Modernes Datenschutzrecht in Europa

Vortrag von Prof. Dr. Alexander Roßnagel, Universität Kassel, am 28. Januar 2011 auf dem 5. Europäischen Datenschutztag „Datenschutz in Europa – Quo vadis?“ in Berlin

Herr Klingbeil hat nach einem Politiker und vor einer Politikerin einen Professor gebeten, zum Thema Modernisierung des Datenschutzrechts in Europa zu sprechen, um damit in Stil und Inhalt einen gewissen Gegenpol zu setzen. Ich will versuchen, dieser Erwartung gerecht zu werden. Ich werde daher nicht von aktuellen Debatten oder Dokumenten ausgehen, sondern will grundsätzliche Überlegungen zu Bedarf, Vorschlägen und Realisierung einer Modernisierung des Datenschutzes anstellen

Ich sehe zwei unterschiedliche Modernisierungsbedarfe, die aber zusammenhängen: Das Datenschutzrecht muss systematisch, verständlich und lesbar und es muss den wesentlichen gegenwärtigen und künftig absehbaren Herausforderungen für das Grundrecht auf informationelle Selbstbestimmung gerecht werden.

I. Der erste Modernisierungsbedarf betrifft einen eher formalen Aspekt: Das geltende Datenschutzrecht ist vielfach unübersichtlich, unlesbar, unsystematisch und widersprüchlich. Das hat zu einem wesentlichen Teil seinen Grund im Volkszählungsurteil. Für die unfreiwillige Erhebung und Verarbeitung personenbezogener Daten forderte das Bundesverfassungsgericht, „dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt“. Die ungewollte Folge dieser Forderung war eine Flut immer feiner differenzierender Normen für nahezu jeden Spezialbereich. Statt normenklarer, auch für den Bürger verständlicher Gesetze, entstand eine „überdetaillierte, unübersichtliche und schwer zu vollziehende Normenmasse“ (Kloepfer). In dieser finden sich heute verschiedene Schichten von Ablagerungen aus 40 Jahren Geschichte der Datenschutzgesetzgebung.

Daher muss jede Modernisierung die Fülle der Datenschutzregeln in weit über 1000 Gesetzen erheblich reduzieren und deren Begriffe, Konzepte, Systematiken und Anforderungen aufeinander abstimmen und systematisieren. Dieser Modernisierungsbedarf hat sich seit unserem Gutachten 2001 nicht verringert, im Gegenteil hat sich alles nur verschlimmert. Hier hängen beide Modernisierungsbedarfe miteinander zusammen. Wenn die Gesetzgeber aktuelle Probleme zu lösen versuchen, dann nicht dadurch, dass sie die überholte Grundstruktur des Datenschutzrechts anpassen. Vielmehr kleben sie an das bestehende Recht einfach nur zusätzliche Einschränkungen und Ausnahmen, Zusatzeinschränkungen und Rückausnahmen an. Dadurch trägt man zur Verständlichkeit des Datenschutzrechts nichts bei, sondern verschlimmbessert alles nur.

Denken sie nur an die Novellen aus dem Jahr 2009. Schauen Sie sich heute die Grundnorm des privaten Datenschutzrechts, § 28 BDSG, an. Von der Eleganz und Verständlichkeit einer Grundnorm, wie sie etwa im BGB zu finden sind, hat diese Vorschrift mit ihren 11 Absätzen und 1.429 Worten nichts, aber auch gar nichts. Mit jeder gesetzgeberischen Einzelreaktion auf ein aktuelles Thema ohne grundsätzliche Reform der Strukturen wird das Datenschutzrecht nur noch unverständlicher – ein Recht das dem Bürger Rechte geben soll und das er deswegen auch verstehen können muss.

