Peter Hustinx
Europäischer Datenschutzbeauftragter

Führende Rolle Europas beim Schutz der Privatsphäre und beim Datenschutz[1]

Dieses Buch mit Beiträgen zur vorgeschlagenen Datenschutz-Grundverordnung der EU bietet eine hervorragende Gelegenheit, die führende Rolle Europas beim Schutz der Privatsphäre und beim Schutz personenbezogener Daten zu unterstreichen. Diese Rolle hat sich im Laufe von Jahrzehnten entwickelt, auf europäischer Ebene zunächst im Rahmen des Europarates, später dann im Wesentlichen im Rahmen der Europäischen Union. In diesem Zusammenhang ist deutlich geworden, dass zunehmend zwischen „Privatsphäre" und „Datenschutz" als zwei eigenständigen Konzepten unterschieden wurde, in jüngerer Zeit auch in der Charta der Grundrechte der Europäischen Union. Gleichzeitig war zu beobachten, dass ein *stärkerer* und *wirksamerer* Schutz personenbezogener Daten und ein *kohärenterer* Schutz in allen EU-Mitgliedstaaten immer größeres Gewicht erhielten. Alle diese Strömungen fließen in dem Vorschlag für eine Datenschutz-Grundverordnung zusammen. Natürlich war der Bedarf an einem starken, wirksamen und kohärenten Schutz personenbezogener Daten niemals größer und dürfte er in Zukunft wohl noch wachsen.

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

Das Konzept des „Datenschutzes" wurde vor 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 für jegliche Verwendung der Informationstechnologie zur Verarbeitung von Daten über natürliche Personen Garantien zu bieten. Grundlage war die früh gewonnene Überzeugung,

[1] Dieser Artikel wird erscheinen in: "Hacia un nuevo régimen europeo de protección de datos / Towards a new European Data Protection Regime", Valencia 2015.

dass der intensive Einsatz der Informationstechnologie für diesen Zweck weit reichende Auswirkungen auf die Rechte und Interessen natürlicher Personen haben könnte.

2. Das Konzept des „Rechts auf Privatsphäre“ tauchte erst nach dem Zweiten Weltkrieg im internationalen Recht auf. Zunächst erschien es relativ schwach ausgeprägt in Artikel 12 der Allgemeinen Erklärung der Menschenrechte, dem zufolge niemand *willkürlichen* Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr ausgesetzt werden darf.

Stärkeren Schutz bot später Artikel 8 der Europäischen Menschenrechtskonvention (EMRK), 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“ lässt sich auf verfassungsrechtliche Traditionen in vielen Ländern weltweit zurückführen, als gemeinsames Erbe einer langen Entwicklung, die sich mitunter über viele Jahrhunderte erstreckte, aber die Hervorhebung von „Privatsphäre“ und „Privatleben“ war neu und ganz offensichtlich eine Reaktion auf die Ereignisse während des Zweiten Weltkriegs.

Den Geltungsbereich und die Konsequenzen dieses Schutzes hat der Europäische Gerichtshof für Menschenrechte in einer Reihe von Urteilen erläutert. 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 dem so sein sollte, ob es dafür eine *angemessene*, also klare, nachvollziehbare und vorhersehbare Rechtsgrundlage gab, und ob er für die fraglichen legitimen Interessen *notwendig* und verhältnismäßig war.

3. Zu Beginn der 1970er Jahre befand der Europarat, Artikel 8 EMRK weise im Hinblick auf neue Entwicklungen, insbesondere im Hinblick auf den wachsenden Einsatz von Informationstechnologie, eine Reihe von Schwachstellen auf: Es wird nicht ganz klar, was genau unter „Privatleben“ zu verstehen ist, dem Schutz vor Eingriffen durch „Behörden“ wird große Bedeutung beigemessen, und es fehlt an einem eher proaktiven Ansatz, der auch einen möglichen Missbrauch personenbezogener Daten durch Unternehmen oder andere relevante Organisationen im privaten Sektor erfassen würde.

