formellen Rechts auf informationelle Selbstbestimmung. Mit der Erwähnung der Rechte auf Auskunft und Berichtigung unterstreicht auch Artikel 8 Absatz 2 der Charta die Bedeutung dieser Kontrolle.

[150] Siehe weiter unten Abschnitt 6 Teil A.

Es sei angemerkt, dass die derzeitigen Rechte der betroffenen Person in der Verordnung sämtlich bestätigt, dabei jedoch gestärkt oder sogar ausgeweitet wurden.[151] Das Erfordernis der eindeutigen Einwilligung ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage wurde klargestellt und leicht durch die Bedingung verstärkt, die Einwilligung müsse „explizit" gegeben werden. Dies ist eine willkommene Reaktion auf eine im Internet weitverbreitete Praxis, bei der von einer gar nicht eindeutigen Einwilligung ausgegangen wird. Gleichzeitig ist die Verordnung flexibel genug, um sich mit einer Erklärung oder sonstigen eindeutigen Handlung zufriedenzugeben.[152]

Auch das Widerspruchsrecht wurde gestärkt. Es wird von der betroffenen Person nicht verlangt, zwingende schutzwürdige Gründe für den Widerspruch anzugeben; vielmehr hat der für die Verarbeitung Verantwortliche die zwingende Notwendigkeit der Verarbeitung nachzuweisen.[153] Es stehen außerdem bessere Mittel zur Verfügung, mit denen sich die Wahrung der Rechte der betroffenen Person in der Praxis gewährleisten lässt.[154] Es wird mehr Gewicht auf Transparenz gelegt,[155] und es gibt eine Bestimmung, die kollektive Rechtsbehelfe einführt, nicht im Sinne einer Sammelklage nach US-Art, aber doch für Organisationen, die im Namen ihrer Mitglieder oder ihrer Klientel tätig werden.[156]

Viel diskutiert wurde auch über das „Recht auf Vergessenwerden"; bei näherem Hinschauen wird dabei nur betont, dass Daten zu löschen sind, wenn „kein guter Grund besteht, sie aufzubewahren";[157] außerdem besteht die Verpflichtung, angemessene Anstrengungen zur Kontaktierung von Dritten zu unternehmen, um die Wirkungen einer Veröffentlichung von Daten im Internet aufzuheben.[158] Das Recht auf „Datenübertragbarkeit" ist im Grunde nur eine genauere Fassung des bestehenden Rechts, eine Kopie der über eine Person gespeicherten Daten verlangen zu können, nunmehr aber auch in einem bestimmten Format.[159]

Verantwortlichkeit

Das größte Augenmerk liegt jedoch auf einer echten Übernahme von Verantwortung durch verantwortliche Organisationen. Verantwortung ist kein Konzept, das erst *am Ende* greift, wenn etwas schiefgegangen ist. Vielmehr handelt es sich um eine proaktive Verpflichtung, in

[151] Siehe insbesondere die Artikel 11-19, die nunmehr EU-weit einheitliche Vorschriften vorsehen.
[152] Artikel 4 Absatz 8.
[153] Artikel 19.
[154] Artikel 12 sieht beispielsweise eine angemessene „Infrastruktur" vor: Er verlangt von dem für die Verarbeitung Verantwortlichen, „proaktiv" Verfahren festzulegen, damit die betroffene Person ihre Rechte ausüben kann.
[155] Siehe Artikel 11 über nachvollziehbare und für jedermann leicht zugängliche Strategien sowie transparente Information und Kommunikation.
[156] Artikel 73-76.
[157] In *Google Spain* (Fußnote 45), Randnrn. 73-74, 88, 93-94 und 98-99, schlägt der Gerichtshof die gleiche Richtung ein.
[158] Artikel 17.
[159] Artikel 18.

der Praxis ein angemessenes *Datenmanagement* zu entwickeln. Dies zeigt sich an Formulierungen wie etwa der, dass „durch geeignete Maßnahmen sichergestellt wird, dass die Bestimmungen der Verordnung eingehalten werden“ und dass „die Wirksamkeit dieser Maßnahmen zu überprüfen und der Nachweis dafür zu erbringen ist“.[160]

Hier findet eine der wichtigsten Verschiebungen im Datenschutzrecht statt. Sie impliziert, dass die *Beweislast* in vielen Fällen bei der verantwortlichen Organisation liegt. Diese muss nachweisen, dass für die Verarbeitung eine angemessene Rechtsgrundlage besteht, dass es sich bei der Einwilligung um eine echte Einwilligung handelt und dass Maßnahmen nach wie vor wirksam sind.[161] Dies erklärt auch, weshalb in einschlägigen Diskussionen so häufig von „Rechenschaftspflicht“ die Rede ist.[162]

Die Verordnung beinhaltet ferner einige spezifische Anforderungen, etwa die Notwendigkeit einer Datenschutz-Folgenabschätzung, die Dokumentation der Datenverarbeitung und die Ernennung eines Datenschutzbeauftragten.[163] Nach Auffassung vieler Beobachter gingen einige dieser Bestimmungen, insbesondere diejenigen über Dokumentation, viel zu sehr in die Einzelheiten, weshalb über sie sowohl im Parlament als auch im Rat intensiv diskutiert wurde. Einige Ausnahmen in eben diesen Bestimmungen wie die für kleine und mittlere Unternehmen mögen nicht umfassend begründet worden sein. Mehr Ausgewogenheit in diesem Teil des Vorschlags könnte beide Probleme lösen. In diesem Zusammenhang ist von entscheidender Bedeutung, dass die allgemeinen Bestimmungen im derzeitigen und im künftigen Rahmen grundsätzlich skalierbar sind. Unangemessene Detailbestimmungen können hingegen zu unnötigen Ausnahmen führen. Dieses Streben nach Ausgewogenheit erfolgt nunmehr unter dem Begriff „risikogestützter Ansatz“.[164]

Darüber hinaus wurde eine allgemeine Bestimmung zur Meldung von Sicherheitsverletzungen aufgenommen[165]. Derzeit sieht das EU-Recht eine solche Meldung nur für Telekommunikationsanbieter vor.[166] Betrachtet werden könnte dies als Rechenschaftsmechanismus „am Ende“, der ein Datenmanagement anhand des „Lebenszyklus“ stärkt.

[160] Artikel 22.
[161] Artikel 5 Buchstabe f, Artikel 7 Absatz 1 und Artikel 22 Absatz 1.
[162] Siehe Artikel 29-Datenschutzgruppe, Stellungnahme 3/2010 zum Grundsatz der Rechenschaftspflicht, angenommen am 13. Juli 2010, (WP 173). Nähere Ausführungen zu den Themen Rechenschaftspflicht und Einhaltung der Vorschriften siehe weiter unten Abschnitt 7 Teil B.
[163] Artikel 22 Absatz 2, Artikel 28, Artikel 33 und Artikel 35-37.
[164] Siehe weiter unten Abschnitt 6 Teil B.
[165] Artikel 31.
[166] Artikel 4 Absatz 3-5 der Richtlinie 2002/58/EG (siehe Fußnote 63), in der Fassung von 2009.

Aufsicht und Durchsetzung

Ein dritter Schwerpunkt der Verordnung ist der Bedarf an wirksamerer Aufsicht und Durchsetzung. Die Garantien für eine vollständige Unabhängigkeit von Aufsichtsbehörden wurden im Einklang mit der Rechtsprechung des Gerichtshofs gestärkt.[167]

Die Verordnung sieht zudem in allen Mitgliedstaaten Aufsichtsbehörden mit starken Durchsetzungsbefugnissen vor.[168] Bußgelder in Millionenhöhe – in derselben Größenordnung wie im Wettbewerbsrecht – haben viel Aufmerksamkeit auf sich gezogen, aber die Botschaft, die damit vermittelt werden soll, ist folgende: „Wenn das hier wichtig ist, soll entsprechend damit umgegangen werden". Dies wird dazu führen, dass der „Datenschutz" in den Chefetagen auf der Tagesordnung nach oben rückt, was sehr zu begrüßen wäre.

In der Praxis sehen wir bereits jetzt auf nationaler Ebene eine rasche Zunahme verschiedener strengerer Durchsetzungsmaßnahmen wie Abhilfesanktionen, Bußgelder und gelegentlich höhere Verbindlichkeiten. Dieser Trend dürfte in naher Zukunft anhalten, möglicherweise verstärkt durch die Verordnung.

Die internationale Zusammenarbeit zwischen Datenschutzbehörden wird in der Verordnung ebenfalls stark unterstützt und erleichtert.[169] Die Einführung einer federführenden Behörde für Unternehmen mit mehreren Niederlassungen ist eine gute Idee, aber auch diese federführende Behörde wird nicht alleine handeln, sondern *de facto* Teil eines eng zusammenarbeitenden Netzwerks mit anderen zuständigen Behörden sein.[170]

Ein weiteres sehr wichtiges Element ist die Einführung eines Kohärenzverfahrens im Zusammenhang mit einem Europäischen Datenschutzausschuss, der auf der derzeitigen Artikel 29-Datenschutzgruppe aufgebaut werden soll. Mit diesem Verfahren sollen kohärente Ergebnisse von Aufsicht und Durchsetzung in allen Mitgliedstaaten gewährleistet werden.[171]

Datenschutz weltweit

Ein letztes Element ist die internationale Dimension der Verordnung im weiteren Sinn. Der Anwendungsbereich des neuen Rechtsrahmens wurde klargestellt und ausgeweitet. Seine Bestimmungen gelten nunmehr nicht nur für alle Datenverarbeitungen im Rahmen einer Niederlassung des für die Verarbeitung Verantwortlichen in der EU,[172] sondern auch wenn Waren oder Dienstleistungen von einer Niederlassung in einem Drittstaat auf den

[167] Artikel 47.
[168] Artikel 53 und 79.
[169] Artikel 45 und Artikel 55-56.
[170] Artikel 51 Absatz 2 und weiter unten Abschnitt 6 Teil C.
[171] Artikel 57-61 und 64-72.
[172] Wie kürzlich in *Google Spain* erläutert (Fußnote 45).

europäischen Markt angeboten werden oder wenn das Verhalten von betroffenen Personen in der EU überwacht wird.[173]

Dies ist heutzutage im Internet zunehmend Realität. Gleichzeitig ist es ein realistischer Ansatz, der auf einer wachsenden Konvergenz der Ansichten über den Datenschutz in vielen relevanten Ländern weltweit aufbaut.[174] Die Richtlinie 95/46/EG hat erheblichen Einfluss auf weltweite Standards ausgeübt; warum sollte es bei der Verordnung nicht ebenso sein? Auch die geballte Marktmacht von 500 Mio. Verbrauchern auf dem EU-Markt wird dazu beitragen, dass die Vorschriften eingehalten werden.

