

Besserer Datenschutz bei einer Reform des Meldewesens

Datenschutzbedarf für den elektronischen Personalausweis

Ausgewählte Aspekte zum Novellierungsbedarf des Datenschutzrechts in Deutschland

Vortrag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Peter Schaar, auf der „5. RISER Konferenz zum Europäischen Meldewesen“ am 6. Mai 2010 in Berlin

Sehr geehrte Damen und Herren,

die Digitalisierung unserer Lebensumgebung schreitet unaufhörlich voran. Jeder Einzelne von uns ist – ob er will oder nicht – Teil der Informationsgesellschaft, die längst die nationalen Grenzen überschritten hat. Diese Entwicklung bedeutet eine große Herausforderung für den Datenschutz. Dieser ist demzufolge nicht mehr national realisierbar, sondern nur mehr durch internationale Kooperation sicher zu stellen.

Auch der Datenschutz hat gegenüber seinen Anfängen in den 1970er und 1980er Jahren andere Dimensionen angenommen. War der Datenschutz früher überwiegend juristisch geprägt, wird er daneben in Zukunft immer stärker auch technologische Dimensionen berücksichtigen müssen. Vermutlich werden die technologischen Aspekte sogar zunehmend in den Vordergrund treten.

Der Umgang mit elektronischen Identitäten im virtuellen Raum des Internets ist in diesem Zusammenhang von besonderer Bedeutung. Hier hinein spielen unter Datenschutzgesichtspunkten neben der Identitätsfeststellung, also der Identifizierung im engeren Sinne, auch die Authentifizierung, also die Sicherung der Identität, und die Autorisierung, also die Zuweisung von Rechten, etwa im Rahmen von Altersverifikationssystemen. Dabei handelt es sich um zentrale Fragen des Systemdatenschutzes, der sich der Gestaltung technischer Infrastrukturen zuwendet und sich nicht auf den normativen Aspekt der Zulässigkeit der Datenverarbeitung beschränkt. Letztlich geht es darum, die Autonomie des Einzelnen in einem immer komplexeren technologischen Umfeld zu gewährleisten.

Auch vor der öffentlichen Verwaltung macht die technologische Entwicklung nicht Halt. eGovernment und damit auch die Notwendigkeit der elektronischen Identifizierung sind drän-

gende Zeitfragen. Ich freue mich daher, in diesem Kontext zunächst über das „weite Feld“ des Datenschutzes im Meldewesen zu Ihnen sprechen zu können. Anschließend werde ich auf Datenschutzfragen im Zusammenhang mit der Einführung des elektronischen Personalausweises und auf ausgewählte Aspekte der avisierten Reform des Datenschutzrechts in Deutschland eingehen.

Zunächst zum Meldewesen. Wir erinnern uns: Die Föderalismusreform 2006 übertrug die Gesetzgebungskompetenz für das Melderecht auf den Bund.

Das Bundesministerium des Innern (BMI) hatte daraufhin beabsichtigt, das Meldewesen gesetzlich umfassend neu zu regeln und ein **Bundesmelderegister als Zentralregister** einzurichten. Dieses Vorhaben konnte in der zurückliegenden Legislaturperiode nicht verwirklicht werden. Denn das BMI hatte innerhalb der Bundesregierung hierüber kein Einvernehmen herbeiführen können. Auch ich hatte erhebliche Bedenken dagegen erhoben, zumal der **Bedarf** für ein zusätzliches umfangreiches zentrales Melderegister auf Bundesebene vom **BMI - bis heute - nicht belegt werden konnte**. Vielmehr hatte ich geltend gemacht, dass die datenschutzrechtliche Position der Meldepflichtigen insgesamt nicht nur erhalten, sondern unter Nutzung moderner Technologien noch deutlich verbessert werden muss.

Nach der Föderalismusreform ist eine Rahmengesetzgebungskompetenz, die der Bund früher im Melderecht hatte, verfassungsrechtlich überhaupt nicht mehr vorgesehen. Angesichts der nun bestehenden Gesetzgebungskompetenz auf Bundesebene ist das BMI in der laufenden Legislaturperiode gehalten, erneut das Projekt eines Bundesmeldegesetzes proaktiv zu betreiben. Folgerichtig sehen die Koalitionsvereinbarungen der Bundesregierung die Reform des Melderechts als Arbeitsziel der laufenden Legislaturperiode vor.