II. Wichtiger aber ist die inhaltliche Seite. Dieser Teil der notwendigen Modernisierung betrifft die Risikoadäquanz und damit die Gegenwarts- und Zukunftsfähigkeit des Datenschutzrechts. Um diese zu gewährleisten, kann es nicht darum gehen, jeder Erscheinungsweise moderner Informationstechnik – von Skandal zu Skandal – jeweils eigene Regeln zu geben. Um

aber tiefer liegende Gefährdungen und prinzipiellere Strukturen des Grundrechtsschutzes diskutieren zu können, ist es sinnvoll, sich den Modernisierungsbedarf durch einen kurzen Rück- und Vorblick der gemeinsamen Entwicklung von Informationstechnik und Datenschutzrecht deutlich zu machen.

Das geltende Datenschutzrecht stammt konzeptionell aus den 60er und 70er Jahren. In dieser Zeit fand die Datenverarbeitung in Rechenzentren statt. Die Daten wurden in Formularen erfasst und per Hand eingegeben. Die Datenverarbeitung betraf nur einen kleinen Ausschnitt des Lebens und war – soweit die Daten beim Betroffenen erhoben worden waren – für diesen weitgehend kontrollierbar. Wurde die Zweckbindung beachtet, wusste der Betroffene in der Regel, wo welche Daten über ihn verarbeitet wurden. Für diese Stufe der Datenverarbeitung sind die Schutzkonzepte der ersten Datenschutzgesetze entwickelt worden. Aus dieser Zeit stammen die Regelungen zur Zulässigkeit der Datenverwendung, die Anforderung an Unterrichtung und Benachrichtigung, an Zweckbestimmung und Zweckbindung, an die Erforderlichkeit der Datenverwendung, an die Rechte der Betroffenen und die Kontrolle durch Aufsichtsbehörden. Auch die 1995 in Kraft getretene europäische Datenschutzrichtlinie gehört zur Generation dieser Datenschutzgesetze. Die Nutzung von PCs ab den 80er Jahren hat die Datenschutzrisiken zwar erhöht, aber nicht auf eine neue qualitative Stufe gehoben.

Die zweite, qualitativ neue Entwicklungsstufe wurde mit der – weltweiten – Vernetzung der Rechner erreicht. Dadurch entstand ein eigener virtueller Sozialraum, in den nahezu alle Aktivitäten aus der körperlichen Welt übertragen wurden. Jede Handlung in diesem Cyberspace hinterlässt Datenspuren, die ausgewertet werden können und auch werden. Weder die Erhebung der Daten noch deren – letztlich weltweite – Verbreitung und Verwendung können vom Betroffenen kontrolliert werden. Web 2.0 oder Cloud-Computing sind weitere Ausprägungen dieser Entwicklungsstufe. Für sie versuchen die in den 90er Jahre erlassenen Multimedia-Datenschutzgesetze die Risiken in den Griff zu bekommen. Sie haben für die Internetdienste die Anforderungen an Transparenz, Zweckbindung und Erforderlichkeit verschärft und vor allem das neue Prinzip der Datensparsamkeit eingeführt. Diese normativen Vorgaben können allerdings nur im Wirkungsbereich des Nationalstaats zur Geltung gebracht werden. Die neue Datenverarbeitung betrifft je nach Nutzung des Internet einen großen oder kleinen Ausschnitt des täglichen Lebens, diesen aber potenziell vollständig. Allerdings kann der Betroffene diesen Risiken zumindest noch dadurch entgehen, dass er den virtuellen Sozialraum meidet – bildlich gesprochen, den Stecker zieht.

In einer weiteren, dritten Entwicklungsstufe, in der wir uns gegenwärtig befinden, gelangt die Datenverarbeitung in die körperliche Welt. RFID, Biometrie, Sensorkommunikation, mobiles Internet, Location Based Services, GPS, Geodatenverarbeitung und die vielen IT-Systeme im Automobil sind Vorboten hierfür. An Energieinformationsnetzen, die den Energieverbrauch in der Wohnung und Büro erfassen und steuern, wird gearbeitet. Die aus solchen Beispielen entstehende allgegenwärtige Datenverarbeitung erfasst potenziell alle Lebensbereiche und diese potenziell vollständig. In dieser Welt wachsen Körperlichkeit und Virtualität zusammen. Informationen aus der virtuellen Welt werden in der körperlichen Welt verfügbar, Informationen aus der realen Welt in die virtuelle Welt integriert. Aus dieser Welt und der in ihr stattfindenden Datenverarbeitung gibt es aber keinen Ausweg mehr. Insofern verschärft sich das Problem des Datenschutzes radikal und seine Lösung wird existenziell. Für diese neuen Herausforderungen gibt es noch keine spezifischen Regelungen.

