Deutscher Bundestag

Projektgruppe
„Datenschutz, Persönlichkeitsrechte“

Berlin, 07. Oktober 2010

Enquete-Kommission Internet und digitale Gesellschaft

Ergebnisprotokoll der dritten Sitzung der Projektgruppe am 04. Oktober 2010

Vor Eintritt in die Tagesordnung

Es wird erläutert, dass der Spiegelstrich „Beschäftigtendatenschutz“ unter 2.3 des am 16. August 2010 beschlossenen Themenkatalogs auch Beschäftigtenverhältnisse im öffentlichen Dienst umfasse. Das Protokoll der Sitzung vom 16. August 2010 wird mit großer Mehrheit genehmigt.

Die am 30. September 2010 versandte Tagesordnung wird ohne Änderungen einvernehmlich beschlossen.

Die Online-Redaktion der Enquete-Kommission nimmt die Berichterstattung aus den Projektgruppen auf. Um einerseits die Nichtöffentlichkeit der Sitzungen zu wahren und andererseits eine frühzeitige Einbeziehung der Öffentlichkeit in die Arbeit der Projektgruppen zu gewährleisten, erfolgt die Berichterstattung durch die Online-Redaktion des Sekretariats auf der Microsite der Kommission neutral und ohne Nennung von Namen. Die Projektgruppe erklärt ihr Einverständnis mit dieser Verfahrensweise.

Die Projektgruppe kommt einvernehmlich überein, dass Tagesordnungen, Sitzungstermine und Protokolle (in anonymisierter Form) vom Sekretariat auf der Microsite der Enquete-Kommission veröffentlicht werden, nicht aber vorbereitende Papiere aus den Reihen der Mitglieder der Projektgruppe. Eine Veröffentlichung dieser Papiere durch die jeweiligen Verfasser an anderer Stelle ist möglich.

Eine zu TOP 2 überreichte Tischvorlage wird als Sitzungsunterlage aufgenommen. Für Sitzungen am Montag sollen Vorlagen jedoch grundsätzlich bis zum Donnerstag der Vorwoche im Sekretariat vorliegen.

Für die nächsten Sitzungen der Projektgruppe soll nochmals versucht werden, Termine in einer Sitzungswoche und ohne zeitliche Überschneidung mit parlamentsinternen Veranstaltungen und anderen Projektgruppen auszumachen. Hierzu wird es zeitnah weitere Informationen per E-Mail geben. Für den Fall, dass dies nicht zum Erfolg führt, wird die Frage nochmals in einer Enquete-Sitzung angesprochen werden.

TOP 1:
Diskussion zu Gliederungspunkt 1. des Arbeitsprogramms „Bestandsaufnahme“

Hierzu liegt ein Textvorschlag vor. Er wurde auf der Grundlage der Gliederung erstellt, die in der Sitzung vom 16. August 2010 vorgelegt wurde.

Die Projektgruppe stellt einvernehmlich fest, dass der derzeitige Stand der normierten Gesetzgebung in dem Papier ausreichend festgehalten sei. Bevor die Projektgruppe sich unter Punkt 3. des Themenkataloges mit dem politischen Handlungsbedarf befassen wird, soll überprüft werden, ob sich zwischenzeitlich der Bedarf einer Aktualisierung, insbesondere im Bereich der Rechtsprechung, ergeben hat.

TOP 2:
Diskussion zu Gliederungspunkt 2.1 des Arbeitsprogramm „Datenschutz: Prinzipien, Ziele, Werte“

Auf der Grundlage der eingereichten Beiträge wurden folgende Gesichtspunkte (entsprechend der Gliederung des Themenkataloges) angesprochen:

Recht auf informationelle Selbstbestimmung / Einwilligung / Grundrechtsverzicht/ Schutz des Allgemeinen Persönlichkeitsrechts

- Verhältnis der einschlägigen Grundrechte zueinander (Grundrecht auf informationelle Selbstbestimmung, Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme - „IT-Grundrecht“) sowie die Bedeutung des IT-Grundrechts; Grundzüge der verfassungsgerichtlichen Rechtsprechung (Richtervorbehalt, Verhältnismäßigkeit und dabei vorzunehmende Güterabwägung,

Eingriffsvoraussetzungen für Sozialsphäre, Privatsphäre und Intimsphäre).