In diesem Zusammenhang möchte ich vor einer Fehldeutung warnen: die ausschließliche Gesetzgebungskompetenz des Bundes bedeutet keineswegs, dass es in Zukunft ein umfassendes zentrales Melderegister geben muss. Vielmehr sind auch andere Lösungen denkbar: So wäre es durchaus verfassungskonform, wenn der Bund es bei der bisherigen organisatorischen Zersplitterung des Meldewesens belassen und sich auf Vorgaben hinsichtlich des Inhalts und der Verwendung des Melderegisters beschränken würde. In einem solchen Fall würden die bisher im Melderechtsrahmengesetz enthaltenen Vorschriften zu verbindlichem, direkt anwendbarem Recht, das keiner Umsetzung durch Landesgesetze mehr bedarf.

Denkbar und nicht einmal unwahrscheinlich ist es, dass es auch in Zukunft kein zentrales Melderegister geben wird, sondern dass sich der Bund darauf konzentriert, die Melderegister weiter zu standardisieren und miteinander zu verknüpfen.

Vor diesem Hintergrund möchte ich meine datenschutzrechtlichen Überlegungen und Forderungen vorstellen. Im Mittelpunkt sollen dabei Überlegungen darüber stehen, wie sich das Streben nach einer modernen, effizienten Verwaltung mit dem Recht auf informationelle Selbstbestimmung, also dem Datenschutz, vereinbaren lässt. Dabei geht es sowohl um rechtliche Vorgaben als auch um technologische Aspekte. Bestimmte Entscheidungen zur Struktur und Funktionsweise des Meldewesens sind für die Möglichkeiten, die gespeicherten Daten unzulässig oder zumindest verfassungsrechtlich problematisch zu verwenden, von essenzieller Bedeutung. Wir Datenschützer sprechen hier von "Datenschutz durch Technik" oder "Privacy by Design".

Das Meldewesen ist einer der wenigen Bereiche der öffentlichen Verwaltung, der Daten über alle Einwohner sammelt und für administrative Zwecke zur Verfügung stellt. Schon 1978 hatte deshalb der damalige Bundesbeauftragte für den Datenschutz in seiner vom BMI erbetenen gutachtlichen Stellungnahme die **hohe datenschutzrechtliche Bedeutung des Meldewesens** herausgestellt und datenschutzrechtliche Forderungen geltend gemacht, die weitgehend in das Melderechtsrahmengesetz vom 16. August 1980 Eingang fanden.

Die seinerzeitigen Kernforderungen haben angesichts der heutigen informationstechnischen Möglichkeiten deutlich an Bedeutung gewonnen:

- Beschränkung der Aufgaben der Meldebehörden auf den Identitätsnachweis,
- schlanker gesetzlich festgelegter Merkmalskatalog,
- strenge Zweckbindung der über die Grunddaten hinausgehenden Angaben,
- gesetzlich festgelegte Betroffenenrechte (gebührenfreie Auskunft, Berichtigung, Löschung, Unterrichtung über die Erteilung sog. erweiterter Auskünfte, Übermittlungs- und Auskunftssperren).

In dem vom BMI im April 2008 vorgelegten Referentenentwurf für ein Bundesmeldegesetz (BMG) blieben diese von mir erneuerten datenschutzrechtlichen Forderungen aber leider weitgehend unberücksichtigt.

Ich hatte im Gegenzug Folgendes zu bedenken gegeben:

Die Einführung eines zentralen umfänglichen Bundesmelderegisters (BMR) wäre mit **erheblichen verfassungsrechtlichen Risiken** behaftet. Nach ständiger Rechtsprechung des Bundesverfassungsgerichts darf es keine Datenspeicherung auf Vorrat für unbestimmte Zwecke geben. Deshalb müssen gerade bei einem Register, das von einer Vielzahl öffentlicher und nicht-öffentlicher Stellen für unterschiedliche Verwendungszwecke zugänglich sein soll, hohe Anforderungen hinsichtlich des Umfangs der erfassten personenbezogenen Daten, der Ver-

wendungszwecke und der Definition von Zugriffsrechten, der Form der Speicherung und der Maßnahmen zur Gewährleistung des Datenschutzes gestellt werden. Der Gesetzgeber hat dabei auch – und hier möchte ich aus dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983 wörtlich zitieren - „organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken“. Das Bundesverfassungsgericht hat in seinem Urteil zur Vorratsdatenspeicherung in der Telekommunikation vom 2. März 2010 die verfassungsrechtliche Problematik einer derartigen umfassenden Datensammlung noch einmal unterstrichen.

