Projektgruppe „Datenschutz“

Informationsgespräch mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) Peter Schaar in der Sitzung am 21.2.2011 (Kurzprotokoll)

Der **Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) Peter Schaar** gibt einleitend einen Überblick über das Thema „Datenschutz und Internet“ und nimmt nachfolgend zu den Fragen aus der Projektgruppe Stellung.

Im Hinblick auf das Internet werde zwar teilweise von einer „Post-Privacy-Ära“ gesprochen, aber auch im Internetzeitalter und angesichts neuer Technologien seien Persönlichkeitsrechte zu wahren.

Unter Hinweis auf das Papier der **Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Ein modernes Datenschutzrecht für das 21. Jahrhundert“**[1] vom 18. März 2010 plädiert Herr Schaar dafür, in Datenschutzgesetzen auf einen „Maßnahmenbezug“ zu verzichten. So sei etwa nach Nr. 1 der Anlage zu § 9 Bundesdatenschutzgesetz (BDSG) Unbefugten der Zutritt zu Datenverarbeitungsanlagen zu verwehren. Diese Formulierung sei im Hinblick auf Laptops ungeeignet. Das Recht sei in vielen Punkten zu starr. Technikregelungen müssten abstrakter, dafür zielorientiert gefasst werden. Notwendige Konkretisierungen könnten dann auf untergesetzlicher Ebene, etwa durch Verordnungen oder technische Standards erfolgen.

Auch **Selbstregulierung** könne einen Beitrag zur Lösung datenschutzrechtlicher Fragen leisten, Selbstregulierung allein reiche aber nicht aus. Insbesondere müsse Selbstregulierung verbindlich gemacht und auch diejenigen einbezogen werden, die sich nicht verpflichten lassen wollten.

Grundidee des Datenschutzes sei es, die Souveränität des Einzelnen über seine Daten im Rahmen eines sozialen Kontextes zu gewährleisten. Die Einwilligung sei eine Operationalisierung dieses Ziel. Es komme auf die jeweilige Konstellation an, ob **Einwilligung oder Widerspruch** geeignete Mechanismen seien. Im öffentlichen Bereich sei Datenerhebung und -verarbeitung nur auf der Grundlage gesetzlicher Befugnis oder einer Einwilligung des Betroffenen möglich. Im nichtöffentlichen Bereich sei dies nicht so eindeutig. Denn es gehe um das Verhältnis Privater untereinander. Aber der Schutzauftrag des Staates führe dazu, dass Betroffene auch in diesem Bereich die Kontrolle über ihre Daten – jedenfalls im Prinzip – bekommen müssten. Vielfach werde das ohne Einwilligung nicht möglich sein; jedenfalls sei dies im Bereich struktureller Ungleichgewichte (z. B Arbeitsverhältnisse) der Fall.

Einwilligung und Widerspruch lägen zwar nahe beieinander, machten aber im Konkreten einen großen Unterschied aus. Denn derjenige, der aktiv werden müsse, etwa um Voreinstellungen zu ändern, bleibe häufig passiv. Eine Widerspruchslösung als Voreinstellung sei daher aus seiner Sicht sehr zweifelhaft. Deshalb plädiere er auch im nichtöffentlichen Bereich dem Grundsatz nach für Einwilligungslösungen. Andere Lösungen seien aber in bestimmten Fallkonstellationen denkbar, etwa im Hinblick auf die fehlende Sensibilität von Daten, z. B. bei Straßenansichtsdiensten.