Das Ergebnis war im Januar 1981 die Annahme des Datenschutzübereinkommens, auch bekannt als Übereinkommen Nr. 108, das bisher von 46 Staaten ratifiziert worden ist, darunter alle EU-Mitgliedstaaten, die meisten Mitgliedstaaten des Europarats und ein Nicht-

Mitgliedstaat.[2] Zweck dieses Übereinkommens ist es, 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"). Der Begriff „personenbezogene Daten" ist definiert als „jede Information über eine bestimmte oder bestimmbare natürliche Person („Betroffener").

Das bedeutet, dass „Datenschutz" *breiter gefasst* ist als „Schutz der Privatsphäre", weil er auch andere Grundrechte und -freiheiten abdeckt, außerdem alle Arten von Daten unabhängig von ihrer Beziehung zur Privatsphäre; gleichzeitig ist der Begriff *eingeschränkter*, weil er sich nur auf die Verarbeitung personenbezogener Daten bezieht und andere Aspekte des Schutzes der Privatsphäre außer Acht lässt.

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 verbunden sind. Das eigentliche Ziel des Übereinkommens besteht daher darin, natürliche Personen (Bürger, Verbraucher, Arbeitnehmer usw.) vor der unberechtigten Erhebung, Speicherung, Verwendung und Weitergabe ihrer 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 Entscheidungsprozessen gehen.

4. Das Übereinkommen enthält einige grundlegende Prinzipien für den Datenschutz, die jede Vertragspartei in innerstaatliches Recht umsetzen muss. Diese Grundsätze bilden den Kern aller einzelstaatlichen Rechtsvorschriften in diesem Bereich. Das Übereinkommen geht *nicht* davon aus, dass die Verarbeitung personenbezogener Daten immer als *Eingriff* in das Recht auf Privatsphäre betrachtet werden sollte, sondern stützt sich eher auf den Gedanken, dass zum Schutz der Privatsphäre und anderer Grundrechte und -freiheiten bei jeder Verarbeitung personenbezogener Daten *immer* bestimmte rechtliche Bedingungen erfüllt sein müssen. Dazu gehört der Grundsatz, dass personenbezogene Daten nur für konkrete rechtmäßige Zwecke verarbeitet werden dürfen, sofern dies für diese Zwecke erforderlich ist, und dass sie nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise verwendet werden dürfen.

Gestützt auf diesen Ansatz wurden die Kernelemente von Artikel 8 EMRK, wie ein Eingriff in das Recht auf Privatsphäre nur mit einer angemessenen Rechtsgrundlage und gegebenenfalls für einen rechtmäßigen Zweck, in einen größeren Kontext übernommen. Dies funktioniert in der Praxis allerdings nur, wenn das im Übereinkommen vorgesehene System

[2] Im April 2013 ratifizierte Uruguay als erster Nicht-Mitgliedstaat das Übereinkommen.

von Kontrolle und Gegenkontrolle - bestehend aus materiellen Bedingungen, individuellen Rechten, Verfahrensbestimmungen und unabhängiger Aufsicht – hinreichend flexibel ist, um unterschiedliche Gegebenheiten berücksichtigen zu können, und wenn es pragmatisch angewandt wird und den Interessen betroffener Personen und anderer wichtiger Akteure gegenüber aufgeschlossen ist. 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.

Das Übereinkommen hat in den meisten Mitgliedstaaten des Europarates bei der Formulierung ihrer Gesetzgebungsstrategie eine wichtige Rolle gespielt. In diesem Zusammenhang ist der „Datenschutz“ von Anfang an als eine Frage von großer struktureller Bedeutung für eine moderne Gesellschaft betrachtet worden, in der der Verarbeitung personenbezogener Daten eine ständig wachsende Bedeutung zukommt.

5. 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. 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. Dieser Ansatz sollte 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 großen Einfluss hatten, insbesondere in nicht-europäischen Ländern wie den Vereinigten Staaten, Kanada, Australien und Japan. 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“. 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 Weiteren fehlten in den Leitlinien das Erfordernis eines *rechtmäßigen* Zwecks und einer

gesetzlichen Grundlage für die Verarbeitung personenbezogener Daten generell. Beide Aspekte spielen in den weltweiten Diskussionen noch immer eine sehr wichtige Rolle.