Und auch die alten Regelungen greifen nicht mehr. In einer Welt allgegenwärtiger Datenverarbeitung laufen die bekannten Anforderungen der Zweckbindung, der Erforderlichkeit, der Transparenz, der Einwilligung und der Betroffenenrechte ins Leere. Wenn die allgegenwärti-

ge Rechnertechnik gerade im Hintergrund und damit unmerklich den Menschen bei vielen Alltagshandlungen unterstützen soll, wird es niemand akzeptieren, wenn er täglich zur Durchsetzung des Transparenzprinzips tausendfach bei meist alltäglichen Verrichtungen Anzeigen, Unterrichtungen oder Hinweise zur Kenntnis nehmen müsste. Wenn die Techniksysteme kontextsensitiv und selbstlernend sein sollen, werden sie aus den vielfältigen Datenspuren, die der Nutzer bei seinen Alltagshandlungen hinterlässt, und seinen Präferenzen, die seinen Handlungen implizit entnommen werden können, entgegen jeder Zweckbindung im Interesse des Nutzers vielfältige Profile erzeugen. Wenn die Nutzer die Datenspeicher der sie umgebenden Gegenstände nutzen, um ihr eigenes löchriges Gedächtnis zu erweitern, läuft das Erforderlichkeitsprinzip in Leere. Für die Gedächtnisfunktion ist für sehr lange Zeit eine Datenspeicherung auf Vorrat erforderlich, weil niemand wissen kann, an was man sich irgendwann einmal erinnern möchte. Diese Beispiele zeigen: Die neuen Technikanwendungen der allgegenwärtigen Datenverarbeitung verursachen nicht nur ein weiteres Vollzugs-, sondern ein grundlegendes Konzeptproblem. Sie stellen die zentralen Schutzkonzepte des Datenschutzrechts in Frage.

Alle drei Entwicklungsstufen bestehen heute parallel und beeinflussen sich gegenseitig. Für jede besteht ein spezifischer Modernisierungsbedarf – für die erste Stufe etwa in der Umsetzung moderner Datenschutzprinzipien beim Aufbau gigantischer Datenbanken für staatliche Zwecke wie etwa ELENA oder private Zwecke wie in Auskunfteien und im Adresshandel. Für die zweite Stufe besteht der Modernisierungsbedarf vor allem darin, der technischen Mächtigkeit globaler Systeme wie google mit Konzepten des Selbst- und Systemdatenschutzes zu begegnen und informationelle Selbstbestimmung auch in neuen Nutzungsformen (z.B. sozialen Netwerken) zu sichern. Für die dritte Stufe besteht der Modernisierungsbedarf vor allem darin, neue Schutzkonzepte für die informationelle Selbstbestimmung zu entwickeln, weil die bisherigen wie Transparenz, Zweckbindung und Erforderlichkeit gegenüber den neuen Technikanwendungen leer laufen.

III. Eine Modernisierung, die ein zukunftsfähiges Datenschutzrecht entwickeln will, muss Antworten für die absehbaren Probleme aller drei Entwicklungsstufen bieten. Vorschläge hierzu finden sich aktuell in der Bundesrepublik vor allem in dem Eckpunktepapier der Konferenz der Datenschutzbeauftragten und in Europa im Konzept der Europäischen Kommission zur Novellierung der Datenschutzrichtlinie. Ergänzend zu dieser Diskussion möchte ich einige grundsätzliche Aspekte eines modernen Datenschutzrechts in Deutschland und in Europa aufgreifen, um vor allem der zweiten und der dritten Entwicklungsstufe gerecht zu werden:

1. müssen Zulassungsregeln durch Gestaltungs- und Verarbeitungsregeln ergänzt werden. Bisher liegt das Schwergewicht auf einer einmaligen Entscheidung über die Zulässigkeit durch Zwecksetzung des Gesetzgebers oder des Betroffenen, die sehr lange vor der Datenverarbeitung liegen kann. Viel wichtiger aber sind Gestaltungs- und Verarbeitungsregeln, die permanent zu beachten sind.