[1] abrufbar unter http://www.baden-wuerttemberg.datenschutz.de/service/gem-materialien/modernisierung.pdf

Als Kriterien für eine Differenzierung sei die **Eingriffstiefe** denkbar, d. h. in welchem Maße die Daten geeignet seien, Persönlichkeitsrechte zu verletzen. Daten, die aus der Öffentlichkeit entnommen wurden, öffentliches Verhalten abbilden, seien weniger schutzwürdig. Dasselbe gelte für Informationen, die ein Nutzer selbst auf seiner Homepage oder bei Facebook einstelle. Anders seien Informationen zu bewerten, die bei der Nutzung von Diensten anfallen (Nutzungs- oder Verkehrsdaten). Für letztere sei eine Einwilligung erforderlich, soweit es um die Verwendung für Zwecke gehe, die über die Ermöglichung der Nutzung der Dienste hinausgingen.

Auf Nachfrage führt der **Bundesbeauftragte Peter Schaar** als Beispiel für einen klaren Verstoß gegen das Gebot der Datensparsamkeit und den Grundsatz der Zweckbindung das Taschenlampen-App an, das zugleich Standortdaten erhebe.

Soweit nach § 28 Abs. 3 BDSG die Verwendung für Werbezwecke für bestimmte Daten auch ohne Einwilligung möglich sei, sehe er das kritisch, weil in der Regelung nur auf die Art der Daten und nicht auf den Verwendungskontext und die Art und Weise der Entstehung der Daten abgestellt werde.

Dass die Erstellung von Persönlichkeitsprofilen unter Verwendung von Verkehrsdaten nur mit Einwilligung des Betroffenen zulässig sei, ergebe sich seiner Auffassung nach schon aus geltendem Recht. Weiteres Kriterien der Abgrenzung von Einwilligungs- und Widerspruchslösungen könne sein, wie direkt oder wie einfach ein **Personenbezug** herstellbar sei.

Auf Frage eines Projektgruppenmitglieds äußert der **Bundesbeauftragte Peter Schaar** sich zu dem **Problem der Grenzen nationalen Rechts**, wenn im Internet Dienste grenzüberschreitend angeboten werden. Nach europäischem und deutschen Recht, sei nationales Recht erst anwendbar, wenn eine Niederlassung im Inland besteht oder wenn Daten im Inland erhoben oder verarbeitet werden. Diese Regelung sei unzureichend. Vielmehr müsse nationales (bzw. europäisches) Recht schon dann anwendbar sein, wenn Unternehmen auf dem hiesigem Markt aktiv seien, etwa Daten hier lebender Menschen erheben. Entsprechendes gebe es schon jetzt im Verbraucherschutzrecht. Deutsche Internet-Unternehmen wiesen vor diesem Hintergrund auf Wettbewerbsnachteile gegenüber Wettbewerbern hin, die nicht den europäischen Datenschutzstandards unterworden seien.

Auf die Frage mehrerer Projektgruppenmitglieder zu **Geodatendiensten** unterstreicht der **Bundesbeauftragte Peter Schaar**, dass er eine Widerspruchsmöglichkeit gegen die Veröffentlichung für ausreichend gehalten hätte und die jetzt von Google Street View vorgenommene Rohdatenlöschung nicht für zwingend erforderlich gehalten habe. Wichtig sei die Möglichkeit des Vorabwiderspruchs, der also schon vor der Veröffentlichung abgegeben werden könne. Bei dem von den Fragestellern geschilderten Zielkonflikt, z. B. zwischen Mieter und Hauseigentümer oder zwischen Wohnungsmieter und Betreiber eines darunter gelegenen Restaurants, stünden sich das Recht auf informationelle Selbstbestimmung und das Recht auf informationelle Selbstdarstellung gegenüber, daneben komme eventuell auch das Eigentumsrecht nach Art. 14 GG ins Spiel. Ein Ausgleich dieser widerstreitenden Interessen könne eventuell auch technisch gewährleistet werden, so dass die Abbildung des Erdgeschosses auch dann möglich sei, wenn obere Geschosse verpixelt seien.