- Datenschutz als unverzichtbares Recht, das eine verfassungsrechtliche Ausgestaltung als Grundrecht auf informationelle Selbstbestimmung gefunden habe. Die Preisgabe eigener Daten sei in diesem Rahmen möglich und stelle keinen Verzicht auf das Grundrecht dar. Da in der digitalen Welt jede Äußerung Daten hinterlasse, sei der Stellenwert des Datenschutzes und ggf. auch die sich daraus ergebende Notwendigkeit von Regulierungen gestiegen, gerade auch im nichtöffentlichen Bereich (Nutzer gegenüber Unternehmen).

- Kern der Diskussion sollten soziale Regeln, nicht aber die derzeitige Rechtslage sein.

- Recht und Grundrechte seien unmittelbarer Ausdruck ethischer Überzeugungen. Auf das Grundrecht auf informationelle Selbstbestimmung könne – auch aus verfassungsrechtlichen Gründen – nicht verzichtet werden, weil die Menschenwürde tangiert sei.

- Die Projektgruppe solle eine Aussage zur allgemeinen Geltung des Zweckbindungsgrundsatzes treffen. Der Grundsatz der Datenvermeidung und Datensparsamkeit solle gestärkt und mit Sanktionen bewehrt werden.

- Eine Einwilligung bedürfe immer einer gesetzlichen Grundlage.

- Die Hinterlegung eigener Daten in sozialen Netzwerken bedeute gerade die Wahrnehmung des Grundrechts und keinen Verzicht. Hierfür ein Gesetz als Grundlage zu fordern, sei unzutreffend.

- Dem Einzelnen komme ein dem Eigentum vergleichbares, absolutes Herrschaftsrecht über seine Daten zu.

- Der Begriff des Untermaßgebotes sei zu klären, insbesondere da es vorliegend um den Schutzbereich der Menschenwürde gehe.

Dürfen Einzelne gegen ihren Willen geschützt werden? Differenzierung des Datenschutzbedürfnisses

- Es gebe gegenwärtig einen Prozess der Wertebildung. Das Internet wolle Transparenz schaffen. Bezogen auf Staaten sei das ein allgemeines zentrales Anliegen, auch im Bezug auf Unternehmen und gesellschaftliche Organisationen. Diese Transparenzerwartung werde heute teilweise auch auf den Einzelnen bezogen. Die Frage sei, ob dies negativ zu bewerten oder die Rechtsordnung das befördern solle. Informationen über andere Menschen seien für den gesellschaftlichen Diskussionsprozess förderlich. Dies nütze der Autonomie des Einzelnen und bedeute einen gesellschaftlichen und individuellen Nutzen. Genau zu untersuchen sei allerdings, wo spezielle Schutzbedürfnisse bestehen (etwa bei Kindern und Jugendlichen) und wann der Staat den Einzelnen vor sich selbst schützen dürfe. Das Grundgesetz gehe nicht vom Verständnis eines paternalistischen Staates aus. Dem sei zuzustimmen. Es gebe ein Recht zur Selbstgefährdung, solange Bedeutung und Tragweite der eigenen Entscheidung klar seien. Das Kräfteverhältnis zwischen Nutzer und Anbieter habe sich verschoben. Der Nutzer könne heute stärker auf alternative Angebote ausweichen als früher. Die Gesellschaft könne einen adäquaten Schutz in vielen Fällen selbst generieren.

- Auch in anderen Bereichen gelte, dass der Staat spätere Korrekturen durch den Wettbewerb nicht abwarte, sondern die Beeinträchtigung von Rechtsgütern durch gesetzliche Standards möglichst von vornherein verhindere.

- Transparenz und Autonomie stießen dann an Grenzen, wenn die Menschenwürde oder Daten Dritter betroffen seien. In anderen Bereichen (Auskunfteien, Scoring) handele es sich trotz formal vorliegender Einwilligung nicht um die freiwillige Preisgabe von Daten. Freiwilligkeit und Unfreiwilligkeit seien insoweit zu unterscheiden.

- Die Vorstellung, das Internet wolle Transparenz schaffen, würde von vielen so nicht nicht geteilt. Für viele Menschen sei das Internet ein Mittel, sich zu informieren, zu kommunizieren, Geschäfte zu tätigen, sozusagen statt der herkömmlichen Kommunikation durch Telefon,

Zeitung, etc. Diese Menschen hätten das Bedürfnis, dort einen geschützten Raum vorzufinden.