Ein Beispiel sind Transparenzanforderungen. Statt sie auf eine einmalige Unterrichtung und auf einzelne Daten zu begrenzen, sollten sie stärker auf Strukturinformationen bezogen sein und durch eine ständig einsehbare Datenschutzerklärung im Internet gewährleistet werden. Eine andere Transparenzforderung wäre, immer eine technisch auswertbare Signalisierung zu fordern, wenn Daten erhoben werden.

Ein anderes Beispiel: Nutzt der Betroffene freiwillig Techniksysteme und -dienste, die seine individuellen Fähigkeiten unterstützen und verstärken sollen, könnte dies wie eine – ansonsten notwendige (schriftliche) – Einwilligung ebenfalls als Opt-in anzusehen sein. Zum Aus-

gleich müssten die Systeme und Dienste so gestaltet sein, dass sie über Datenschutzfunktionen verfügen, die er auswählen und für sich konfigurieren kann.

Ein drittes Beispiel: Je stärker das Zusammenspiel zwischen enger Zwecksetzung und strenger Erforderlichkeit bei individualisierten adaptiven Systemen an Grenzen stößt, desto stärker muss das Datenschutzrecht die Möglichkeiten sinnvollen anonymen und pseudonymen Handelns einfordern und Zweckbindung stärker auf Missbrauchsvermeidung und Erforderlichkeit stärker auf Löschungsregeln hin konzentrieren – als Voraussetzung für ein Recht auf Vergessen.

Erleichtert würde der Datenschutz für viele Anwendungen, wenn als zulässiger Zweck das Erbringen einer rein technischen Funktion anerkannt würde. Für diese Datenverarbeitungen ohne gezielten Personenbezug sollte auf eine vorherige Unterrichtung des Betroffenen verzichtet und ein Anspruch auf Auskunft auf eine Strukturauskunft reduziert werden. Zum Ausgleich sollte die Verwendung der Daten strikt auf diese Funktion begrenzt werden. Sie ist außerdem gegen Zweckentfremdung zu schützen. Die Daten sind nach der Verarbeitung sofort zu löschen. Für sie sollte ein Verwertungsverbot gelten.

2. sollten die Gestaltungs- und Verarbeitungsregeln technisch unterstützt werden. Technische Infrastrukturen sollten ermöglichen, auf Gefährdungen automatisch zu reagieren, ohne dass dies aufdringlich oder belästigend wirkt. Ein Beispiel: Die Einhaltung von Verarbeitungsregeln zu kontrollieren, darf nicht die permanente persönliche Aufmerksamkeit erfordern, sondern muss automatisiert erfolgen. Wenn datenverarbeitende Systeme ein Signal aussenden, kann dies von einem Endgerät des Betroffenen erkannt werden und zu einer automatisierten Auswertung der zugehörigen Datenschutzerklärung führen. Entsprechend der voreingestellten Datenschutzpräferenzen kann ein P3P-ähnlicher Client eine Einwilligung erteilen oder ablehnen. In Zweifelsfällen kann das Gerät je nach Voreinstellung den Betroffenen warnen und ihm die Erklärung anzeigen oder akustisch ausgeben. Die Durchsetzung von Verarbeitungsregeln muss im Regelfall durch Technik und nicht durch persönliches Handeln des Betroffenen erreicht werden.

Technischer Datenschutz hat gegenüber rein rechtlichen Vorgaben Effektivitätsvorteile: Was technisch verhindert wird, muss nicht verboten werden. Gegen Verhaltensregeln kann verstoßen werden, gegen technische Begrenzungen nicht. Datenschutztechnik kann so Kontrollen und Strafen überflüssig machen.