6. Der Europarat setzte zwar mit großem Erfolg den „Datenschutz“ auf die Tagesordnung und legte die Kernelemente eines Rechtsrahmens fest, doch war er weniger erfolgreich bei der Gewährleistung einer ausreichenden Kohärenz in seinen Mitgliedstaaten. Einige Mitgliedstaaten setzten das Übereinkommen Nr. 108 mit Verspätung um, und diejenigen, die es umsetzten, gelangten zu unterschiedlichen Ergebnissen, wobei in einigen Fällen sogar der Datenverkehr mit anderen Mitgliedstaaten eingeschränkt wurde.

Die Europäische Kommission hegte daher große Bedenken, dass dieser Mangel an Kohärenz die Entwicklung des Binnenmarktes in einer Reihe von Bereichen – einschließlich der Freizügigkeit und des freien Dienstleistungsverkehrs – behindern könnte, in denen die Verarbeitung personenbezogener Daten eine immer wichtigere Rolle spielen würde. Ende 1990 legte sie daher den Entwurf einer Richtlinie zur Harmonisierung der einzelstaatlichen Rechtsvorschriften über den Datenschutz im privaten und in weiten Teilen des öffentlichen Sektors vor. Nach vierjährigen Verhandlungen kam es zur Annahme der derzeit geltenden Richtlinie 95/46/EG, die zweierlei Ziele verfolgt: Gewährleistung eines hohen Schutzniveaus für personenbezogene Daten in allen Mitgliedstaaten und Gewährleistung eines freien Datenverkehrs zwischen Mitgliedstaaten vorbehaltlich vereinbarter Garantien.

Damit ging die Richtlinie von den im Übereinkommen Nr. 108 des Europarates niedergelegten Grundprinzipien des Datenschutzes aus. Gleichzeitig führte sie diese Grundsätze näher aus und ergänzte sie durch weitere Anforderungen und Bedingungen. Da in der Richtlinie jedoch allgemein formulierte Konzepte und offene Standards niedergelegt wurden, verfügten die Mitgliedstaaten bei ihrer Umsetzung immer noch über einen beachtlichen Ermessensspielraum. Im Ergebnis hat die Richtlinie zu mehr Kohärenz zwischen Mitgliedstaaten geführt, aber mit Sicherheit nicht zu identischen oder vollständig übereinstimmenden Lösungen.

Da die Richtlinie außerdem in einer Zeit angenommen wurde, in der das Internet noch in den Kinderschuhen steckte, dürfte klar sein, dass der Bedarf an stärkerem Schutz und mehr Kohärenz erst in den letzten Jahren gewachsen ist. Zu beiden Punkten sollen mit der vorgeschlagenen Datenschutz-Grundverordnung die nächsten Schritte unternommen werden.

7. Auch wenn die Richtlinie mit dem Ziel angenommen wurde, das reibungslose Funktionieren des Binnenmarktes zu gewährleisten, vermittelten ihre Geschichte und ihr Hintergrund noch eine weiter reichende Botschaft. Der Europäische Gerichtshof hat seitdem wiederholt die Auffassung vertreten, dass sie einen weiten Anwendungsbereich hat und auch

für den öffentlichen Sektor der Mitgliedstaaten maßgeblich ist.[3] Dieser Ursprung in den Grundrechten ist im Laufe der Jahre immer sichtbarer geworden.

Die Annahme der anfänglich als politisches Dokument gedachten EU-Charta der Grundrechte im Dezember 2000 ermöglichte weitere Entwicklungen in dieser Richtung. 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".

8. Die in Artikel 7 der Charta garantierten Rechte entsprechen denen, die in Artikel 8 EMRK garantiert werden. Beide sind typische Beispiele für klassische Grundrechte, bei denen ein *Eingriff* nur unter strengen Bedingungen erfolgen darf. Artikel 8 beruht weitgehend auf der Richtlinie 95/46/EG und auf dem Übereinkommen Nr. 108 des Europarates.

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 gedacht als ein System von Kontrollen und Gegenkontrollen, 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. Dabei wurden die wesentlichen Grundsätze des Datenschutzes, die Pflichten von für die Verarbeitung Verantwortlichen, die Rechte der betroffenen Personen und das Erfordernis einer unabhängigen Aufsicht zu den zentralen strukturellen Elementen des

[3] Verbundene Rechtssachen C-465/00, C-138/01 und C-139/01, *Österreichischer Rundfunk*, [2003] Slg. I-04989, Randnr. 41-43, und Rechtssache C-101/01, *Bodil Lindqvist*, [2003] Slg. I-12971, Randnr. 39-41. Siehe ferner Rechtssache C-524/06, *Huber*, [2008] Slg. I-09705, und Rechtssache C-553/07, *Rijkeboer*, [2009] Slg. I-03889.