Ein BMR, das die Daten sämtlicher Einwohner enthält, würde erheblich tiefer in den Datenschutz eingreifen als dezentrale Register, insbesondere weil die Auswirkungen eines eventuellen Datenmissbrauchs erheblich größer wären. Zudem würde ein BMR die Möglichkeit eines direkten Zugriffs auf sämtliche Melderegisterdaten und ihre Verknüpfung mit anderen Dateien ermöglichen. Da das BMR die kommunalen Register nicht ersetzen, sondern nur ergänzen soll, muss für jedes in das BMR aufzunehmende Merkmal der Nachweis geführt werden, dass seine Speicherung in einer bundesweiten Datei erforderlich ist. Andererseits führt - auch das möchte ich nicht verhehlen - die rasant fortschreitende technologische Entwicklung mit ihren Möglichkeiten zur umfassenden Vernetzung dezentraler Datenbestände ebenfalls zu Missbrauchsmöglichkeiten, die über eine unzulässige Verwendung der in einem einzigen dezentralen Register vorhandenen Daten hinausgehen. Letztlich bleibt jedoch ein Unterschied erhalten: da verschiedene Stellen für die Speicherung der dezentral gespeicherten Daten verantwortlich sind, wäre ein zentraler, quasi von oben angeordneter Zugriff jedenfalls unter den gegebenen föderalen Verhältnissen in der Bundesrepublik Deutschland bei Beibehaltung der dezentralen Meldestrukturen deutlich erschwert.

Ein BMR - oder miteinander verknüpfte dezentrale Melderegister - darf auch nicht den Weg zu einem **allgemeinen Personenkenntzeichen** bereiten, mit dessen Hilfe sich eine Vielzahl von Dateien außerhalb des Meldewesens verknüpfen ließe. Ein solches wäre, wie das Bundesverfassungsgericht bereits 1969 in seiner Mikrozensusentscheidung dargelegt hatte, nicht mit dem Grundgesetz vereinbar. Da sich eine umfassende Datei aller gemeldeten Personen in besonderer Weise eignen könnte, die verfassungsrechtlich gebotene „informationelle Gewaltenteilung“ zu unterlaufen, müssen bei der Konzeption des BMR zusätzliche Vorkehrungen getroffen werden, die eine zweckübergreifende Zusammenführung und Nutzung personenbezogener Daten verhindern.

Eine Melderechtsreform und die darauf basierende Reorganisation des Meldewesens dürfen demnach nicht dazu führen, dass große Datensammlungen bereichsübergreifend zusammengeführt werden können. „Sprechende“ oder einheitlich durchgängige Ordnungsmerkmale im Melderegister wären mit diesem Grundsatz nicht vereinbar. Notwendig ist daher ein **daten-**

schutzrechtlich wirkungsvolles Identitätsmanagement mit Generierung und Management bereichsspezifischer Ordnungsmerkmale.

Um die Persönlichkeitsrechte und den Schutz der Identität des Einzelnen zu gewährleisten, sind die folgenden Funktionsbedingungen unerlässlich:

Die Minimierung der Datenspeicherung ist ein wesentliches Element des Datenschutzes. Wenn also auch in Zukunft der Gedanke eines zentralisierten Meldedatenbestandes weiterverfolgt werden sollte, was ich unter den gegebenen politischen Konstellationen eher für unwahrscheinlich halte, müssen zusätzliche Datenschutzsicherungen eingebaut werden, damit auch bei einem solchen Funktionsmodell das Recht auf informationelle Selbstbestimmung gewahrt wird. In einem BMR dürften - sofern überhaupt ein Bedarf für eine zentrale Speicherung belegt werden kann - allenfalls Grundpersonalien dauerhaft gespeichert werden. Diese dienen der eindeutigen Identifikation des Einzelnen oder ausdrücklich dem Persönlichkeitsschutz, z. B. in Form der Eintragung von Übermittlungssperren. Weitere Daten dürfen aus meiner Sicht von der kommunalen Meldebehörde nur dann und insoweit zentral bereitgestellt werden, wie sie für einen konkreten Übermittlungsbedarf benötigt werden. Diese weiteren Daten wären nach der Übermittlung unverzüglich zu löschen.