3. muss – wie in anderen Rechtsbereichen – Vorsorge die Gefahrenabwehr ergänzen. Sie bewirkt eine Reduzierung von Risiken und eine präventive Begrenzung potenzieller Schäden. Die Risiken für die informationelle Selbstbestimmung sind in der zweiten und dritten Entwicklungsstufe nicht mehr ausreichend zu bewältigen, wenn nur auf die Verarbeitung personenbezogener Daten abgestellt wird. Vielmehr sind im Sinn vorgreifender Folgenbegrenzung auch Situationen zu regeln, in denen noch keine personenbezogenen Daten entstanden sind. So bedürfen zum Beispiel die Sammlungen von Sensorinformationen, Umgebungsdaten oder von pseudonymen Präferenzen einer vorsorgenden Regelung, wenn die Möglichkeit oder gar die Absicht besteht, sie irgendwann einmal mit einem Personenbezug zu versehen. Auch sind zur Risikobegrenzung Anforderungen an eine transparente, datensparsame, kontrollierbare und missbrauchsvermeidende Technikgestaltung zu formulieren, der Risikoabschätzungen und Sicherheitskonzepte vorausgehen. Ebenso entspricht es dem Vorsorgegedanken, die einzusetzenden Techniksysteme präventiven freiwilligen Prüfungen ihrer Datenschutzkonformität zu unterziehen und diese Prüfungen zu dokumentieren.

4. Allerdings dürften Regelungen, die sich nur an Datenverarbeiter richten, viele Gestaltungsziele nicht erreichen. Auch die Datenverarbeiter sind den technischen Gestaltungsentscheidungen unterworfen. Daher sind in viel stärkerem Maß die Technikhersteller und -gestalter anzusprechen. Diese sollten vor allem Prüfpflichten für eine datenschutzkonforme Gestaltung ihrer Produkte, eine Pflicht zur Dokumentation dieser Prüfungen für bestimmte Systeme und Hinweispflichten für verbleibende Risiken treffen. Auch sollten sie ihre Produkte mit datenschutzkonformen Defaulteinstellungen ausliefern müssen.

5. Die datenschutzgerechte Gestaltung der künftigen Welt, insbesondere die Umsetzung von Zielen wie Datensparsamkeit oder Anonymität, fordert die aktive Mitwirkung der Entwickler, Gestalter und Anwender. Sie werden hierfür aber nur zu gewinnen sein, wenn sie davon einen Vorteil haben. Daher sollte die Verfolgung legitimen Eigennutzes in Formen ermöglicht werden, die zugleich auch Gemeinwohlbelangen dienen. Datenschutz muss daher zu einem Werbeargument und Wettbewerbsvorteil werden. Dies ist möglich durch die freiwillige Auditierung von Anwendungen, die Zertifizierung von Produkten und die Präsentation von Datenschutzerklärungen. Werden diese von Datenschutzrankings oder durch die Berücksichtigung bei öffentlichen Auftragsvergaben begleitet, kann ein Wettbewerb um den besseren Datenschutz entstehen. Dann werden die Gestaltungsziele beinahe von selbst erreicht.

6. Der Schutz der informationellen Selbstbestimmung darf nicht von der individuellen Kontrolle und der individuellen Wahrnehmung von Rechten abhängig gemacht werden. Daher sind die Datenschutzbeauftragten zu stärken sowie Konkurrenten- und Verbandsklagen zu ermöglichen. Gegenstand der Kontrolle müssen Systeme mit ihren Funktionen und Strukturen sein, nicht so sehr die individuellen Daten. Ziel der Kontrolle muss es sein, die individuellen und gesellschaftlichen Wirkungen der technischen Systeme zu überprüfen und diese datenschutzgerecht zu gestalten.