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.

9. Der Konvent, der die Charta vor ihrer Annahme ausgearbeitet hat, 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. Die in Artikel 8 Absatz 2 und 3 verankerten Elemente wie Verarbeitung nach Treu und Glauben, Zweckbindung, Auskunfts- und Berichtigungsrecht und unabhängige Überwachung entsprechen somit den Kerngrundsätzen der Richtlinie 95/46/EG.

Außerdem kann nicht ausgeschlossen werden, dass der Gerichtshof noch andere Elemente des Datenschutzes findet, die ihren Ausdruck nicht 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.

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.

10. Das Inkrafttreten des Vertrags von Lissabon im Dezember 2009 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 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. 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 ausdrücklich erwähnt. Das bedeutet, dass einige der Hauptelemente der Richtlinie 95/46/EG nunmehr die Ebene des EU-Primärrechts erreicht haben.

Zweitens bietet Artikel 16 Absatz 2 AEUV jetzt eine allgemeine Rechtsgrundlage für gemäß dem ordentlichen Gesetzgebungsverfahren durch das Europäische Parlament und den Rat erlassene Vorschriften „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 Behörden überwacht wird.

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. 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.

11. Die allgemeine Grundlage für die Überarbeitung des 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 vorgeschlagene Datenschutz-Grundverordnung, die zu gegebener Zeit an die Stelle der Richtlinie 95/46/EG treten soll, vereint Kontinuität und Innovation. Alle grundlegenden Konzepte und Prinzipien wurden bekräftigt, in der Regel nach einer gewissen Klarstellung. Die Verordnung wird auch weiterhin einen breit gefassten Anwendungsbereich haben, höchstwahrscheinlich unter Einbeziehung des öffentlichen Sektors, und für betroffene Personen gestärkte Rechte, für für die Verarbeitung Verantwortliche stärkere Pflichten und für Kontrolle und Durchsetzung strengere Regelungen, einschließlich Geldbußen in Höhe mehrerer Millionen Euro, vorsehen. Dies geschieht in Anerkennung der wachsenden Bedeutung des Datenschutzes in der digitalen Wirtschaft.

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 „progressiven risikogestützten Ansatz“ (progressive risk based approach) abhängen wird. 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.

Der territoriale Anwendungsbereich der Verordnung wird vermutlich auch Unternehmen umfassen, die auf dem EU-Markt von einer Niederlassung in anderen Teilen der Welt aus tätig sind. Vor kurzem hat der Gerichtshof auf der Grundlage der derzeit geltenden Richtlinie in einem Urteil bereits einen interessanten Schritt in diese Richtung getan, indem er die kommerziellen Tätigkeiten der Niederlassung einer großen Suchmaschine in Spanien mit denen der eigentlichen Suchmaschine verknüpfte, die ihren Hauptsitz in den Vereinigten Staaten hat.[4]

12. Der Verordnungsvorschlag wurde natürlich nicht „im luftleeren Raum" erarbeitet. Sowohl der Europarat als auch die OECD sind dabei, ihre Regelwerke zu überarbeiten, und die Ergebnisse gehen offensichtlich alle in die gleiche Richtung, nämlich die eines wirksameren Datenschutzes in der Praxis. Die Verordnung dürfte daher - nach ihrer voraussichtlichen Annahme im Laufe des Jahres 2015 – eine starke Wirkung als Meilenstein zeitigen, sowohl für andere Länder in der Welt als auch für Wirtschaftsteilnehmer, deren Erfolg vielleicht von ihrer Fähigkeit abhängt, einen wirksamen Schutz der Privatsphäre und der personenbezogenen Daten ihrer Kunden zu gewährleisten.

[4] Rechtssache C-131/12, *Google Spain*, 13. Mai 2014, noch nicht veröffentlicht, Randnr. 55-56.