Hierzu ist unbedingt zu erwähnen, dass sich die internationale Zusammenarbeit zwischen Datenschutzbehörden auch in einem größeren Kontext weiterentwickelt (z. B. zwischen der Federal Trade Commission in den USA und Aufsichtsbehörden in der EU), und zwar in einem weltweiten Netz von Datenschutzdurchsetzungsbehörden (Global Network of Privacy Enforcement Authorities – GPEN).[175] Damit wird es möglich sein, wirksamer mit globalen Akteuren im Internet umzugehen. Diese Entwicklung profitiert von einer wachsenden Annäherung von Grundsätzen und Praktiken des Datenschutzes weltweit, die auch durch die einander teilweise überschneidenden Regelwerke des Europarats und der OECD gefördert wird. [176]

Abschließend sei noch darauf hingewiesen, dass die Bestimmungen über den grenzüberschreitenden Datenverkehr in der jetzigen Richtlinie weiterentwickelt und dort, wo es möglich war, vereinfacht wurden. Es gibt nun auch eine spezifische Bestimmung zu verbindlichen unternehmensinternen Vorschriften, die eine Reihe von Vereinfachungen mit sich bringt.[177]

6. Zentrale Themen in der Gesetzgebungsdebatte

A. Ein einziges Regelwerk?

In Abschnitt 5 Teil B haben wir bereits erwähnt, dass die Verordnung mehr Harmonisierung – im Prinzip ein einziger, in allen Mitgliedstaaten geltender Rechtsakt – und mehr Kohärenz mit sich bringt. Dies ist ganz ohne Zweifel ein großer Erfolg. Im derzeitigen System gilt das innerstaatliche Recht eines Mitgliedstaats normalerweise für die Verarbeitungen personenbezogener Daten, die im Rahmen der Tätigkeiten einer Niederlassung des für die

[173] Artikel 3.
[174] Siehe weiter unten Abschnitt 6 Teil D.
[175] Global Privacy Enforcement Network (https://www.privacyenforcement.net), errichtet auf der Grundlage der OECD-Empfehlung vom 12. Juni 2007 über die grenzüberschreitende Zusammenarbeit bei der Durchsetzung von Datenschutzgesetzen (Cross-border Co-operation in the Enforcement of Laws Protecting Privacy), abrufbar unter: http://www.oecd.org/internet/ieconomy/38770483.pdf (zuletzt aufgerufen am 31. Mai 2014).
[176] Siehe weiter unten Abschnitt 6 Teil D.
[177] Artikel 40-45 (siehe Artikel 43 zu den verbindlichen unternehmensinternen Vorschriften).

Verarbeitung Verantwortlichen im Hoheitsgebiet dieses EU-Mitgliedstaats durchgeführt werden.[178] Dies hat zur Folge, dass es ein Mitgliedstaat je nach dem Kontext, in dem personenbezogene Daten verarbeitet werden, in seinem Hoheitsgebiet mit verschiedenen einzelstaatlichen Rechtsvorschriften zu tun haben kann. Betroffene Personen können es ebenfalls neben dem Gesetz ihres Landes mit anderen einzelstaatlichen Gesetzen zu tun haben. In Zukunft wird die Verordnung nicht nur den externen Anwendungsbereich von EU-Recht, sondern auch das überall in der EU anzuwendende Recht festlegen.

Aber bedeutet dies, dass es nur ein einziges Regelwerk geben wird? Die Kommission hat dieses Argument wiederholt bei ihrer Werbung um Unterstützung für die Verordnung angeführt, und es war auch für das Parlament und andere Akteure ein wichtiges Argument in ihrer Unterstützung. Aus mindestens zwei Gründen dürfte diese Behauptung jedoch nicht ganz gerechtfertigt sein.

Erster Grund: Die Verordnung mag durchaus ein wichtiger Bestandteil eines Gesamtkonzepts sein, ist aber keinesfalls der einzige Bestandteil. Sie scheint tatsächlich Bestandteil eines mehrstufigen Gesamtkonzepts zu sein, doch steht weder kurz- und mittelfristig noch langfristig fest, dass die Verordnung für alle wichtigen Fragen des Datenschutzes das einzige anzuwendende Regelwerk sein wird.[179] Viel wahrscheinlicher ist, dass auch andere, spezifischere Vorschriften gelten werden, wie die derzeitige Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation). Es wäre ein gutes Ergebnis, wenn diese anderen Vorschriften mit den Anforderungen der Verordnung vollkommen in Einklang stünden.

Der zweite Grund ist eher grundlegender Natur. Wie bereits in Abschnitt 5 Teil C ausgeführt, trügt der Eindruck, dass die Verordnung an die Stelle aller einschlägigen einzelstaatlichen Rechtvorschriften treten wird. Dies hängt auch von der Art und Weise ab, in der die Verordnung die Beziehung zwischen EU-Recht und einzelstaatlichem Recht regelt. Es gibt hier unterschiedliche Wege, auf denen einzelstaatliches und Unionsrecht nebeneinander existieren und in Wechselwirkung miteinander stehen werden. Es kann passieren, dass die Verordnung auf einzelstaatlichem Recht *aufbaut* oder umgekehrt einzelstaatlichem Recht die Möglichkeit einräumt oder ihm vorgibt, auf der Verordnung aufzubauen und ihr *Wirkung* zu verleihen. Es gibt aber auch Beispiele von Bestimmungen, bei denen die Verordnung dem einzelstaatlichen Recht erlaubt oder sogar von ihm verlangt, ihre Vorschriften in bestimmten Bereichen näher zu *spezifizieren* oder sogar unter bestimmten Voraussetzungen von ihren Bestimmungen *abzuweichen*.[180]

[178] Artikel 4 Absatz 1 Buchstabe a. Siehe ferner Fußnote 45.
[179] Siehe Fußnote 124.
[180] Siehe Stellungnahme des EDSB vom 7. März 2012 (Fußnote 135), Punkte 50-55. In Artikel 46-49 wird von den Mitgliedstaaten verlangt, im Einklang mit diesen Bestimmungen eine oder mehrere unabhängige Aufsichtsbehörden einzurichten. Beispiele für die drei anderen Kategorien folgen unmittelbar im Anschluss.

Beispiele für die erste Kategorie – *Aufbau* auf einzelstaatlichem Recht – lassen sich in den Bestimmungen über die Bedingungen für die Rechtmäßigkeit der Verarbeitung finden. Gemäß Artikel 6 Absatz 1 der Verordnung ist die Verarbeitung personenbezogener Daten nur rechtmäßig, wenn sie c) zur Erfüllung einer gesetzlichen Verpflichtung erforderlich ist, der der für die Verarbeitung Verantwortliche unterliegt, oder e) für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde. In beiden Fällen baut die Verordnung auf Bedingungen für die Verarbeitung auf, die in den meisten Fällen im Wesentlichen im einzelstaatlichen Recht geregelt sein dürften.

In den beiden letzten Kategorien – *Spezifikation* oder *Abweichung* – räumt die Verordnung für die Annahme einzelstaatlicher Vorschriften zu bestimmten Themen unterschiedlich großen Spielraum ein.[181] In manchen Situationen ist dieser Spielraum erheblich, was bedeutet, dass auch viel Raum für Vielfalt und damit für Unterschiede bei in diesen Bereichen anzuwendenden Vorschriften bestehen wird. Dies könnte sich durchaus als ein einfacher Hinweis auf die Grenzen von Harmonisierung und Kohärenz in einem EU-Kontext erweisen.

In den meisten Mitgliedstaaten dürfte es zahlreiche innerstaatliche Gesetze geben, die sich eigentlich nicht mit dem Datenschutz befassen, aber dennoch eine Vielzahl von Bestimmungen über die Erhebung, die Speicherung, den Austausch oder die Veröffentlichung personenbezogener Daten oder dazu enthalten, wie die Rechte betroffener Personen in einem bestimmten Bereich ausgeübt oder gewahrt werden sollten. Viele dieser Gesetze dürften in den Anwendungsbereich der Richtlinie 95/46/EG fallen und Teil ihrer Umsetzung in einzelstaatliches Recht gewesen sein.[182] In den meisten Mitgliedstaaten dürften diese Gesetze im Einklang mit dem nationalen Datenschutzrecht stehen. Sie treten häufiger im öffentlichen Sektor auf, können aber auch für andere Bereiche von Belang sein.

Natürlich müssen solche Rechtsvorschriften, wenn sie mit der Verordnung nicht vereinbar sind, geändert werden, falls ihre Bestimmungen keine Grundlage für eine rechtmäßige Verarbeitung personenbezogener Daten wären (wie in der ersten Kategorie) und in der Verordnung nicht irgendwie vorgesehen sind. Dies würde eine Anpassung solcher einzelstaatlichen Rechtsvorschriften an die Bestimmungen der Verordnung erforderlich machen, die auch den in Artikel 1 des Vorschlags erwähnten allgemeinen Grundsatz des freien Verkehrs personenbezogener Daten innerhalb der EU umfassen müsste.

[181] Siehe insbesondere Artikel 21 (Beschränkungen) und Artikel 80-85 (besondere Situationen).
[182] Dazu können Sozialversicherung, Steuern, Bevölkerungsregister, Personenstandsregister usw. gehören. Siehe ferner die in Fußnote 148 zitierten Urteile des Gerichtshofs.

Diese kurze Analyse zeigt, dass es wohl kaum ein einziges Regelwerk anzuwendender Vorschriften geben wird und dass die Festlegung der genauen Beziehung zwischen EU-Recht und einzelstaatlichem Recht sowohl auf EU-Ebene als auch in den Mitgliedstaaten der sorgfältigen Prüfung und Feinabstimmung bedarf. Dies trifft umso mehr zu, wenn die Verordnung auch weiterhin für den privaten und den öffentlichen Sektor gelten soll. Auf der anderen Seite wird die Verordnung einen großen und wünschenswerten Schritt in Richtung größere Harmonisierung und Kohärenz geschafft haben, sollten diese Bemühungen von Erfolg gekrönt sein.