Ein Projektgruppenmitglied bittet um eine genauere Darstellung der kollidierenden gegenläufigen Schutzgüter und fragt, ob dann, wenn Netzwerke kommunikativen Zielen dienten, eher ein Opt-out als ein Opt-in angemessen sei. Der der **Bundesbeauftragte Peter Schaar** unterstreicht die Bedeutung des Kommunikationsgrundrechts für unsere Gesellschaft, wie sich jetzt wieder in den arabische Staaten zeige. Aber es gebe auch eine Diskussion um die Realnamenpflicht bei sozialen Netzwerken. Denn autoritäre Staaten nutzten Erkenntnisse aus sozialen Netzwerken zur Bekämpfung der Opposition. Hier wäre eine Voreinstellung, die eine anonyme oder pseudonyme Nutzung ermögliche, hilfreich. Der Datenschutz spiele daher auch bei der Wahrnehmung des Kommunikationsgrundrechts eine Rolle. Durchgehend nur Widerspruchslösungen vorzusehen, werde dem nicht gerecht.

Auch eine Registrierung von Nutzungsverhalten sei eine Einschränkung von Kommunikation. Eine flächendeckende Registrierung von Kommunikationsverhalten stelle einen schwerwiegenden Eingriff in die informationelle Selbstbestimmung dar, der nur mit Einwilligung oder im Interesse sehr viel höherer Rechtsgüter zulässig sei.
Andererseits sei es sicher nicht Aufgabe des Datenschutzes, Menschen vor ihrer eigenen Kommunikation zu schützen. Es sei im konkreten Fall immer zu fragen, wem die Daten preisgegeben würden und zu welchem Zweck. Die erwartete Verwendung der Daten und der Verwendungskontext seien dabei einzubeziehen.

Noch zu überdenken sei die Frage, ob die Presseprivilegien für jeden einzelnen Internetnutzer, der eine Meinung äußere, gelten würden und ob damit auch die Auferlegung der entsprechenden Verpflichtungen, etwa hinsichtlich von Gegendarstellungen, einhergehen müsse.

Anbieter müssten den Erwartungen der Nutzer durch Privatsphäreeinstellungen Rechnung tragen. Dies müsse nicht unbedingt durch Einwilligung oder Widerspruch geschehen, sondern könne auch durch privatsphärefreundliche Technik realisiert werden.

Auf eine Frage eines Projektgruppenmitglieds berichtet der **Bundesbeauftragte Peter Schaar**, dass es zwar eine kritische Diskussion, aber keine direkten Verhandlungen zu einer Revision des Safe Harbor-Abkommens gebe. Das Problem sei, dass die im Safe-Harbor Abkommen zu Grunde gelegten Datenschutzgrundsätze nicht identisch mit europäischen Datenschutzprinzipien seien und dass es neben der Selbstverpflichtung der teilnehmenden Unternehmen keine Überprüfung der Einhaltung gebe. Von US-amerikanischer Seite werde vorgebracht, dass keine nennenswerten Beschwerdefälle vorlägen. Dies sei auch zutreffend.

Die EU-Kommission wolle die Grenzen der Anwendbarkeit europäischen Datenschutzrechts neu regeln. Seiner Auffassung nach könne man diesen Aspekt zeitlich vorziehen und vor Abschluss der Reform des europäischen Datenschutzrechts, die sich noch länger hinziehen werde, regeln. Dies zu unterstützen, sei eine Aufgabe der Bundesregierung.

Zur Realisierung von Einwilligung und Widerspruch im Internet brauche man einfache technische Lösungen. Dabei müsse transparent sein, wer welche Daten zu welchem Zweck verarbeite. Diese Information müsse an erster Stelle stehen. Zur technischen Umsetzung sei beim Opt-out oder Opt-in nicht erforderlich, dass eine Erklärung unter Angabe der Identität übersandt werde.

Vielmehr könne vieles etwa durch entsprechende Einstellungen von Software erreicht werden, wie dies auch der Erwägungsgrund Nr. 66 der E-Privacy-Richtlinie[2] vorsehe.