Das Ordnungsmerkmal eines Registers ist das bedeutsamste Zugriffs- und ggf. Verknüpfungselement. Die datenverarbeitungstechnische Organisation von Ordnungsmerkmalen hat daher unter Datenschutzaspekten höchste Bedeutung und stellt das Kernelement für den Schutz der Identität des Einzelnen dar. Dies gilt gleichermaßen für zentrale Registerstrukturen wie für dezentral organisierte, miteinander verknüpfte Melderegister. Hier müsste das bereits erwähnte datenschutzrechtlich wirkungsvolle Identitätsmanagement ansetzen:

Nach meiner Auffassung darf das Ordnungsmerkmal eines Registers ausschließlich internes Ordnungs- und Zugriffsinstrument sein. Dieses wäre abstrakt zu bilden und dürfte sich nicht aus personenbezogenen Daten herleiten und keinen Rückschluss auf eine konkrete Person ermöglichen (kein „sprechendes“ Ordnungsmerkmal, kein „sprechender“ Schlüssel). Dieses Ordnungsmerkmal dürfte auch nicht übermittelt werden. Für den jeweiligen Adressaten müsste vielmehr ein spezifisches eigenes abstraktes Ordnungsmerkmal dem jeweiligen personenbezogenen Meldedatensatz beigegeben werden. Dies hätte im automatisierten Verfahren im Zuge des Versendens oder Empfangens des personenbezogenen Meldedatensatzes zu erfolgen. Dieser Prozess sollte für die am Meldevorgang beteiligten Mitarbeiter nicht sichtbar sein. Die Generierung und das Management der bereichsspezifischen Ordnungsmerkmale müssten von einer unabhängigen Vertrauensstelle bei der Registerbehörde nach mathematisch sicherem Algorithmus vorgenommen werden. Eine Speicherung der rein zum Zweck der bilateralen Übermittlung generierten Ordnungsmerkmale dürfte im Register nicht stattfinden.

Auch wenn das BMI in einem neuen Entwurf eines Bundesmeldegesetzes auf ein bundeszentrales Register verzichten sollte und anderen Lösungen den Vorzug gäbe, müssten aus Datenschutzsicht die Merkmale des **Identitätsmanagements** im Ergebnis erfüllt werden, zum Beispiel hinsichtlich der empfängerbezogenen temporären Ordnungsmerkmale auch bei Übermittlung direkt aus dem kommunalen Melderegister. Festzuhalten bleibt also: ob mit oder ohne bundeszentrales Melderegister: **nur ein datenschutzrechtlich wirkungsvolles Identitätsmanagement garantiert den Persönlichkeitsschutz.**

Unabhängig davon halte ich das Meldewesen in seiner Gesamtheit unter folgenden Aspekten für verbesserungsbedürftig:

- Die Datenkataloge bedürfen einer grundlegenden Überarbeitung unter dem Gesichtspunkt der Erforderlichkeit des jeweiligen Datums für die meldebehördlichen Kernaufgaben.
- Die datenschutzrechtliche Position der Meldepflichtigen muss dadurch gestärkt werden, dass bestehende bloße Widerspruchsrechte (z.B. gegen Melderegisterauskünfte an Parteien zur Wahlwerbung oder an Adressbuchverlage) durch das Erfordernis einer vorherigen Einwilligung in die entsprechenden Datenübermittlungen ersetzt werden.
- Unbefriedigend ist auch die sog. einfache Melderegisterauskunft, die praktisch keinerlei Einschränkungen unterliegt. Der Betroffene kann zurzeit – von wenigen gesetzlichen Ausnahmeregelungen abgesehen – nicht verhindern, dass seine Grunddaten an jedermann herausgegeben werden. Ich fordere daher, als Korrektiv zumindest ein generelles Widerspruchsrecht des Betroffenen gegen einfache Melderegisterauskünfte einzuführen, weil es sich hier um personenbezogene Daten handelt, die zwangsweise beim Bürger und primär zur Erfüllung hoheitlicher Aufgaben erhoben werden.
- Die Auskunftsrechte der Betroffenen gegenüber den Meldebehörden sollten gestärkt werden. Die Betroffenen können nicht erkennen, an welche Stellen Meldedaten fließen. Sie sollten daher die Möglichkeit erhalten zu erfahren, welche Datenübermittlungen im Einzelfall stattgefunden haben und welche öffentlichen und privaten Stellen Melderegisterauskünfte über sie eingeholt haben. Das bestehende Auskunftsrecht über regelmäßige Datenübermittlungen an andere Stellen sollte entsprechend ergänzt werden.
- Die allgemeine Hotelmeldepflicht sollte endlich abgeschafft werden. Die mit der Hotelmeldepflicht verbundene millionenfache Datenerhebung ist unverhältnismäßig. Hotelgäste können nicht schlechthin als Gefahrenquellen oder potentielle Straftäter angesehen werden.