B. Verwaltungsaufwand und Neuerungen

Die vorgeschlagene Verordnung wurde nicht nur begrüßt, sondern von Unternehmensverbänden heftig kritisiert und war Gegenstand von Lobbykampagnen bisher unbekannten Ausmaßes. In gewisser Weise bestätigt dies die Bedeutung des Themas für unsere digitalen Volkswirtschaften und für unsere zunehmend IKT-abhängigen Gesellschaften insgesamt. Zwei einander teilweise überschneidende Themen stehen bei diesen kritischen Reaktionen im Vordergrund: Erstens führe die Verordnung bei den für die Verarbeitung Verantwortlichen und hier vor allem bei kleinen und mittleren Unternehmen zu erheblichem Verwaltungsaufwand und zweitens würde sie Innovationen in Bereichen ersticken, die für die weitere Entwicklung unserer Volkswirtschaften von zentraler Bedeutung sind.

Es ist bemerkenswert, dass diese beiden Themen eine so große Rolle spielen, denn die Kommission hat ja immer wieder unterstrichen, dass die vorgeschlagene Verordnung auch auf Vereinfachung und Kostensenkung abhebt. In Abschnitt 5 Teil B haben wir drei Beispiele angeführt: die deutliche Verringerung der Zahl der Meldungen an Datenschutzbehörden, die Einführung einer zentralen Anlaufstelle für Unternehmen mit Niederlassungen in verschiedenen Mitgliedstaaten und eine unmittelbar verbindliche Verordnung, die für mehr Harmonisierung und Kohärenz in allen Mitgliedstaaten sorgen soll. Es sei ferner darauf hingewiesen, dass Datenschutz und Vertrauen zentrale Themen in der Digitalen Agenda der Kommission sind, einem Kernbestandteil der EU 2020-Strategie für ein intelligentes, nachhaltiges und integratives Wachstum.[183] Ziel starker und wirksamer Garantien für den Schutz personenbezogener Daten ist es ja auch, zu Wirtschaftswachstum und der Schaffung neuer Arbeitsplätze beizutragen. Anscheinend gibt die Debatte nur die beiden Seiten ein- und derselben Medaille wieder und fügt sich nahtlos in die Suche nach einem Gleichgewicht zwischen Mitteln und Zielen und zwischen Kosten und Nutzen ein. Das Erfordernis der

[183] Siehe http://ec.europa.eu/digital-agenda und http://ec.europa.eu/europe2020/europe-2020-in-a-nutshell/flagship-initiatives/index_de.htm (zuletzt aufgerufen am 31. Mai 2014)

Verhältnismäßigkeit ist ebenfalls ein wichtiger, eher allgemeiner Grundsatz des EU-Rechts.[184]

In diesem Zusammenhang drei Anmerkungen. Zunächst einmal möchte wohl niemand Innovation im Keim ersticken, doch wäre es dumm, würden wir unsere Augen vor der Tatsache verschließen, dass Innovation auch ihre negativen Seiten hat, mit denen sich die politischen Entscheidungsträger auseinandersetzen müssen. Dies trifft vor allem auf die Entwicklung der Informationstechnologie zu, die immer weiter in unsere Gesellschaften eindringt. Das Konzept des Datenschutzes wurde erdacht, um natürliche Personen gegen den missbräuchlichen oder übermäßigen Einsatz von Informationstechnologie bei der Verarbeitung sie betreffender personenbezogener Daten rechtlich zu schützen. Das Recht auf den Schutz personenbezogener Daten ist unterdessen ein Grundrecht geworden und durch eine verpflichtende Rechtsgrundlage für Vorschriften gestärkt worden, mit der seine fortgesetzte Wirksamkeit in einer modernen Gesellschaft gewährleistet werden soll. Inhaltlich müssen diese Vorschriften jedoch stets im Einklang mit dem angestrebten Ziel stehen und dürfen nicht über dieses Ziel hinausschießen. Gleichzeitig sollte mehr Innovation gefördert werden, um den Datenschutzanforderungen von Anfang an gerecht zu werden („Datenschutz durch Technik"), was billiger und wirksamer ist, als im Nachhinein Technologie nachzurüsten, damit sie den Vorschriften besser entspricht.

Zweitens muss klar unterschieden werden zwischen Maßnahmen, mit denen für die Einhaltung bestehender Vorschriften gesorgt wird, und neuen rechtlichen Anforderungen. Es kann durchaus vorkommen, dass Organisationen, die bisher für ihre jeweiligen Online- oder Offline-Tätigkeiten die Bedeutung bestehender Datenschutzvorschriften unterschätzt oder auch gar nicht wahrgenommen haben[185] und daher dem bestehenden Recht nicht Genüge tun, durch Bemühungen, Grundsätzen, die seit geraumer Zeit im Raum stehen, mehr Durchschlagskraft und Wirksamkeit zu verleihen, unangenehm überrascht werden. Ein Argument in der intensiven Lobbyarbeit gegen die vorgeschlagene Verordnung besagt, dass dies in der Tat auf Neulinge und vielleicht auch auf einige erfolgreiche Wirtschaftsteilnehmer im Internet zutreffe. Dies ist jedoch kein Grund, den legitimen Zweck zu vernachlässigen, bessere Garantien vorzusehen, um die fortgesetzte Wirksamkeit eines Grundrechts zu gewährleisten.

Drittens bleibt daher die Suche nach einem ausgewogenen Verhältnis zwischen dem Erfordernis, natürlichen Personen in einem häufig dynamischen Umfeld wirksamen Schutz zu gewährleisten, und der Notwendigkeit, unnötigen Verwaltungsaufwand zu vermeiden,

[184] Siehe Artikel 5 EUV und Protokoll Nr. 2 über die Anwendung der Grundsätze der Subsidiarität und der Verhältnismäßigkeit im Anhang zu den Verträgen.
[185] In diesem Zusammenhang könnte *Google Spain* (Fußnote 45) eine Art „Weckruf" für Wirtschaftsteilnehmer gewesen sein, ihre derzeitigen Geschäftsmodelle und die entsprechenden rechtlichen Regelungen zu überdenken.

übrig. Die Diskussion über dieses Thema wurde durch die Tatsache weitgehend ausgelöst, dass die einschlägigen Bestimmungen in dem Verordnungsvorschlag den allgemeinen Grundsätzen der Verantwortlichkeit und Rechenschaftspflicht der für die Verarbeitung Verantwortlichen nicht genügend Gewicht beimaßen, sondern sich stattdessen allzu schnell mit spezifischen Anforderungen befassten, die wiederum eine ganze Reihe spezifischer Ausnahmen zur Folge hatten, um unter anderem kleine und mittlere Unternehmen vor übermäßigem Verwaltungsaufwand zu schützen.[186] Es trifft zwar zu, dass einige spezifische Bestimmungen im Hinblick auf eine kohärente Anwendung der Verordnung überall in der EU unvermeidbar waren, doch hätte eine stärkere Betonung der Grundsätze der Verantwortung einen besseren Rahmen für die Analyse ergeben. Eine stichhaltige Frage lautet beispielsweise, welche Folgen die allgemeine Verpflichtung für den für die Verarbeitung Verantwortlichen, „angemessene Maßnahmen" zu ergreifen, in Fällen hat, in denen die spezifischen Anforderungen nicht gelten.

Dieses Problem wird jetzt mithilfe des „risikogestützten Ansatzes" angegangen. Dieser sollte sorgfältig von dem Begriff des „Risikos" als einer *Schwellenwert*bedingung für die Geltung eines Schutzes unterschieden werden, und noch mehr von einem Ansatz, bei dem Schutz nur für die risikoreichsten Verarbeitungen gelten würde. Es sollte jedoch berücksichtigt werden, dass jede Verarbeitung von Daten Risiken birgt. Ein „gestaffelter" risikogestützter Ansatz würde stattdessen bedeuten, dass bei größeren Risiken detailliertere Verpflichtungen und bei geringeren Risiken weniger aufwändige Verpflichtungen gelten. Dieser Ansatz bietet zwei große Vorteile: Erstens bedeutet er, dass Bemühungen um die Einhaltung der Vorschriften vorrangig in den Bereichen unternommen werden sollten, in denen sie am nötigsten sind, wenn es beispielsweise um die besondere Schutzwürdigkeit der Daten oder die mit einer bestimmten Verarbeitung einhergehenden Risiken geht, und dass nicht nur irgendwo ein Kästchen angekreuzt wird, um bürokratischen Anforderungen Genüge zu tun. Zweitens bedeutet er, dass für Bereiche mit minimalem Risiko eine lockerere Regelung vorgesehen werden kann. Es sei jedoch darauf hingewiesen, dass die allgemeinen Bestimmungen sowohl im jetzigen als auch im künftigen Rahmen grundsätzlich skalierbar und daher immer einzuhalten sind. Die spezifischen Rechte der betroffenen Person sollten unabhängig vom jeweiligen Risiko gewahrt sein.

Es laufen Bemühungen um eine genauere Beschreibung des Begriffs „Risiko", was zwangsläufig eine gewisse Bewertung beinhaltet. Im Interesse der Rechtssicherheit sollte die Verordnung hinreichend klare Kriterien vorgeben, anhand derer für die Verarbeitung Verantwortliche eine solche Risikobewertung vornehmen können; dabei sollten sowohl objektive Faktoren (wie z. B. die Zahl der von einer bestimmten Verarbeitung betroffenen Personen) als auch eher subjektive Faktoren (z. B. mögliche Beeinträchtigungen der

[186] Siehe Artikel 22-37 und weiter oben Abschnitt 5 Teil C.

Privatsphäre einer Person) herangezogen werden.[187] Auf der Grundlage solcher allgemeinen Kriterien in der Verordnung könnten weitere Orientierungshilfen entweder vom Europäischen Datenschutzausschuss oder gegebenenfalls in delegierten Rechtsakten gegeben werden, beide vorbehaltlich angemessener Aufsicht und Durchsetzung. Ein solcher Ansatz böte größere Rechtssicherheit für den für die Verarbeitung Verantwortlichen, einen wirksameren Schutz für die betreffenden Personen und ausreichend Flexibilität, um sich zu bewähren.