7. sollte im Ausgleich mit Sicherheitsinteressen die informationelle Selbstbestimmung aller Bürger soweit irgend möglich respektiert werden. Dies legt die Unterscheidung zwischen Ausnahmefall und Normalfall nahe, um unnötige Grundrechtseingriffe zu vermeiden. Für den Normalfall sollten anlasslose, flächendeckende Überwachungsmaßnahmen, die nicht in der Lage sind, zwischen Zielpersonen und sonstigen – gesetzestreuen – Bürgern zu unterscheiden, vermieden werden. Im Ausnahmefall sollten dann die zuständigen Behörden effektive Befugnisse und wirkungsscharfe Instrumente haben, die anlassbezogen gezielt und schnell eingesetzt werden können.

8. Diese Unterscheidung zwischen Normalität und Ausnahme ist insbesondere für Überwachungsmaßnahmen in einer Welt allgegenwärtiger Datenverarbeitung zu beachten. Protokollieren die uns umgebenden Alltagsgegenstände permanent unsere alltäglichen Lebensvollzüge – etwa den Energieverbrauch eines Haushalts – entstehen viele für die Sicherheitsprävention interessante Daten. Hierfür ist die Anforderung des BVerfG zu einer Überwachungsgesamtrechnung umzusetzen. Nach seiner Entscheidung zur Vorratsdatenspeicherung müssen die Gesamtbelastungen bürgerlicher Freiheiten durch die Gesamtheit aller verfügbaren staatlichen Überwachungsmaßnahmen verhältnismäßig sein. Dies gilt nicht nur für die Forderung einer Ausweitung anlassloser Vorratsspeicherungen (Hierfür ist eine Auseinandersetzung mit der grenzenlosen Logik der Prävention erforderlich). Dies gilt auch – im Zusammenhang mit der Vorgabe einer Beobachtungspflicht des Gesetzgebers – für das Hineinwachsen von Lebensbereichen in das Anwendungsfeld einer Überwachungsmaßnahme – etwa durch die Ausweitung von Telekommunikationsanwendungen im Hinblick auf die Vorratsdatenspeicherung von Verkehrsdaten.

IV. Die bisherigen Novellen zum Datenschutzrecht zeigen, wie schwierig eine Modernisierung sein wird. Datenschutz liegt quer zu allen anderen Gesellschafts- und auch Rechtsbereichen. Für die Modernisierung des Datenschutzrechts gilt erst recht die Forsthoff'sche Regel, dass Interessen umso schwerer zu organisieren und durchzusetzen sind, je allgemeiner sie sind. Nehmen wir die Novellen 2009. Bei ihnen ging es nur um beschränkte Korrekturen und dennoch konnte sich das Interesse aller auf Schutz ihrer informationellen Selbstbestimmung kaum gegen den hoch organisierten und effektiven Lobbyismus deren durchsetzen, die individuelle Nachteile befürchteten. Dies lässt für die noch immer anstehende Modernisierung des Datenschutzrechts wenig hoffen.

Eine Modernisierung des Datenschutzrechts in einem Guss dürfte für die Bundesrepublik Deutschland eine politisch zu anspruchsvolle Aufgabe sein. Neben der Unfähigkeit der Politik, eine so umfassende Neuordnung durchzusetzen, dürften hierfür vor allem die Ungleichzeitigkeiten des objektiven Modernisierungsdrucks in unterschiedlichen Lebensbereichen und ihre unterschiedliche Wahrnehmung entscheidend sein. Auch wird der Bedarf an rechtlicher Vorsorge für künftige Entwicklungen unterschiedlich eingeschätzt. Daher dürfte viel dafür sprechen, die Modernisierung des Datenschutzrechts in mehreren Schritten umzusetzen.

Um für die einzelnen Schritte sicherzustellen, dass sie zueinander passen und insgesamt das Ziel erreichen, sollte ein Mustergesetz erarbeitet werden, das als Orientierungsrahmen für die einzelnen Modernisierungsnovellen dient. Daher sollte die Skizze der Konferenz der Datenschutzbeauftragten zu einem solchen Mustergesetz weiter entwickelt werden.