Angesichts der technologisch bedingt zunehmenden Missbrauchsmöglichkeiten bekräftige ich die generelle Notwendigkeit, bereits technologisch weitestgehende Vorkehrungen zu treffen, damit Datenschutzverletzungen von vornherein vereitelt werden. Auch hier gilt also der bewährte Grundsatz: **Vorsorge ist der beste Schutz.**

So weit das Meldewesen. Jetzt einige Ausführungen zum Datenschutz in Zusammenhang mit dem **neuen elektronischen Personalausweis (nPA)**:

Anders als beim herkömmlichen Personalausweis wird das Lichtbild des Ausweisinhabers nicht nur in den Ausweis eingedruckt, sondern für Zwecke staatlicher Kontrollen im sog. Biometrie-Chip des nPA auch digitalisiert gespeichert. Optional können dort für staatliche Kontrollzwecke auch die Zeigefingerabdrücke des Inhabers gespeichert werden.

Die Entscheidung zur Einführung des elektronischen Personalausweises ist insoweit die Fortsetzung der seit 2004 erfolgenden Einführung biometrischer Merkmale in den Reisepässen. Die biometrischen Merkmale sind auf internationaler Ebene von den Regierungen vereinbart worden, um die missbräuchliche Verwendung von Reisedokumenten zu erschweren. Letztlich handelt es sich um eine Maßnahme, die ohne die Terroranschläge des Jahres 2001 wohl nicht hätte durchgesetzt werden können.

Der nPA soll aber nicht nur der Identifikation anlässlich hoheitlicher Identitätskontrollen dienen, sondern - optional - auch zur elektronischen Identifikation für Zwecke des eCommerce und des eGovernment genutzt werden. Er soll es den Bürgerinnen und Bürgern erleichtern, vom heimischen PC aus am Wirtschaftsleben teilzunehmen und mit staatlichen und kommunalen Behörden zu kommunizieren, und dabei das Missbrauchsrisiko, insbesondere die Gefahr des Identitätsdiebstahls reduzieren. Der „beweissichere“ Abschluss von Rechtsgeschäften soll durch eine - ebenfalls optionale - Signaturfunktion ermöglicht werden.

Aus meiner Sicht beinhaltet der nPA Risiken für den Datenschutz, besitzt aber auch das Potenzial, den elektronischen Geschäftsverkehr und die Kommunikation mit Behörden sicherer und datenschutzfreundlicher zu gestalten.

Wenn persönliche Daten zusätzlich auf einem per Funk auslesbaren Chip gespeichert werden, ist dies zunächst einmal mit zusätzlichen Risiken verbunden. Dies gilt sowohl für die biometrischen Daten (elektronisches Gesichtsbild und - auf freiwilliger Basis - Fingerabdruck), aber auch für sonstige Identifizierungsdaten, die für die Kommunikation über das Internet verwendet werden sollen. Zum einen geht es also darum, ein unautorisiertes Auslesen dieser Daten zu verhindern. Die hierfür vorgesehenen Verschlüsselungsfunktionen sollen dies gewährleis-

ten. Missbrauchsrisiken sollen zudem mit einer **Trennung der Daten und Funktionen** und mit einer **zuverlässigen Zugriffssicherung** reduziert werden.

Biometriedaten müssen von den Identifizierungsdaten abgeschottet werden. Die Technik ist dabei so zu gestalten, dass etwa der Grenzbeamte nur die Lichtbild- und Fingerabdruckdaten aufrufen kann, aber keinen Zugriff auf die elektronische Signatur oder die für eCommerce und eGovernment verwendeten Identifizierungsfunktionen (eID) erhält. Umgekehrt muss ausgeschlossen werden, dass die für hoheitliche Zwecke gespeicherten Biometriedaten von unbefugten Dritten - vielleicht sogar per Fernzugriff aus dem Internet - abgefragt werden können.