- Einen Zwang zur Transparenz müsse man verhindern. Auch die geschilderte Transparenz etwa der politischen Einstellung von Gesprächspartnern sei problematisch. Das angesammelte Wissen könne missbraucht werden. Nicht überall und jederzeit herrschten demokratische Verhältnisse. Die Aussage, Transparenz bezogen auf den Einzelnen fördere die Demokratie, sei daher problematisch.

- Die Vorstellung von Transparenz dürfe nicht der Bevölkerungshälfte oktroyiert werden, die eine weitreichende Transparenz ablehnten, oder dies auch als „Nacktsein“ empfänden. Die Regularien müssten beiden Gruppen gerecht werden, insoweit gehe es hier- wie auch sonst häufig im Datenschutz - um Solidarität. Im Übrigen stünden hinter Forderungen nach Transparenz häufig auch kommerzielle Interessen.

Stärkung des Datenschutzbewusstseins / Selbstdatenschutzes

- Beim Thema Selbstdatenschutz sei ein weitgehender Konsens dahingehend zu erwarten, dass die Medienbildung zu stärken sei, damit der Nutzer hinreichend über Bedeutung und Folgen einer Datenpreisgabe informiert sei. In der Sache handele es sich um eine Ländersache, so dass keine gesetzgeberischen Empfehlungen an den Bundestag zu richten seien. Viele Nutzer seien sehr arglos, auch weil Geschäftsmodelle nicht verstanden würden. Entgegen der Prognose der vorausgegangenen Enquete-Kommission erweise sich die Notwendigkeit der Preisgabe eigener Daten nicht als Hürde für Geschäftsmodelle im Internet.

- Unter dem Gesichtspunkt des Selbstdatenschutzes sei nicht nur die Medienkompetenz zu stärken, sondern auch Transparenz auf Seiten des Vertragspartner einzufordern (was ist das für ein Dienst? wie werden Daten erhoben und verarbeitet?). Hier gehe es um Informationspflichten, da dies vom Nutzer nicht geleistet werden könne. Zu diskutieren seien Alternativen außerhalb (zunehmend unübersichtlicher) AGB, etwa durch Buttons. Konsens solle auch darüber erzielt werden, dass die Privatsphäre begünstigende Voreinstellungen (Privacy by default), technische Möglichkeiten des Selbstdatenschutzes, z. B.

durch Browsereinstellungen, und z. B. anonyme Bezahldienste zu fördern seien.

- Neben den genannten Gesichtspunkten gehe es auch um unterschiedliche Nutzergruppen mit differenziertem Schutzbedürfnis.

- Auch die Frage, wie man mit falschen Angaben im Netz umgehe (falsche Angaben Dritter über die eigene Person), sei eine Frage der Medienkompetenz, etwa der Gewichtung der Information und der Glaubwürdigkeit der Quelle; rechtlich könne und solle man dagegen nicht vorgehen.

Grenzen des nationalen Datenschutzrechts

- Die Forderung, bei der Formulierung internationaler Datenschutzstandards das jeweils höchste beteiligte Datenschutzniveau zu Grunde zu legen, sei nicht realistisch, da dann keine Verhandlungsergebnisse erzielt würden.

- Nationale datenschutzrechtlichen Mindestvorstellungen sollten auch im internationalen Bereich angestrebt werden; eine These hierzu sei, dass ein hoher Schutzstandard auch einen Wettbewerbsvorteil darstelle.

Recht auf Anonymität

- Die Formulierung, Anonymisierungstechniken für die legale Nutzung des Internets bereitzustellen, werfe die Frage auf, wie legale und illegal Nutzung abgegrenzt werden sollten.

- Es bestehe ein Missverhältnis zwischen der Möglichkeit, sich anonym im Netz zu bewegen und der Unmöglichkeit, anonym im Netz Geschäfte zu tätigen. Beides stehe im krassen Gegensatz zur „analogen“ Welt, in der insbesondere viele Rechtsgeschäfte anonym abgewickelt werden könnten. Beide Aspekte seien mit datenschutzrechtlichen Fragen verbunden (mögliche Grenzen der Kriminalitätsbekämpfung in Fällen der Anonymisierung, Fehlen eines digitalen Bargelds), die zu diskutieren seien.