Für die Modernisierung des Datenschutzrechts ist die Überarbeitung der europäischen Datenschutzrichtlinie von größter Bedeutung. Das Gesamtkonzept, das die Europäische Kommission hierfür vorgelegt hat, enthält viele unterstützenswerte Vorschläge. Die Kommission will jedoch nicht nur die Rechte des Betroffenen stärken, sondern auch die Transfers personenbezogener Daten im Binnenmarkt und weltweit erleichtern. Diese Zielsetzung führt allerdings nur dann zu einer Modernisierung des Datenschutzes, wenn der Grundsatz des freien Verkehrs der Daten *durch* Datenschutz konsequent durchgehalten wird. Zielführend ist, dass die Kommission die Bedeutung datenschutzfreundlicher Technologien und Datenschutz durch Technik erkannt hat. Allerdings hat sie die notwendige Verknüpfung von Recht und Technik noch nicht in ihr Konzept aufgenommen. In diesem fehlen Vorgaben an Hersteller und Technikgestalter zum Selbst- und Systemdatenschutz.

Das Konzept der Kommission zielt allerdings vor allem auf die Beseitigung von Defiziten in der Umsetzung von Datenschutzgrundsätzen aus der ersten Entwicklungsstufe. Für viele aktuelle Herausforderungen der zweiten und erst recht der dritten Entwicklungsstufe enthält sie keine Lösungsvorschläge. Aber vielleicht würde man damit die Kommission und die Datenschutzrichtlinie auch überfordern. Sie muss eine Mindestharmonisierung des Datenschutzes in der gesamten Union bewirken. Sie muss Rücksicht nehmen auf differenzierte Ausprägungen von Problemen, auf unterschiedliche politische Kulturen des Datenschutzes in den Mitgliedstaaten, auf unterschiedliche Debatten zur Modernisierung des Datenschutzes und damit auf unterschiedliche politische Erwartungen. Die Kommission kann damit schwer zum Protagonisten einer anspruchsvollen Modernisierung werden, die Datenschutzrichtlinie schwer zu ihrer Leitnorm.

Die Richtlinie wird daher nicht selbst die notwendige umfassende Modernisierung bewirken – hierfür ist ihr Anwendungsbereich zu breit und zu vielfältig, hierfür ist sie auch zu sehr den Fragen der ersten und (zum Teil) der zweiten Entwicklungsstufe verhaftet. Sie kann aber durch klare Zielsetzungen und förderliche Strukturen die notwendige Modernisierung in den Mitgliedstaaten unterstützen.

Sie darf aber keinesfalls die notwendige Modernisierung behindern. Dies wäre aber der Fall, wenn die Kommission weiterhin auf dem Ziel einer Vollharmonisierung für den gesamten europäischen Binnenmarkt beharrt und im Interesse einheitlicher Wettbewerbsbedingungen keine von der Richtlinie abweichenden nationalen Datenschutzanforderungen zulässt.

Bis die Neufassung der Richtlinie in Kraft getreten ist, sind seit der ersten Fassung beinahe 20 Jahre vergangen. Wenn es bis zur nächsten grundsätzlichen Novellierung der Datenschutzrichtlinie wieder einen vergleichbaren Zeitraum benötigt, hieße dies, dass bis dahin keine relevanten Maßnahmen zur Modernisierung des nationalen Datenschutzrechts möglich sind. Dies hieße zugleich, dass die nicht von der Richtlinie erfassten alten und aktuellen Herausforderungen für ein oder zwei Jahrzehnte nicht durch Neuregelungen angegangen werden könnten. Dies hieße weiter, dass gerade die vielfältigen Herausforderungen, die in den nächsten ein oder zwei Jahrzehnten durch die technisch-wirtschaftliche Entwicklung erst noch entstehen, nicht auf nationaler Ebene gelöst werden könnten. Angesichts der Schnelligkeit der technischen Entwicklung und der Vielfalt ihrer Anwendungen müssen jedoch Freiräume für gesetzgeberische Experimente in den Mitgliedstaaten offen gehalten werden. Die Richtlinie darf daher keine Vollharmonierung anstreben.