C. Zentrale Anlaufstellen für Bürger und Unternehmen

Eine der in der Verordnung vorgesehenen Neuerungen ist die Einführung zentraler Anlaufstellen für Unternehmen mit Niederlassungen in mehreren Mitgliedstaaten.[188] In einfachen Worten bedeutet dies, dass in Fällen, in denen die Verarbeitung personenbezogener Daten in mehr als einem Mitgliedstaat stattfindet, eine einzige Aufsichtsbehörde für die Überwachung der Tätigkeit des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters in der gesamten Union zuständig ist und die entsprechenden Beschlüsse fasst. Laut Vorschlag wäre dies im Regelfall die Aufsichtsbehörde des Mitgliedstaats, in dem die Daten verarbeitende Stelle ihre „Hauptniederlassung“ hat; diese Behörde würde als „federführende Behörde“ bezeichnet. Die Rolle einer federführenden Behörde sollte *nicht* als *ausschließliche* Zuständigkeit verstanden werden, sondern vielmehr als eine strukturierte Zusammenarbeit mit anderen, örtlich zuständigen Aufsichtsbehörden. Die federführende Behörde würde nämlich in allen Phasen des Prozesses in hohem Maße von Beiträgen und der Unterstützung der anderen Aufsichtsbehörden abhängen.

Zu diesem Thema äußerte sich die vorgeschlagene Verordnung sehr unklar. Die Kommission schien der Auffassung zu sein, die federführende Behörde sei ausschließlich zuständig. Andererseits sah die Verordnung für die federführende Behörde außerhalb ihrer Rechtsordnung nicht ausdrücklich angemessene Befugnisse vor. Gleichzeitig sah sie eine enge Verknüpfung mit der Bestimmung über die Zusammenarbeit mit anderen Aufsichtsbehörden vor, was wiederum der federführenden Behörde die Möglichkeit geben sollte, ihre Aufgabe wirksam wahrzunehmen. Darüber hinaus sollte eine Entscheidung der federführenden Behörde in der gesamten EU nur dann durchsetzbar sein, wenn die Angelegenheit in einem Kohärenzverfahren unter Beteiligung aller anderen Aufsichtsbehörden im Europäischen Datenschutzausschuss behandelt wurde.[189] Auf diese Weise sollten andere (örtlich zuständige) Aufsichtsbehörden in die Lage versetzt werden, sich

[187] Ein ganz anderer Aspekt des Risikos ist die Frage, welche Konsequenzen die Nichteinhaltung von Vorschriften für die für die Verarbeitung Verantwortlichen selbst haben kann, beispielsweise in Form von Sanktionen, Haftung und Verlust des Vertrauens der Verbraucher.

[188] Siehe insbesondere Artikel 51 Absatz 2. Siehe ferner Punkt 2 des Schreibens des EDSB vom 14. Februar 2014 an den Rat zu den Fortschritten beim Datenschutzreformpaket, abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2014/14-02-14_letter_Council_reform_package_EN.pdf (zuletzt aufgerufen am 31. Mai 2014)

[189] Artikel 63.

in allen relevanten Fällen in die Zusammenarbeit einzubringen und Einfluss auf die abschließende Entscheidung der federführenden Behörde zu nehmen.

Der Grundsatz der zentralen Anlaufstelle ist ein wichtiges Element der Harmonisierung des EU-Datenschutzregelwerks. Er wurde von der Kommission ins Spiel gebracht, um die einheitliche Anwendung der Vorschriften zu verbessern, Rechtssicherheit zu gewährleisten und unnötigen Verwaltungsaufwand der für die Verarbeitung Verantwortlichen und Auftragsverarbeiter zu verringern, die in mehr als einem Mitgliedstaat tätig sind. Er verringert ferner die Fragmentierung der Datenschutzlandschaft. Für Unternehmen ist es wichtig, mit (im Idealfall) einem Gesprächspartner und nicht mit (möglicherweise) 28 nationalen Aufsichtsbehörden zu tun zu haben.

Obwohl der Rat den Grundsatz im Oktober 2013 billigte, prüfte er doch in der Folge eine Reihe von Einwänden gegen den Grundsatz der zentralen Anlaufstelle, die vom eigenen Juristischen Dienst erhoben worden waren.[190] Diese Einwände betrafen seine Vereinbarkeit mit der Charta der Grundrechte, insbesondere mit Artikel 47, der das Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht vorsieht und inhaltlich Artikel 13 sowie Artikel 6 Absatz 1 EMRK entspricht. Die größten Bedenken schienen bezüglich der „Nähe“ zwischen der federführenden Aufsichtsbehörde, die in einem konkreten Fall einen Beschluss fasst, und dem einzelnen Bürger zu bestehen, die als ein wichtiger Aspekt des Schutzes der Rechte des Einzelnen angesehen wird. Generell wurde der Grundsatz der zentralen Anlaufstelle als Bevorteilung multinationaler Unternehmen auf Kosten einzelner Bürger angesehen.

Diese Auslegung des Grundsatzes der zentralen Anlaufstelle malt ein unangemessen schwarzes Bild des derzeit vorliegenden Vorschlags. Es ist nämlich durchaus möglich, den Grundsatz mit einem hohen Niveau des Schutzes für die Grundrechte der Bürger, einschließlich der durch Artikel 47 der Charta geschützten, zu vereinbaren. Diese Auffassung stützt sich auf verschiedene Erwägungen.

Zu allererst sei darauf hingewiesen, dass derzeit gemäß Artikel 28 Absatz 6 der Richtlinie 95/46/EG eine Kontrollstelle im Hoheitsgebiet ihres Mitgliedstaats immer für die Ausübung ihrer Befugnisse zuständig ist (die auch die Untersuchung von Beschwerden umfassen). Sofern es sich nicht um eine Beschwerde über einen für die Verarbeitung Verantwortlichen (oder einen Auftragsverarbeiter) mit einer Niederlassung oder Ausrüstung in dem betreffenden Mitgliedstaat handelt, können die tatsächlichen Befugnisse dieser Kontrollstelle in der Praxis allerdings durchaus beschränkt sein. Die Notwendigkeit nämlich, in einem

[190] Siehe den Vermerk des Vorsitzes vom 26. Mai 2014 an den Rat zum Mechanismus der zentralen Anlaufstelle, abrufbar unter: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010139%202014%20INIT (zuletzt aufgerufen am 30. Juni 2014).

konkreten Fall das einzelstaatliche Recht eines anderen Mitgliedstaats anzuwenden, sowie fehlende Möglichkeiten zur Durchführung von Untersuchungen oder zur Verhängung von Sanktionen, wenn der für die Verarbeitung Verantwortliche/Auftragsverarbeiter physisch nicht präsent ist, können die Anrufung der Kontrollstelle zu einer rein theoretischen und weitgehend unwirksamen Lösung machen.

Die vorgeschlagene Verordnung würde hingegen einen einheitlichen rechtlichen Rahmen gewährleisten und verschiedene Mechanismen für eine wirksame Durchsetzung in der Praxis vorsehen. Die Bürger hätten zur Ausübung ihrer Rechte ausdrücklich das Recht auf Beschwerde bei der örtlichen (oder auch einer anderen) Aufsichtsbehörde.[191] In der Praxis dürfte wohl die örtliche Aufsichtsbehörde für Bürger in der betreffenden Rechtsordnung als zentrale Anlaufstelle fungieren. In Fällen allerdings, in denen heute eine Aufsichtsbehörde nur über begrenzte Möglichkeiten verfügen würde, würde die neue Verordnung für eine wirksame Durchsetzung durch die federführende Behörde im Rahmen der zentralen Anlaufstelle für Unternehmen (und mit Unterstützung durch das Kohärenzverfahren) sorgen, bei Bedarf auch mit Unterstützung durch die örtlich zuständige Aufsichtsbehörde. Darüber hinaus hat jede natürliche Person stets das Recht, gegen ein in ihrem Land niedergelassenes Unternehmen vor den Gerichten dieses Landes wegen eines mutmaßlichen Verstoßes gegen die Verordnung Klage zu erheben.[192]

Aus diesem Blickwinkel wird sich die Verordnung äußerst positiv auf die Möglichkeiten natürlicher Personen auswirken, ihre Datenschutzrechte durchzusetzen; somit würde sie den Schutz des Rechts auf wirksamen Rechtsbehelf, wie er in Artikel 47 der Charta verankert ist, deutlich verbessern.

Die Verordnung sieht ferner eine Überprüfung von Entscheidungen von Aufsichtsbehörden durch die Gerichte vor. In Fällen, in denen der Grundsatz der zentralen Anlaufstelle gilt, müsste eine natürliche Person, die eine Entscheidung der federführenden Aufsichtsbehörde anfechten möchte, dies vor einem Gericht in dem Mitgliedstaat der federführenden Behörde tun;[193] in vielen Fällen würde dies in der Praxis bedeuten, dass Klage in einem anderen Mitgliedstaat erhoben werden muss.

In diesem Zusammenhang beraubt allein die Tatsache, dass Gerichte in einem anderen Mitgliedstaat als dem Wohnsitzmitgliedstaat eines Bürgers angerufen werden müssen, diesen nicht eines wirksamen Rechtsschutzes. Nach der derzeit anzuwendenden Richtlinie 95/46/EG ist es nämlich durchaus möglich, dass sich Bürger, die sich über die Verarbeitung personenbezogener Daten durch ein in mehreren Mitgliedstaaten tätiges Unternehmen

[191] Artikel 73.
[192] Artikel 75.
[193] Artikel 74 Absatz 3.

beschweren möchten, an eine bestimmte Aufsichtsbehörde wenden müssen und, falls sie deren Entscheidungen anfechten möchten, den Rechtsstreit in eben diesem Mitgliedstaat führen müssen. Bisher bestand kein Anlass, mit Blick auf die Charta dieses Merkmal des bestehenden Systems infrage zu stellen.

Kritisiert wird der vorgeschlagene Grundsatz der zentralen Anlaufstelle auch, weil er angeblich übermäßig hohe Hindernisse für Bürger aufbaut, die gerichtlichen Rechtsbehelf in Anspruch nehmen wollen, und zwar aufgrund geografischer Entfernung, mangelnder Kenntnis der ausländischen Rechtsordnung, der Notwendigkeit der Klageerhebung und Führung des Verfahrens in einer Fremdsprache oder der Kosten eines solchen Verfahrens.

Die hierzu vorgeschlagene Alternative scheint die Einrichtung einer EU-Einrichtung mit eigener Rechtspersönlichkeit zu sein, die die Funktion der zentralen Anlaufstelle sowohl für Bürger als auch für Unternehmen übernehmen würde. Dies würde eine grundlegende Zentralisierung der bestehenden dezentralen Struktur der Aufsicht im Bereich Datenschutz erfordern, die eine Entscheidungsfindung innerhalb annehmbarer Fristen nicht unbedingt erleichtern und gewiss weder für Bürger noch für Unternehmen mehr „Nähe“ bedeuten würde. Wichtiger ist jedoch, dass sie für einen besseren Schutz der Grundrechte von Bürgern nicht erforderlich zu sein scheint.