Die eID-Funktion darf dem jeweiligen Partner im eCommerce und im eGovernment **weder die Inhalte** früherer geschäftlicher und behördlicher Kontakte **erkennbar** machen, **noch den Kontakt** „als solchen“. Es darf auch **keine zentrale Speicherung geben**, die staatlichen oder privaten Stellen eine Rückverfolgung und Profilbildung erlauben könnte.

Leider nicht aufgegriffen wurde meine Forderung nach einem umfassenden **Datenschutzaudit** für die Diensteanbieter, die ein Berechtigungszertifikat für den Zugriff auf die eID-Funktion nutzen wollen. Deshalb befürchte ich, dass nicht alle Unternehmen, die den neuen Personalausweises im eCommerce nutzen wollen, das erforderliche hohe Schutzniveau gewährleisten. Ich teile auch die Befürchtung von Verbraucherschützern, dass die Vergabe von Zugriffszertifikaten an Unternehmen von den Nutzern als Qualitätsmerkmal der von diesem Unternehmen angebotenen Dienste missverstanden werden könnte. So wäre es z.B. nicht auszuschließen, dass ein Unternehmen ein Zugriffszertifikat bekommt, das in betrügerischer Absicht Internetdienstleistungen anbietet. Zwar lassen sich die Zugriffszertifikate widerrufen, doch setzt der Widerruf voraus, dass die missbräuchliche Verwendung vorher erkannt und moniert wurde. Genau diese Zeitspanne könnte für die unrechtmäßige Datenerlangung und -verwendung benutzt werden.

Bedeutsam ist für mich auch, dass die mit dem nPA vorgesehene Möglichkeit zur sicheren Identifikation nicht als Aufforderung missverstanden wird, bisher ohne Namensangabe nutzbare Internetdienste zukünftig nur noch denjenigen anzubieten, die sich namentlich registrieren lassen. Vielmehr sollte die anonyme oder pseudonyme Inanspruchnahme von Internetangeboten weiterhin möglich bleiben. In diesem Zusammenhang sehe ich es positiv, dass die eID-Funktion auch eine Altersverifikation ohne Registrierung weiterer persönlicher Daten des Ausweisinhabers ermöglicht.

Nun noch einige themenrelevante Ausführungen zu Bedarf und Zielsetzung einer **Reform des Datenschutzrechts in Deutschland**:

Datenschutz hat nicht nur eine Schutzfunktion, er beschreibt auch einen Gestaltungsanspruch der Betroffenen: Jeder Mensch soll selbst bestimmen können, wer was wann über ihn weiß. Datenschutz ist Grundrechtsschutz und die Wahrung der informationellen Selbstbestimmung

eine Funktionsbedingung einer menschenwürdigen Informationsgesellschaft. Doch wie soll das Recht auf informationelle Selbstbestimmung im Zeitalter der allgegenwärtigen Datenverarbeitung gewahrt werden? Ob von staatlichen Stellen oder Unternehmen – unser Verhalten wird beobachtet, registriert und bewertet. Videoüberwachung folgt uns an allen möglichen Orten, wir können durch Ortungstechnik metergenau lokalisiert werden, Kundenkarten und Internet liefern die Daten für Konsum- und Persönlichkeitsprofile und Auskunfteien haben ein waches Auge auf unsere Zahlungsfähigkeit. Das heutige Datenschutzrecht gibt auf diese Probleme nur noch unbefriedigende Antworten und bedarf der Modernisierung.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat **Eckpunkte** formuliert, die Grundlage einer Diskussion über eine Reform des Datenschutzrechts sein sollen.

Zentrale Punkte einer solchen Modernisierung sind etwa die Verankerung konkreter Schutzziele und Grundsätze sowie die Stärkung der Betroffenenrechte. Außerdem sollte den aus der technologischen Entwicklung resultierenden Gefährdungen durch technik-neutrale Vorgaben begegnet werden, die auf konkrete Systeme und Anwendungsfelder durch Auslegung und Normierung konkretisiert werden können.

Im Folgenden möchte ich auf zwei Aspekte einer Modernisierung besonders eingehen: die **Gefahren durch Profilbildung** und die Chancen eines **datenschutzfreundlichen Identitätsmanagements als sachübergreifendes Instrument**.