Zu erwähnen seien auch die Überlegungen der US-amerikanischen Federal Trade Commission in ihrem Bericht vom Dezember 2010 zum „Do Not Track“-Mechanismus.[3]

Zwischen Opt-out und Opt-in bestehe kein unauflöslicher Widerspruch. Beispielsweise könnte der Nutzer bei Installation einer Software gefragt werden, welche Voreinstellung er wähle. Er könne sich dann für Opt-in oder Opt-out entscheiden.

Auf Frage eines Projektgruppenmitglieds erläutert der **Bundesbeauftragte Peter Schaar**, dass in Bereichen echter Abhängigkeitsverhältnisse für eine Einwilligung wegen der fehlenden Freiwilligkeit möglicherweise die Grundlage fehle, z. B. im Arbeitnehmerdatenschutz. Bei einem solchen strukturellen Abhängigkeitsverhältnis sei für eine Einwilligung nicht allzu viel Raum, trotzdem er noch einen gewissen Anwendungsbereich dafür sehe. Ähnlich sei es bei Quasi-Monopolen, etwa bei manchen sozialen Netzwerken. Datenschutzfreundliche kleine Netzwerke seien keine echte Alternative, da im Hinblick auf des Internet gerade der Umfang der Vernetzung entscheidend sei. Kommunikation in einem kleinen Netzwerk sei nicht wirklich möglich. Das BDSG enthalte mit dem Koppelungsverbot den Versuch, dieser Problematik Rechnung zu tragen. Allerdings werde dies eine Ausnahme bleiben müssen. Denn die Alternative sei, dass der Staat diese Frage „durchregele“.

Bei der Frage der Erforderlichkeit staatlicher IT-Projekte sei es wichtig, dass man im Prozess der Gesetzgebung die Grundsätze der Datensparsamkeit und Datenvermeidung berücksichtige, die als nicht sanktionsbewehrte allgemeine Vorgaben im Datenschutzrecht enthalten seien. Er würde eine Operationalisierung dieser Gesetzesziele bevorzugen.

Outsourcing gebe es in vielfältigen Formen, und zwar nicht nur im öffentlichen Bereich. Die Frage, inwieweit der Staat die jeweiligen Aufgaben alle selbst durchführen müsse, verneine er. Aber wenn der Staat Aufgaben durch andere durchführen lasse, müsse er gewährleisten, dass die Beauftragten bei der Datenverarbeitung den gleichen Standards und Regeln unterlägen wie der Staat.

Wichtig sei in diesem Zusammenhang der Begriff der Accountability, also der Zurechenbarkeit und Verantwortlichkeit, die im Datenschutz gestärkt werden sollte. Der jeweilige Auftraggeber (im untechnischen Sinne) müsse die Verantwortung tragen. Es müsse verhindert werden, dass Daten plötzlich anderen Rechtsordnungen unterlägen, die eventuell einen sehr viel weitergehenden Zugriff auf Daten zuließen als in Europa, so z. B. in Indien. Zur Absicherung seien auch technisch-organisatorische Maßnahmen zu treffen, etwa durch Verschlüsselung. Man könne bei dem Versuch ansetzen, das eigentliche Processing der Daten von dem inhaltlichen Zugriff und deren Auswertung zu trennen.

[2] Der entsprechende Satz lautet: „Wenn es technisch durchführbar und wirksam ist, kann die Einwilligung des Nutzers zur Verarbeitung im Einklang mit den entsprechenden Bestimmungen der Richtlinie 95/46/EG über die Handhabung der entsprechenden Einstellungen eines Browsers oder eine anderen Anwendung ausgedrückt werden.“

[3] abrufbar unter http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (Stand 23.02.2011), S. 633 ff. des Reports.