Es ist zu bedenken, dass in den meisten Fällen alle relevanten Akteure – betroffene Personen, für die Verarbeitung Verantwortlicher und Aufsichtsbehörde –auch weiterhin in einem Land ansässig sind. Folglich würde der Grundsatz der zentralen Anlaufstelle für Unternehmen nur in relativ wenigen Situationen zum Tragen kommen. Darüber hinaus könnten Fragen von überwiegend lokaler Bedeutung ausgeschlossen werden, wie beispielsweise Probleme, die sich aus lokalem Recht ergeben. Mit anderen Worten: Auch wenn einige der verbleibenden Fälle möglicherweise große Auswirkungen haben können, würde in der Praxis die Zahl der Fälle, in denen Bürger von Entscheidungen einer federführenden Behörde mit Sitz in einem anderen Mitgliedstaat als ihren Wohnsitzmitgliedstaat betroffen sind, deutlich niedriger ausfallen als die Zahl der Fälle, in denen die „eigene“ Aufsichtsbehörde Entscheidungen trifft.

Schließlich muss der Grundsatz der zentralen Anlaufstelle für Unternehmen in seinem eigenen Kontext als ein wichtiges Element gesehen werden, das zur Gesamtwirksamkeit und Gesamtkohärenz des künftigen Datenschutzrahmens beiträgt. Ganz ohne Zweifel würden sich ein einheitlicheres Datenschutzsystem und niedrigere Prozesskosten (denn Gerichtsverfahren wären auf die Rechtsordnung der federführenden Behörde beschränkt, also auf das Land der Hauptniederlassung) für die Unternehmen in der gesamten EU vorteilhaft auswirken. Allerdings werden auch Bürger von einer kohärenteren Anwendung eines einheitlichen

Datenschutzregelwerks profitieren, wie es in der vorgeschlagenen Verordnung vorgesehen ist.

Ist beispielsweise ein Bürger von einer Datenverarbeitung durch einen für die Verarbeitung Verantwortlichen mit Niederlassungen in verschiedenen Ländern betroffen, werden aber alle Entscheidungen von der Hauptniederlassung des für die Verarbeitung Verantwortlichen in einem anderen Mitgliedstaat getroffen, wäre die Möglichkeit, eine einzige Entscheidung einer Aufsichtsbehörde oder ein Gerichtsurteil zu erwirken, die/das in allen diesen Mitgliedstaaten gültig und vollstreckbar wäre, im Vergleich zur heutigen Situation eine eindeutige Verbesserung.

Im Übrigen verringert die zentrale Anlaufstelle für Unternehmen auch die Wahrscheinlichkeit von Parallelverfahren und daraus resultierender Kompetenzkonflikte, denn ein Verfahren im Mitgliedstaat der federführenden Behörde würde normalerweise ausreichen, um Rechte in der gesamten EU durchzusetzen.

Wie diese Diskussion zeigt, wirft das Konzept der zentralen Anlaufstelle entweder für Unternehmen oder für Bürger einige Fragen auf, die noch eine gewisse Feinabstimmung in der vorgeschlagenen Verordnung erfordern. Deshalb werden auch noch mehrere Optionen geprüft. Feststehen dürfte aber, dass das Ergebnis eher enge Zusammenarbeit zwischen Behörden und weniger ausschließliche Zuständigkeiten heißen wird, wobei dem Bedarf an wirksamem Schutz und mehr Effizienz zweifelsohne angemessenes Gewicht beigemessen wird.

D. Mehr weltweiter Datenschutz und „Interoperabilität“

Das digitale Umfeld hat zunehmend globalen Charakter, da sich dank des Internets und anderer weltweiter Netze Daten an jedem Tag und zu jedem Zeitpunkt rund um die Welt bewegen lassen. Daher wurde den internationalen Dimensionen der Verordnung ebenfalls erhebliche Aufmerksamkeit geschenkt.

In diesem Zusammenhang hebt die Verordnung – wie auch die Richtlinie 95/46/EG, jedoch noch stärker – vorrangig nicht darauf ab, *wo* sich die Daten befinden, sondern wer für die Datenverarbeitung *verantwortlich* ist und welche *Auswirkungen* die Verarbeitung der Daten auf die betroffenen Personen hat. Am offensichtlichsten wird dies beim Anwendungsbereich der Verordnung, den diese gilt nicht nur bei allen Verarbeitungen im Rahmen der Tätigkeiten einer Niederlassung des für die Verarbeitung Verantwortlichen in der EU, sondern auch, wenn Waren oder Dienstleistungen auf den Markt der Union angeboten werden oder wenn das Verhalten von betroffenen Personen in der EU beobachtet wird, unabhängig von wo

aus.[194] In allen diesen Situationen ist der für die Verarbeitung Verantwortliche dafür verantwortlich, dass die Kerngrundsätze des Datenschutzes eingehalten und die Rechte der betroffenen Person gewahrt werden, und unterliegt er der Kontrolle durch unabhängige Aufsichtsbehörden.[195]

Soweit die Verordnung anzuwenden ist, besagt sie, dass personenbezogene Daten nur dann in ein Drittland übermittelt werden dürfen, wenn das Bestimmungsland ein angemessenes Schutzniveau gewährleistet oder auf anderem Wege angemessene Garantien bereitgestellt werden. Diese Bestimmungen sind überarbeitet und vereinfacht worden, sodass es mehr Optionen für die Gewährleistung angemessenen Schutzes in bestimmten Situationen geben wird.[196] Ihnen liegt der Gedanke zugrunde, dass personenbezogene Daten nur in ein Drittland übermittelt werden sollten, wenn die Rechte betroffener Personen dort gewahrt sind. Gleichzeitig sind diese Bestimmungen aber auch so pragmatisch formuliert, dass ein Zusammenspiel mit anderen Teilen der Welt möglich ist. Sie werden daher auch Anwendung finden, wenn personenbezogene Daten im Rahmen des Cloud Computing an Diensteanbieter in Drittländern übermittelt werden. In solchen Fällen bleibt der für die Verarbeitung Verantwortliche für die Einhaltung von Datenschutzanforderungen zumindest mitverantwortlich.[197]

Als Drittes wird die Verordnung auch die Zusammenarbeit mit Datenschutzbehörden in anderen Teilen der Welt fördern.[198] Ihr kommt mit Blick auf den Umgang mit weltweiten Akteuren im Internet große Bedeutung zu. Wie bereits in Abschnitt 5 Teil C ausgeführt,

---

[194] Siehe Artikel 3. Der EuGH hat vor Kurzem in *Google Spain* (siehe Fußnote 45) befunden, die Richtlinie 95/46/EG sei bereits auf eine Suchmaschine anzuwenden, deren Betreiber aus einem Drittstaat über seine Tochtergesellschaft in einem EU-Mitgliedstaat tätig werde. Hierzu vertrat der Gerichtshof die Auffassung, der Suchmaschinenbetreiber sei im Hinblick auf die von der Suchmaschine vorgenommenen Verarbeitungen personenbezogener Daten der für die Verarbeitung Verantwortliche, und die Tätigkeiten der Niederlassung, die zwar auf den Verkauf von Werbeflächen beschränkt sei, seien untrennbar mit der Verarbeitung personenbezogener Daten verbunden, die aus Suchvorgängen resultierten und die Suchmaschine wirtschaftlich rentabel machten (siehe *Google Spain*, Randnrn. 30 und 55-56). Damit hat der Gerichtshof einen großen Schritt in die auch von der Verordnung angestrebte Richtung getan.

[195] In seinem Urteil befand der Gerichtshof, der für die Verarbeitung Verantwortliche müsse in seinem Verantwortungsbereich im Rahmen seiner Befugnisse und Möglichkeiten dafür sorgen, dass seine Tätigkeit den Anforderungen der Richtlinie entspricht (siehe *Google Spain*, Randnr. 38). Dies gilt auch, wenn diese Tätigkeit von Computern auf der Grundlage von Computerprogrammen durchgeführt wird: eine willkommene Unterstützung der Verantwortung von für die Verarbeitung Verantwortlichen und des Geltungsbereichs ihrer Verpflichtungen im Internet. Im Mittelpunkt der Erwägungen des Gerichtshofs steht unter anderem das Erfordernis, einen „wirksamen und umfassenden Schutz" der Grundrechte zu gewährleisten (*Google Spain*, Randnrn. 34, 38, 53 und 58). Ein wichtiges Detail ist, dass der Gerichtshof erneut bekräftigt hat, dass die Richtlinie für personenbezogene Daten gilt, die veröffentlicht worden sind (*Google Spain*, Randnr. 30). Bei der Bestimmung der Rechte der betroffenen Person gemäß Artikel 12 und 14 der Richtlinie (insbesondere des Rechts auf Löschung und des Rechts auf Widerspruch gegen die Verarbeitung personenbezogener Daten) verwies der Gerichtshof ausdrücklich auf Artikel 7 und 8 der Charta (*Google Spain*, Randnrn. 69, 81 und 97). Das Urteil kann daher auch als weiterer Beleg dafür gesehen werden, dass sich die Charta zunehmend auf die Anwendung bestehenden Rechts auswirkt.

[196] Artikel 40-44.

[197] Artikel 24.

[198] Artikel 45.

profitiert diese Entwicklung von einer wachsenden Annäherung von Grundsätzen und Praktiken des Datenschutzes weltweit, die auch durch die einander teilweise überschneidenden Regelwerke des Europarats und der OECD gefördert wird.

Vor Kurzem hat die OECD überarbeitete Datenschutzleitlinien veröffentlicht, die den bisher verfolgten Ansatz im Wesentlichen bestätigen.[199] Besonders unterstrichen werden in den überarbeiteten Leitlinien die Notwendigkeit praktischer Maßnahmen zur Gewährleistung der Wahrung der Datenschutzgrundsätze und die Notwendigkeit der Zusammenarbeit zwischen Datenschutzdurchsetzungsbehörden.[200] Die Überarbeitung des Übereinkommens Nr. 108 des Europarats weist in eine ähnliche Richtung.[201]

Alle diese Elemente zusammen werden eine schrittweise Entwicklung in Richtung weltweiter „Interoperabilität" von Regelwerken für den Schutz der Privatsphäre und den Datenschutz ermöglichen. Zwar ließen sich zwischen diesen Regelwerken relativ leicht jede Menge Unterschiede im Detail ausmachen, doch besteht zwischen ihnen auch viel Raum für Synergien und Konvergenz. Die Verordnung wäre das weltweit am weitesten entwickelte Regelwerk - im Einklang mit der Anerkennung des Rechts auf Datenschutz als Grundrecht in Artikel 8 der Charta –, sie würde aber auch im Einklang mit den Entwicklungen andernorts stehen. Sie könnte darüber hinaus zu gegebener Zeit auch starken Einfluss auf diese Entwicklungen nehmen, so wie es früher die Richtlinie 95/46/EG tat. Die Überprüfung der Richtlinie bietet daher auch eine gute Möglichkeit, zunehmend weltweiten Datenschutz und weltweite Interoperabilität zu gewährleisten.