Die Zusammenführung und Verknüpfung personenbezogener Daten zu Profilen stellt eine besondere Gefahr für das Persönlichkeitsrecht dar. Auf diese Weise können die Persönlichkeit eines Menschen, sein Verhalten, seine Interessen und Gewohnheiten verfügbar und vorhersehbar gemacht werden, was u. A. eine gezielte Manipulation erlaubt, ohne dass sich die Betroffenen dessen überhaupt bewusst sind. Derartige Profile gibt es bereits in vielen Bereichen, etwa als Konsumentenprofil, Bewegungsprofil, Nutzerprofil im Internet. Der rasante technologische Fortschritt in vielen Bereichen lässt Unmengen an personenbezogenen Daten anfallen, oft nur als Nebenprodukt, deren Verknüpfung immer ausgefeiltere Profile möglich macht.

Ich plädiere daher für ein **Verbot der Profilbildung** hinter dem Rücken des Betroffenen. Die Bildung von Profilen sollte nur zulässig sein bei entsprechender konkreter gesetzlicher Grundlage, die dem besonderen Gefährdungspotential von Profilbildung Rechnung trägt, oder bei einer Einwilligung des Betroffenen.

Eine **wirksame Einwilligung** setzt dabei eine umfassende Information über Umfang und Herkunft der verwandten Daten, Zweck und Verwendung des Profils, verantwortliche Stelle und vorgesehene Lösungsfrist voraus. Die Einwilligung muss freiwillig und jederzeit widerruf-

bar sein. Der Widerruf muss die sofortige Löschung des Profils zur Folge haben, auch bei den Stellen, an die es übermittelt worden ist.

Nur durch eine strikte Reglementierung der Profilbildung kann in diesem besonders sensiblen Bereich die informationelle Selbstbestimmung gewährleistet werden.

Rechtliche Regelungen lösen aber nicht alle Probleme. Daher brauchen wir - wie für das Meldewesen bereits dargestellt - **generell ein datenschutzfreundliches Identitätsmanagement**, das eine Zusammenführung von Daten aus unterschiedlichen Bereichen erschwert und an die Mitwirkung des Betroffenen knüpft. Das Identitätsmanagement sollte auf der anonymen oder pseudonymen Nutzung von elektronischen Verfahren und der dezentralen Haltung von Identifikationsdaten unter möglichst weitgehender Kontrolle der betroffenen Bürgerinnen und Bürger basieren. Zentrale Verfahren und Möglichkeiten zur Zusammenführung von Identitätsdaten sind zu vermeiden.

Es muss zudem den jeweiligen Erfordernissen angepasste und abgestufte Nutzungsmöglichkeiten auch hinsichtlich Anonymität und Authentizität geben und eine sichere Authentifizierung auch auf der Anbieterseite. Bei den kommerziellen Dienstleistungen, etwa wenn eine Lizenz einer Software oder eines Spiels genutzt wird, reichen pseudonyme Registrierungen völlig aus, man braucht nicht notwendigerweise auch die Namen der Nutzer.

Dies wird nicht immer einfach umzusetzen sein. So basieren soziale Netzwerke auf sozialen Beziehungen, wo es naheliegt, dass man die Personen kennt. Hier kann man anonyme Nutzungsmöglichkeiten fordern, aber damit wird das Problem nicht gelöst. Doch es kommt darauf an, diese Alternative auch anzubieten: daher muss die Möglichkeit zur **anonymen und pseudonymen Nutzung** und Bezahlung von Online-Angeboten gestärkt werden.

Gleichzeitig ist sicherzustellen, dass bei der Nutzung möglichst wenig personenbezogene Daten preisgegeben werden. Auch ist darauf zu achten, dass die „**informationelle Gewaltenteilung**“ bestehen bleibt. Eindeutige Authentifizierung und Datenvermeidung stehen dabei nicht in einem unauflösbaren Widerspruch, denn intelligente Authentifizierungsmechanismen kommen ohne übergreifende Identifikationsnummern und Personenkennzeichen aus.

Sehr geehrte Damen und Herren, das waren nur einige Aufgaben, die sich aktuell dem Datenschutz stellen. Durch fortschreitende Technisierung werden die Aufgaben des Datenschutzes ständig umfänglicher und inhaltlich anspruchsvoller. Wirkungsvollen Datenschutz zu gewährleisten ist längst keine rein nationale Aufgabe mehr. Hierzu bedarf es vielmehr zielgerichteter effektiver **Zusammenarbeit in Europa und in der Welt**. Dieser Aufgabe sollten wir uns alle verpflichtet fühlen. In diesem Sinne wünsche ich der 5. RISER Konferenz zum Europäischen Meldewesen einen erfolgreichen Verlauf.