Auf eine Frage eines Projektgruppenmitglieds weist der **Bundesbeauftragte Peter Schaar** darauf hin, dass eine dezentrale Speicherung angesichts der Vernetzung im Hinblick auf den Datenschutz an Bedeutung verloren habe. Ob Daten zentral oder dezentral gespeichert seien, sei weniger entscheidend als die Frage, wie die Daten miteinander vernetzt werden könnten und über welche Sicherungsmechanismen der einzelne verfüge. Eine bestimmte Zentralität sei unvermeidbar, zumal wenn es um das Backup bestimmter Informationen gehe.

Infrastrukturen seien so zu gestalten, dass die Datensouveränität des Einzelnen möglichst gewährleistet sei. Wichtige Elemente seien dabei Verschlüsselung, Pseudonymisierung und die Verhinderung der Ent-Pseudonymisierung.

Die Verknüpfung (vom Nutzer selbst) veröffentlichter Daten stelle ein Problem dar. Aber man könne nicht verhindern, dass außerhalb unserer Rechtsordnung diese im Internet verfügbaren Daten zusammengeführt würden.

Eine Anregung eines Projektgruppenmitglieds aufgreifend, formuliert der **Bundesbeauftragte Peter Schaar** drei **zentrale Forderungen an eine Reform des Datenschutzrechts**.

Am wichtigsten sei es, technische Vorgaben so zu formulieren, dass die Grundidee des Datenschutzes, dem Einzelnen die Kontrolle über seine Daten zu geben, realisiert werden könne. Hierzu bedürfe es einer technikneutralen Definition von Zielen, die auch im Papier der Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ formuliert seien, u. a. die Vertraulichkeit, Integrität und Verfügbarkeit von Daten sowie deren Nichtverkettbarkeit.

Daneben seien Mechanismen zu entwickeln, die es ermöglichten, Betroffenenrechte unter Verwendung von Technologie besser wahrzunehmen, online Daten zu sperren oder zu löschen und Datenschutzrechte elektronisch wahrzunehmen.

Nötig sei ein neues Verständnis von Verantwortlichkeit. Bisher gebe es im Datenschutzrecht als Parteien nur den Betroffenen und die verantwortliche Stelle, die Datenverarbeitung im Auftrag und daneben den „Dritten“. Dies Rollenkonzept sei zu überdenken. Verantwortlichkeiten müssten geklärt werden. Auch die Rolle des Nutzers, der selbst - bewusst oder unbewusst- Daten preisgebe, habe sich verändert.

Auf eine Frage eines Projektgruppenmitglieds äußert sich der **Bundesbeauftragte Peter Schaar** abschließend zu der Frage, wie eine **Förderung des Datenschutzes international** vorangetrieben werden könnte. Der Bundesbeauftragte weist darauf hin, dass er den Eindruck, in den USA herrsche ein ganz anderes Datenschutzverständnis, nicht uneingeschränkt teile, etwa wenn man den umfangreichen – allerdings noch nicht beschlossenen - Bericht der Federal Trade Commission vom Dezember 2010 lese. Seine Einschätzung sei daher, dass man auf internationaler Ebene Fortschritte erzielen könne, ohne Abstriche beim eigenen Datenschutzniveau machen zu müssen.

Die internationale Datenschutzkonferenz von Madrid habe 2009 ein sehr gutes Papier mit Vorschlägen für internationale Datenschutzstandards veröffentlicht. Diese entsprächen nicht genau dem europäischen Datenschutzniveau, seien aber einstimmig verabschiedet. Wenn es international auf dieser Grundlage zu Vereinbarungen käme, wäre das ziemlich gut. Voraussetzung seien

aber Versuche seitens der Politik, etwa auch auf UN-Ebene im Rahmen von Regierungskonferenzen.

Datenschutz solle auch als Exportartikel genutzt werden. Zu prüfen sei, ob es neben der Regulierung Mechanismen gebe, die es gestatten würden, Datenschutz als Wettbewerbsvorteil einzusetzen, etwa Datenschutzaudits oder Gütesiegel. Vielleicht sei in dieser Hinsicht auch mehr Marketing nötig.