Schließlich findet die Verordnung keine Anwendung auf Überwachungstätigkeiten von Drittländern oder die einschlägigen Dienste eines EU-Mitgliedstaats. Sie gilt jedoch für Wirtschaftsteilnehmer und andere Diensteanbieter, die ihre Dienstleistungen auf dem europäischen Markt anbieten oder das Verhalten betroffener Personen in der EU überwachen und somit auch anderen Akteuren Gelegenheit zum Ausspionieren bieten können.[202] Die dem für die Verarbeitung Verantwortlichen aus der Verordnung entstehenden Verpflichtungen würden hier als wichtiges Gegengewicht dienen.

Vor diesem Hintergrund und in einem größeren Zusammenhang wäre es hilfreich, wenn die Verordnung auch eine Bestimmung für Fälle enthielte, in denen eine von einem Drittland auferlegte gesetzliche Verpflichtung Tätigkeiten verlangte, die mit dem EU-Recht nicht in

---

[199] Abrufbar unter http://www.oecd.org/sti/ieconomy/privacy.htm#newguidelines (zuletzt aufgerufen am 31. Mai 2014).
[200] Teil Drei über „Umsetzung der Rechenschaftspflicht" und Teil Sechs über „Internationale Zusammenarbeit und Interoperabilität".
[201] Siehe nähere Informationen unter http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp (zuletzt aufgerufen am 31. Mai 2014)
[202] Artikel 3.

Einklang stehen.[203] Grundsätzlich sollten solche Tätigkeiten nicht erlaubt sein, es sei denn, sie wären nach einem internationalen Abkommen zulässig, oder eine unabhängige Justizbehörde oder Aufsichtsbehörde hätte eine Ausnahme gewährt. Eine solche Bestimmung könnte die erforderliche Regulierungsfunktion in Fällen ausüben, in denen internationale Normenkollisionen oder Fragen der öffentlichen Ordnung andernfalls nur auf Kosten von Wirtschaftsteilnehmern, allgemeinen Interessen oder beidem geregelt werden könnten.

7. Sonstige Fragen

A. Binnenmarkt und Grundrechte

Die Richtlinie 95/46/EG wurde als harmonisierter Rechtsrahmen für den Datenschutz in der EU auf einer Binnenmarktrechtsgrundlage angenommen. Doch war von Anfang an auch die Grundrechtsperspektive sichtbar. Der Gerichtshof hat unterstrichen, dass die Richtlinie einen sehr weit gefassten Anwendungsbereich hat und sich die Charta auf ihre Anwendung in der Praxis immer stärker auswirkt. Die Überprüfung der Richtlinie erfolgt nunmehr aus einem anderen Blickwinkel. Artikel 16 AEUV bietet eine allgemeine Rechtsgrundlage für den Schutz personenbezogener Daten in allen Politikbereichen, und die Charta gilt für die Organe und Einrichtungen der EU sowie die Mitgliedstaaten bei Tätigkeiten, die in den Anwendungsbereich des EU-Rechts fallen.

Dieser andere Blickwinkel bedeutet nun aber keineswegs, dass Binnenmarkterwägungen und andere Fragen der öffentlichen Ordnung bei der Überprüfung des bestehenden EU-Rechtsrahmens für den Datenschutz und auch für die Struktur und den Inhalt des neuen Rechtsrahmens keine Rolle mehr spielen. Es liegt auf der Hand, dass Grundlage für die Entscheidung für die vorgeschlagene Verordnung und viele ihrer Hauptelemente der Bedarf an mehr Harmonisierung im Sinne eines stärkeren, wirksameren und kohärenteren Schutzes personenbezogener Daten überall in der EU ist. Mit anderen Worten: Die Auswirkungen der Charta und der Bedarf an EU-weiter Harmonisierung und Kohärenz sind nicht nur miteinander vereinbar und ergänzen sich nicht nur, sondern verstärken einander. Ein starker und kohärenter Datenschutz liegt auch im Interesse des Binnenmarktes.

Man könnte natürlich noch fragen, wie viel Flexibilität Artikel 16 AEUV zulässt und wo die Auswirkungen der Charta möglicherweise gewisse Grenzen bedeuten, die Public Policy-Entwickler und der EU-Gesetzgeber zu achten haben. Wie die Debatte im Rat über die zentrale Anlaufstelle für Unternehmen gezeigt hat, handelt es sich hierbei keineswegs um

[203] Eine solche Bestimmung fand sich in dem Vorschlag der Kommission für die Verordnung, wurde jedoch später gestrichen. Parlament und Rat prüfen verschiedene Fassungen einer ähnlichen Bestimmung. Ihr Nutzen würde über Überwachung hinausgehen und auch andere Bereiche betreffen, in denen internationale Normenkollisionen oder Fragen der öffentlichen Ordnung auftreten können und bei denen es in der Regel um gesetzliche Verpflichtungen geht, die den Zugang zu Informationen in anderen Rechtsordnungen verlangen.

eine rein theoretische Diskussion.[204] Im Zusammenhang mit dem Grundsatz der zentralen Anlaufstelle wurden rechtliche Bedenken hinsichtlich seiner Vereinbarkeit mit der Charta und hier vor allem mit Artikel 47 über das Recht auf wirksamen Rechtsbehelf und ein unparteiisches Gericht geäußert. Diese Einwände überzeugen zwar nicht vollständig, weisen jedoch darauf hin, dass es tatsächlich verschiedene Grenzen gibt, die der EU-Gesetzgeber zu respektieren hat.[205]

Der Gerichtshof hat auch nachgewiesen, dass derartige Grenzen bestehen. Das beste Beispiel hierfür ist die Rechtsprechung zum Erfordernis der „völligen Unabhängigkeit" von Aufsichtsbehörden. Der Gerichtshof hat verschiedentlich festgestellt, das Erfordernis einer unabhängigen Kontrolle sei ein „wesentliches Element" der Wahrung des Schutzes personenbezogener Daten, das sich aus Artikel 8 Absatz 3 der Charta und Artikel 16 Absatz 2 AEUV ergebe.[206] Dies bedeutet, es steht dem EU-Gesetzgeber nicht völlig frei, den bestehenden Rahmen auf eine Weise zu überarbeiten, die mit diesen Bestimmungen des Primärrechts nicht in Einklang stünde.

Ähnliches ließe sich aus dem jüngst ergangenen Urteil des Gerichtshofs über die Stellung von Suchmaschinenbetreibern ableiten. Da der Geltungsbereich des Rechts der betroffenen Person auf Löschung und auf Widerspruch gegen die Verarbeitung personenbezogener Daten gemäß der bestehenden Richtlinie unter ausdrücklicher Erwähnung von Artikel 7 und 8 der Charta abgesteckt wurde,[207] wäre es undenkbar, den Geltungsbereich dieser Rechte ohne angemessene Berücksichtigung der Anforderungen der Charta an jegliche Einschränkung der Ausübung der ausdrücklich in Artikel 8 Absatz 2 und implizit in Artikel 8 Absatz 1 der Charta verankerten Rechte einzuschränken. Der Gerichtshof kam der Feststellung sehr nahe, dass diese Rechte (ebenfalls) „wesentliche Elemente" des Schutzes personenbezogener Daten gemäß Artikel 8 seien. Gleiches könnte in Zukunft mit Blick auf andere Elemente von Artikel 8 geschehen.

Ganz allgemein bedeutet dies, dass Artikel 7 und 8 sowie andere relevante Bestimmungen der Charta in der Diskussion über die Verordnung, bei ihrer Annahme und schließlich bei ihrer Anwendung in der Praxis zu berücksichtigen sind. Und genau hier könnte es sein, dass der Unterschied im Wesen des Rechts auf Achtung des Privatlebens und des Rechts auf den Schutz personenbezogener Daten erneut eine wichtige Rolle spielt. Artikel 7 diente dann vorrangig als Schild gegen ungebührliche Eingriffe in das Privatleben von Personen, während

[204] Siehe weiter oben Abschnitt 6 Teil C.
[205] Siehe hierzu, in einem anderen Zusammenhang, *Digital Rights Ireland* (Fußnote 97), Randnr. 47: „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".
[206] Siehe Fußnote 95.
[207] Siehe Fußnote 195.

Artikel 8 positiv garantieren würde, dass die in dieser Bestimmung verankerten Kernelemente des Schutzes personenbezogener Daten angemessen in die Praxis umgesetzt werden.

Das impliziert wiederum, dass die Verordnung so konzipiert und angewandt werden sollte, dass die Verarbeitung personenbezogener Daten, sei es durch öffentliche oder private Akteure, keinen ungebührlichen Eingriff in das Privatleben von Personen darstellt und dass die wesentlichen Elemente des Datenschutzes sowohl im öffentlichen als auch im privaten Sektor gegeben sind. Jede Verkleinerung des Anwendungsbereichs oder Absenkung des Schutzniveaus nach der bestehenden Richtlinie könnte daher mit gutem Grund unter Berufung auf Artikel 7 und 8 der Charta angefochten werden.

B. Rechenschaftspflicht und Einhaltung der Vorschriften

In Abschnitt 5 Teile B und C haben wir bereits erwähnt, dass eine der wichtigsten Neuerungen der Verordnung darin besteht, dass von der Vorabkontrolle zur Ex post-Kontrolle durch Datenschutzbehörden und von nominaler Verantwortlichkeit zu verstärkter Verantwortlichkeit oder Rechenschaftspflicht des für die Verarbeitung Verantwortlichen übergegangen wurde. Ein Kommentator hat diese Verschiebung als eine „kopernikanische Revolution im europäischen Datenschutzrecht" bezeichnet.[208] Auch wenn diese Formulierung vielleicht ein bisschen übertreibt, unterstreicht sie doch, dass ein völlig anderer Ansatz gewählt wurde, um den Datenschutz in der Praxis wirksamer zu machen.