- Eine komplette Anonymität gebe es im Internet nicht, da im Falle erheblicher Strafvorwürfe stets die IP-Adressen herausgegeben würden. Die Frage anonymer Geschäfte

müsse diskutiert werden. Ein Vergleich mit Geschäften außerhalb des Netzes zeige, dass der Hinweis auf mögliche Straftaten nicht zielführend sei, da außerhalb des Netzes etwa Messer anonym erworben werden könnten.

kollidierende Rechtsgüter

- Zu fragen sei, wann sich der Datenschutz gegen den Schutzwürdigen richte, etwa weil ein zu hoher Preis entstehe oder der Service leide. Ein besonders hohes Schutzniveau bedeute eben auch, dass es manchen Dienst oder manches Angebot in Deutschland nicht geben werde oder auf niedrigerem Niveau. Dabei gehe es um eine Güterabwägung. Anonymität im Netz sei möglich, gehe dann aber möglicherweise etwa zu Lasten der Kriminalitätsbekämpfung.

- Transparenz als Wert stehe im Spannungsverhältnis zu anderen Werten, darunter auch die Sicherheit. Hier liege eine wichtige Aufgabe der Projektgruppe, Vorlagen für die Politik im Sinne eines Zukunftsbildes zu liefern. Das Auftreten von Stuxnet habe gerade in jüngster Zeit gezeigt, dass es virtuelle Straftaten gebe.

- Transparenz und Meinungsfreiheit seien die guten Seiten des Netzes. Probleme begännen bei Angaben über Dritte, auch wegen der Tatsachen, dass Daten im Netz dauerhaft vorhanden seien. Der Begriff der virtuellen oder digitalen Straftat sei irreführend. Es gebe nur Straftaten mit Internetbezug. Das Internet werde dann als Kommunikationsmittel eingesetzt. Aber auch das öffentliche Telefon sei sicher im Zusammenhang mit Straftaten eingesetzt worden, ohne dass es hier Einschränkungen gegeben habe. Die polizeiliche Kriminalitätsstatistik 2007/08 zeige im Übrigen, dass Straftaten mit Internetbezug zu über 80 % aufgeklärt würden, andere Taten nur zu 55 %.

- Hinter der Feststellung, dass zuviel Datenschutz Probleme aufwerfe, stehe ein Konflikt von Rechtsgütern, etwa wenn es um Datenschutz und Meinungsfreiheit gehe. Dies müsse noch diskutiert werden. Jedenfalls bedeute zu strenger Datenschutz nicht die Einschränkung bestimmter Dienstleistungen. Soziale Netzwerke seien auch unter Wahrung des Datenschutzes möglich. Tatsächlich sei der

nicht korrekte Umgang mit dem Datenschutz das von den Unternehmen selbst verursachte Problem.

Schutzgegenstand: Was sind personenbezogene Daten? Wieweit geht der Schutzbedarf?

- Schutzgegenstand seien nur Daten mit Personenbezug. Ein Ausbau des Datenschutzes zu einem weiter verstandenen Informationsschutzrecht sei daher sehr kritisch zu diskutieren. Eine solche Ausweitung des Schutzgegenstandes sei der Informationsgesellschaft ebenso abträglich, wie die Übertragung der Grundsätze des Arbeitnehmerdatenschutzes auf soziale Netzwerke.

- Die Frage des Schutzgegenstand (personenbezogene oder auch personenbeziehbare Daten) müsse vertieft diskutiert werden, insbesondere wann ein Datum als personenbezogen anzusehen sei.

TOP 3:
Weitere inhaltliche Arbeit: Struktur und Zeitplan

Es bestand Einvernehmen, die mittlerweile eingerichtete Etherpad-Teamsite zur Bearbeitung von Texten zu nutzen.

Weiter wurde aus den Reihen der Projektgruppenmitglieder angeregt, die eingereichten Papiere als Grundlage für Pads zu nutzen, konsensuale Passagen und kontroverse Punkte zu ermitteln und auch den Inhalt der Diskussion während der Sitzung in die Texte einzubeziehen.

Es sollen zeitnah neue Threads im Forum der Projektgruppe eingerichtet werden, innerhalb derer die heutige Diskussion fortgeführt werden könnte. Weiterhin soll eine Synopse der eingereichten Papiere erstellt werden.