Es sei kurz erläutert, welche Konsequenzen diese Verschiebung hat. Zunächst einmal ändert sie nichts an der bestehenden Verantwortung des für die Verarbeitung Verantwortlichen, der für die Beachtung der grundlegenden Prinzipien des Datenschutzes und die Wahrung spezifischer Rechte betroffener Personen zu sorgen hat. Vorbehaltlich einiger Klarstellungen und Verbesserungen in der Verordnung bleiben alle diese Kernelemente unangetastet.

In der bestehenden Richtlinie wird dies durch eine allgemeine Pflicht zur Vorabmeldung von Datenverarbeitungen bei der zuständigen Datenschutzbehörde, für die es Ausnahmen geben kann, oder durch eine Pflicht zur Vorabkontrolle bei risikobehafteten Verarbeitungsvorgängen ergänzt.[209] In der Praxis hat dies nicht nur zu einer sehr großen Vielfalt in den Mitgliedstaaten geführt, und zwar sowohl bei der Meldepflicht und den Ausnahmen als auch bei den einzelstaatlichen Vorgehensweisen in den einzelnen Kategorien. Viel wichtiger ist, dass verantwortliche Organisationen tendenziell die Meldung und nicht die Einhaltung der Datenschutzgrundsätze als ihre Hauptverpflichtung ansehen. Damit hat die Funktion von Datenschutzbehörden zu viel Gewicht erhalten, und dies zu Lasten der Aufgabe der für die Verarbeitung Verantwortlichen, in ihren Organisationen für guten Datenschutz zu

[208] Siehe C. Kuner (Fußnote 128).
[209] Artikel 18-20.

sorgen. Die Verpflichtung zur Vorabmeldung einzelner Verarbeitungen wird heute weitgehend als unwirksamer und unnötiger Verwaltungsaufwand betrachtet.

Stattdessen hat die Verordnung nun der Verantwortlichkeit der für die Verarbeitung Verantwortlichen größeres Gewicht beigemessen. Dies bedeutet, dass sie nicht nur die grundlegenden Prinzipien einzuhalten und die Rechte betroffener Personen zu wahren haben, sondern auch alle erforderlichen Schritte ergreifen müssen, um die Einhaltung der Vorschriften zu gewährleisten, sowie überprüfen und nachweisen müssen, dass diese Maßnahmen vorhanden und weiterhin wirksam sind. [210] Dieser Grundsatz der Rechenschaftspflicht sollte vorbehaltlich des in Abschnitt 6 Teil B erwähnten „gestaffelten" risikogestützten Ansatzes ein besseres *Datenmanagement* in der Praxis zur Folge haben. Die Befugnisse der Datenschutzbehörden zur Durchsetzung und zur Verhängung von Sanktionen wegen Nichteinhaltung der Vorschriften wurden ebenfalls spürbar verstärkt.[211]

Die eigenständige Verpflichtung, angemessene Maßnahmen zu ergreifen und deren Existenz und fortgesetzte Wirksamkeit nachzuweisen, soll als Anreiz für die für die Verarbeitung Verantwortlichen und als Instrument für die Datenschutzbehörden bei der Überwachung von Datenmanagementpraktiken dienen, ohne unbedingt zeitaufwändige Analysen inhaltlicher Fragen durchführen zu müssen. Ein „gestaffelter" risikogestützter Ansatz, wie er bereits erwähnt wurde, würde in diesem Zusammenhang sowohl für die für die Verarbeitung Verantwortlichen als auch für die Datenschutzbehörden gut funktionieren. Hierzu dürften einige praktische Hinweise von diesen Behörden erforderlich sein, am besten im Rahmen des Europäischen Datenschutzausschusses, damit eine ausreichende EU-weite Kohärenz gewährleistet ist.

Es lässt sich unschwer voraussagen, dass für die Verarbeitung Verantwortliche Beratung dazu suchen werden, wie sie in ihren Organisationen die Einhaltung der Vorschriften am besten gewährleisten. Dies bedeutet, dass steigende Nachfrage nach Datenschutzexperten sowie für den Datenschutz relevanten Produkten und Dienstleistungen bestehen wird, möglicherweise mit einer Zertifizierung auf der Grundlage der Verordnung.[212] Auf der anderen Seite sieht die Verordnung eine vielfältige Auswahl an Optionen für die Durchsetzung vor, die von Einzel- oder Sammelklagen interessierter Parteien bis hin zu verschiedenen Eingriffen von Datenschutzbehörden reicht, unter Umständen im Zusammenhang mit der zentralen Anlaufstelle, unterstützt durch das Kohärenzverfahren und die Funktion des Europäischen Datenschutzausschusses. Mit anderen Worten: Die für die Verarbeitung Verantwortlichen können ihrer Verantwortung nachkommen, bei Bedarf mithilfe anderer, und Gegenstand

[210] Artikel 22.
[211] Artikel 53 und 79.
[212] Artikel 39.

verschiedener Durchsetzungsmaßnahmen in Abhängigkeit davon sein, ob sie mehr oder weniger erfolgreich sind.

Auf diese Weise wird die Verordnung eine bessere Verteilung von Verantwortlichkeiten erreichen und einige attraktive Anreize für die Einhaltung der Vorschriften bieten, die vermutlich einen wirksameren Schutz in der Praxis zur Folge haben.

C. Unabhängige Aufsicht und Kohärenz

Das Erfordernis einer unabhängigen Aufsicht ist weiter oben bereits mehrfach als ein „wesentliches Element" des Datenschutzes bezeichnet worden, und der Bedarf an größerer Kohärenz wurde ebenfalls als Voraussetzung für eine größere Wirksamkeit dieses Rechts überall in der EU genannt. Sind aber diese beiden Anforderungen miteinander vollkommen vereinbar? Auf den ersten Blick scheint es sich um ein echtes Paradoxon in der Governance des EU-Datenschutzes zu handeln.

Nach der Rechtsprechung des Gerichtshofs bedeutet das Erfordernis der „vollständigen Unabhängigkeit" einer Kontrollstelle, dass diese frei von *jedem* äußeren Einfluss sein muss.[213] Das schließt natürlich nicht aus, dass diese Behörden zusammenarbeiten und zu gewissen Fragen eine gemeinsame Haltung erarbeiten. Bei Meinungsverschiedenheiten ist allerdings die Frage, wer eine verbindliche Entscheidung trifft, dazu angetan, große Probleme aufzuwerfen. Sollte eine Minderheit durch die Ansichten einer Mehrheit gebunden sein, käme dies direktem externem Einfluss gleich und wäre mit der vollständigen Unabhängigkeit kaum vereinbar. Stünde es hingegen jeder Aufsichtsbehörde frei, ihre eigenen Ansichten umzusetzen, wäre es praktisch unmöglich, bei irgendeinem Thema Kohärenz zu erreichen.

Es sei darauf hingewiesen, dass am Ende des in der vorgeschlagenen Verordnung vorgesehenen Kohärenzverfahrens keine verbindliche Entscheidung, sondern eine *Stellungnahme* steht, aufgrund derer die zuständige Datenschutzbehörde ihre Haltung überdenken müsste.[214] Wird der Stellungnahme Folge geleistet, entsteht kein Problem. Wäre die zuständige Datenschutzbehörde mit ihr nicht einverstanden, gäbe es theoretisch im Wesentlichen zwei Optionen.

Erste Option: Die zuständige Datenschutzbehörde begründet ihre Haltung und erläutert, warum sie sich nicht an die Stellungnahme hält. Dies hätte zweifelsohne eine genaue Prüfung der Maßnahme durch die interessierten Parteien und alle anschließend beteiligten Gerichte zur Folge. Diese Option würde die Unabhängigkeit in vollem Umfang wahren, lediglich Verfahrensdruck schaffen, möglicherweise aber auch zu einer eingeschränkten Kohärenz führen, dies jedoch vielleicht erst nach einer endgültigen Entscheidung des Gerichtshofs.

[213] Siehe Fußnoten 51 und 52.
[214] Artikel 58.

Zweite Option: Das Kohärenzverfahren tritt in eine neue Phase ein. In diesem Zusammenhang hatte die Kommission eine größere Rolle für sich selbst vorgesehen, zunächst durch Vorlage einer Stellungnahme, aufgrund derer die zuständige Behörde ihre Haltung noch ernsthafter überdenken müsste, dann durch Aussetzung der ins Auge gefassten Maßnahme und schließlich durch eine allgemeine verbindliche Regelung der Frage im Wege eines Durchführungsrechtsakts.[215] Dieser Ansatz wurde weitgehend als unangemessen kritisiert. Obwohl die Kommission gemäß den Verträgen verpflichtet ist, ihre Tätigkeit in voller Unabhängigkeit auszuüben[216], verfolgt diese Anforderung doch ein anderes Ziel und würde als Rechtfertigung eines direkten Eingriffs in einen Fall vor einer unabhängigen Behörde nicht ausreichen.

Dieser Sachverhalt hat ein Überdenken der Frage angestoßen, wie unabhängige Behörden möglicherweise beim Erreichen guter und kohärenter Ergebnisse zusammenarbeiten können. So gab es den Vorschlag, Fragen, die rein oder überwiegend lokaler Natur sind – wenn also alle Akteure in einem Land ansässig sind oder sich Probleme aufgrund lokalen Rechts ergeben –, ganz den lokalen zuständigen Datenschutzbehörden zu überlassen. Sind mehrere Rechtsordnungen betroffen, weil entweder der für die Verarbeitung Verantwortliche Niederlassungen in mehreren Rechtsordnungen hat oder natürliche Personen aus verschiedenen Rechtsordnungen betroffen sind, sollte die erste Regel lauten, dass die zuständigen Behörden bei der Suche nach einer Lösung des Problems zusammenarbeiten sollten, die alle Beteiligten mittragen können. In einer solchen Situation könnte die Benennung einer federführenden Behörde auch dann sinnvoll sein, wenn ein für die Verarbeitung Verantwortlicher nur in einer Rechtsordnung niedergelassen ist, aber natürliche Personen aus mehreren Rechtsordnungen betroffen sind. Es kann auch vorkommen, dass der für die Verarbeitung Verantwortliche in der EU überhaupt keine Niederlassung hat, aber natürliche Personen in allen Mitgliedstaaten betroffen sind. Für die Benennung einer solchen federführenden Behörde könnten daher unterschiedliche Szenarien erwogen werden. Solange jedoch das Ergebnis der Zusammenarbeit innerhalb einer angemessenen Frist im Konsensverfahren erreicht wird, besteht mit der Unabhängigkeit kein Problem.

Falls die Zusammenarbeit zwischen den Datenschutzbehörden innerhalb einer angemessenen Frist nicht zu einem Konsens führt, sollte die Frage zur Erörterung an den Europäischen Datenschutzausschuss „hochgereicht“ werden. Wird nach der Diskussion dort eine einmütige Entscheidung erzielt, besteht ebenfalls kein Problem mit der Unabhängigkeit. Gibt es jedoch Mehrheit und Minderheit, sind grundsätzlich zwei Szenarien denkbar. Erstens: Die Meinung der Mehrheit hat nur den Rang einer *Stellungnahme*, die die zuständige Datenschutzbehörde zumindest äußerst sorgfältig prüfen sollte. Besteht auch weiterhin keine Einmütigkeit,

[215] Artikel 59-62.
[216] Artikel 17 Absatz 3 dritter Unterabsatz EUV.

bestünde die Möglichkeit einer Zweitstellungnahme, die dann aber mit qualifizierter Mehrheit anzunehmen wäre. Dies entspräche dem Ansatz, den Verfahrensdruck zu erhöhen, ohne dabei jedoch die Entscheidungsbefugnis der zuständigen Datenschutzbehörde zu beschränken. Es würde ferner auf der Annahme gründen, dass eine Zweitstellungnahme großen Einfluss hätte, ohne jedoch alle Einzelheiten eines Falls vollständig zu entscheiden.

Zweitens: Es wird ein Entscheidungsfindungsverfahren auf einer anderen Ebene eingeführt, beispielsweise im Zusammenhang mit dem Europäischen Datenschutzausschuss. Diese Option könnte sich nachteilig auf die gerichtliche Überprüfung von Entscheidungen auswirken und zu einer unerwünschten Zentralisierung führen. Es gab noch weitere Lösungsvorschläge, doch lösten sie nicht vollständig das Problem einer anders denkenden Minderheit und eines möglichen Mangels an Kohärenz.

Dies erklärt, weshalb die Governance-Fragen im Zusammenhang mit dem Kohärenzverfahren sowie die Architektur der zentralen Anlaufstelle für Unternehmen zu den kompliziertesten und noch immer diskutierten Fragen gehören und dass unterschiedliche Lösungen auf dem Weg zu einem annehmbaren Kompromiss geprüft werden.

8. Schlussbemerkungen

Das Ergebnis der derzeitigen Überprüfung der Richtlinie 95/46/EG – und des EU-Rechtsrahmens für den Datenschutz ganz allgemein – steht noch nicht ganz fest, aber an ihrer Hauptrichtung wird sich nichts mehr ändern; es gibt keine Umkehr mehr. Auf jeden Fall lassen sich schon jetzt einige Schlussfolgerungen ziehen.

Zwischen Privatsphäre und Datenschutz, genauer gesagt: zwischen dem Recht auf *Achtung* der Privatsphäre und dem Recht auf den *Schutz* personenbezogener Daten, bestehen wichtige Verbindungen. Beide sind noch recht junge Ausdrucksformen einer universellen Idee mit starken ethischen Dimensionen: der Würde, Autonomie und *Einzigartigkeit* jedes Menschen. Es bestehen aber auch entscheidende Unterschiede. Das Konzept des „Datenschutzes“ wurde entwickelt, um strukturell natürlichen Personen rechtlichen Schutz gegen den unangemessenen Einsatz der Informationstechnologie zur Bearbeitung sie betreffender Daten zu bieten, und zwar *unabhängig* davon, ob diese Verarbeitung unter das Recht auf Achtung vor dem Privatleben fällt oder nicht. Das dabei entstandene Paket von Garantien – im Wesentlichen ein System von Kontrollen und Gegenkontrollen, bestehend aus sachlichen Voraussetzungen, individuellen Rechten, Verfahrensbestimmungen und unabhängiger Kontrolle – findet grundsätzlich auf alle Verarbeitungen personenbezogener Daten Anwendung.

Dieser Ansatz wurde seinerzeit vom Europarat im Übereinkommen Nr. 108 entwickelt und von der EU in der Richtlinie 95/46/EG weiterentwickelt, parallel zu dem in Artikel 8 EMRK verankerten Recht auf Achtung des Privatlebens. Beide müssen einerseits vom deutschen Konzept der „informationellen Selbstbestimmung", bei dem die Einwilligung der betroffenen Person im Vordergrund steht, und andererseits vom Ansatz der OECD-Leitlinien unterschieden werden, der auf dem Begriff des „Risikos" als einer *Schwellen*bedingung für Schutz beruht und davon ausgeht, dass grundsätzlich jegliche Verarbeitung personenbezogener Daten legitim ist. Diese Unterscheidungen spielen in internationalen Diskussionen eine wichtige, häufig aber nur unausgesprochene und unzureichend anerkannte Rolle.

Ganz allmählich hat die EU vom Europarat die Funktion einer Plattform übernommen, auf der über Datenschutz gesprochen wird. Diesbezüglich hat es eine zweigleisige Entwicklung gegeben: Zum einen geht es darum, die Rechte auf Privatsphäre und Datenschutz *stärker* zu machen, zum anderen soll eine *kohärent*ere Anwendung dieser Rechte in der gesamten EU gewährleistet werden. In beiden Fällen wird ein *wirksamerer* Schutz in der Praxis und weniger *nicht gerade hilfreiche Vielfalt* bei der Erbringung des Schutzes in den Mitgliedstaaten angestrebt. Die wachsenden Auswirkungen der Charta der Grundrechte sowohl auf die Rechtsprechung des Gerichtshofs als auch auf die Überprüfung des bestehenden Rechtsrahmens passen zu dieser langfristigen Tendenz. Dies ist natürlich zu begrüßen, da der Bedarf an einem wirksamen Schutz personenbezogener Daten niemals größer war als heute.

Die Unterscheidung zwischen „Privatsphäre" und „Datenschutz" ist auch für die Charta von Belang. Artikel 7 über das Recht auf Achtung des Privatlebens ist ein typisches Beispiel für ein klassisches Grundrecht, bei dem ein *Eingriff* nur unter strengen Bedingungen erfolgen darf. Artikel 8 über den Schutz personenbezogener Daten lehnt sich mit seinem System eines eher proaktiven Schutzes an das Übereinkommen Nr. 108 und die Richtlinie 95/46/EG an. Dies bedeutet, dass der *Geltungsbereich* von Artikel 8 – alle Verarbeitungen personenbezogener Daten – nicht mit der Frage verwechselt werden sollte, ob es einen *Eingriff* in das in Artikel 8 verankerte Grundrecht gegeben hat. Ein solcher Eingriff liegt normalerweise nur vor, wenn eines oder mehrere Elemente von Artikel 8 Absatz 2 und Artikel 8 Absatz 3 nicht gewahrt wurden. Es kann jedoch nicht ausgeschlossen werden, dass auch Artikel 8 Absatz 1 als Quelle anderer Anforderungen dient, die zwar schon im EU-Datenschutzrecht vorgesehen sind, in der Charta aber noch nicht ausdrücklich verankert wurden.

In seiner jüngeren Rechtsprechung hat der Gerichtshof die Neigung an den Tag gelegt, Artikel 7 und 8 der Charta als „Paket" zu betrachten. Wie wir bereits erläutert haben, trägt dieser Ansatz den erheblichen Unterschieden im Wesen dieser beiden Bestimmungen nicht

Rechnung und verhindert möglicherweise, dass das Potenzial von Artikel 8 voll ausgeschöpft wird. Der Gerichtshof scheint jedoch noch immer mit der richtigen Funktion von Artikel 8 der Charta zu kämpfen und verwendet mitunter verschiedene Terminologien.

Die allgemeine Grundlage für die Überarbeitung der derzeitigen Rechtsrahmens in Artikel 16 AEUV bietet die historische Gelegenheit, die wichtigsten Bestandteile von Artikel 8 der Charta in ein wirksameres und kohärenteres Regelwerk für die gesamte EU zu überführen. Die Datenschutz-Grundverordnung, die zu gegebener Zeit an die Stelle der Richtlinie 95/46/EG treten soll, vereint Kontinuität und Innovation. Eine unmittelbar geltende Verordnung bringt grundsätzlich mehr Kohärenz mit sich, wird in der Praxis aber auch einen gewissen Spielraum für das Zusammenspiel mit einzelstaatlichem Recht lassen, insbesondere im öffentlichen Sektor. Die größten Neuerungen dürfte es bei der gestiegenen Verantwortung der für die Verarbeitung Verantwortlichen geben, auch wenn die Auswirkungen dieser Verlagerung von dem derzeit erörterten „gestaffelten risikogestützten Ansatz“ abhängen werden. Neuerungen sind auch bei Kontrolle und Durchsetzung zu erwarten, insbesondere im Hinblick auf die Details von zentralen Anlaufstellen für Bürger und Unternehmen, und bei anderen Mechanismen, mit denen kohärente Ergebnisse unabhängiger Aufsichtsbehörden gewährleistet werden sollen. Schließlich wird der territoriale Anwendungsbereich der Verordnung vermutlich auch Unternehmen umfassen, die auf dem EU-Markt von einer Niederlassung in anderen Teilen der Welt aus tätig sind.

Da die Charta im Anwendungsbereich des EU-Rechts stets anzuwenden ist, gilt sie auch für den Rechtsrahmen, der irgendwann auf der Grundlage von Artikel 16 AEUV angenommen werden wird. Daraus ergibt sich die Frage, welchen Spielraum der Gesetzgeber bei der Annahme dieser Vorschriften haben wird. Wir haben in unserer Diskussion verschiedene Beispiele eines Ermessensspielraums kennengelernt, der eingeschränkt ist, weil entweder Artikel 8 der Charta bereits bestimmte positive Anforderungen enthält oder weil die Charta auch immer dann eingehalten werden muss, wenn Vorschriften über Datenverarbeitung als Grundlage für einen Eingriff in das Recht auf Achtung des Privatlebens dienen. Probleme mit der Charta dürften ferner auftreten, wenn der Anwendungsbereich der neuen Vorschriften enger oder das von ihnen gebotene Schutzniveau niedriger wäre als im bestehenden Rechtsrahmen.

Schließlich haben wir gesehen, dass Governance-Fragen im Zusammenhang mit der zentralen Anlaufstelle für Unternehmen und das Kohärenzverfahren zu den kompliziertesten Themen gehören, die derzeit noch in der Diskussion sind. Hier werden sowohl Kreativität als auch Pragmatismus vonnöten sein, um zu gewährleisten, dass die wesentlichen Elemente von Artikel 8 der Charta wirksam in die Praxis umgesetzt werden können.