Enquete-Kommission Internet und digitale Gesellschaft

Deu

Deutscher Bundestag
Enquete-Kommission
Internet und digitale Gesellschaft

Ausschussdrucksache
17(24)032

TOP 1c am 4.7.2011

Projektgruppe „Datenschutz, Persönlichkeitsrechte“

30.6.2011

Handlungsempfehlungen

Antrag der Fraktionen CDU/CSU und FDP auf Aufnahme von weiteren Handlungsempfehlungen

Die Enquete-Kommission möge beschließen:

Abschnitt „II. Die Vorgaben für nationalen, europäischen und internationalen Datenschutz“ wird um den nachfolgenden Text nach Nr. 5 ergänzt:

6. Aus Sicht der Enquête-Kommission kann eine datenschutzrechtliche Folgenabschätzung zwar zu einer Förderung des Datenschutzes von Beginn an führen. Sie kann zugleich aber auch zu einem erheblichen bürokratischen Mehraufwand für betroffene Unternehmen führen. Sie sollte daher nur in bestimmten Fällen, in denen sensible Daten verarbeitet werden oder wenn die jeweilige Verarbeitung mit besonderen Risiken verbunden ist verbindlich eingeführt werden.

7. Bereits im geltenden europäischen wie auch im nationalen Datenschutzrecht gibt es ein umfassendes System des individuellen Rechtsschutzes. Die Enquête-Kommission kann daher nicht erkennen, wie die Einführung eines Verbandsklagerechts zu einer Verbesserung dieses individuellen Rechtsschutzes führen kann. Sie gibt zudem zu bedenken, dass im Datenschutzrecht keine vergleichbare Position des Betroffenen wie im Verbraucherschutzrecht vorhanden ist. Schließlich gibt es im Datenschutzrecht gerade nicht ein Verhältnis von Unternehmer und Verbraucher, sondern nur Rechtsbeziehungen zwischen nicht-öffentlichen und öffentlichen Stellen sowie zwischen einzelnen Privatpersonen. Verbandsklagen könnten jedoch, wenn überhaupt, nur in einzelnen Konstellationen zu einer Stärkung der Individualrechte führen. Sie würden im Gegenzug jedoch zu erheblichen Rechtsunsicherheiten bei allen betroffenen Unternehmen führen.

Zudem möge die Enquete-Kommission die nachfolgenden Handlungsempfehlungen beschließen:

XIII. Grundprinzipien des Datenschutzrechts

Die verschiedenen Grundprinzipien des deutschen Datenschutzrechts sind durch die Enquete-Kommission im Kapitel 2.1 – Prinzipien, Ziele, Werte – ausführlich dargestellt worden. Die Enquete-Kommission geht davon aus, dass trotz rasanter technischer Weiterentwicklungen diese Grundprinzipien auch in Zukunft einen Anspruch auf Geltung haben müssen. Dabei sollten die Grundsätze der Verhältnismäßigkeit, der Datensicherheit und Sparsamkeit, der Zweckbindung und Transparenz noch stärker zur Geltung gebracht werden.

Es muss jedoch auch Anspruch des nationalen Gesetzgebers sein, das Datenschutzrecht, unter Berücksichtigung der europarechtlichen Vorgaben, fortlaufend weiter zu entwickeln. Vorrang sollte hierbei auf eine technikneutrale Ausgestaltung von datenschutzrechtlichen Bestimmungen gelegt werden. Angesichts einer zunehmenden Komplexität und Länge der Regelungen müssen auch Übersichtlichkeit, Lesbarkeit und die Verständlichkeit eine größere Rolle einnehmen.

Neben durchzuführenden sprachlichen Vereinfachungen und Verbesserungen sollten auch aktuelle und zukünftige Entwicklungen bei den Definitionen und Begriffsbestimmungen (beispielsweise zur Personenbeziehbarkeit) durch den Deutschen Bundestag beobachtet werden.

XIV. Koppelungsverbot

Die Enquete-Kommission empfiehlt dem Deutschen Bundestag, am bestehenden Koppelungsverbot in § 28 Abs. 3b BDSG festzuhalten. Die bisherige Regelung, die es verbietet, den Vertragsschluss von der Angabe personenbezogener Daten abhängig zu machen, wenn ein anderer Zugang zu gleichwertigen Angeboten und Diensten ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist, also Unternehmen eine marktbeherrschende Stellung haben, stellt einen ausgewogenen Ausgleich zwischen den zu berücksichtigenden Interessen der Nutzer und der Unternehmen dar. Eine Ausweitung des Kopplungsverbotes würde letztlich zu einem vollständigen und damit unnötigen, mithin einem unverhältnismäßigen, gesetzlichen Verbot von Diensten führen.

XV. Auskunfts- und Widerrufsrechte

Bereits nach dem geltenden Datenschutzrecht ist die Wirtschaft gefordert, für Transparenz beim Umgang mit personenbezogenen Daten zu sorgen und den Nutzer nicht im Unklaren über die Speicherung und Nutzung seiner Daten zu lassen. Für die Zukunft empfiehlt die Enquete-Kommission dem Deutschen Bundestag,

den Transparenzgrundsatz technikneutral auszugestalten. Für die Nutzer muss insbesondere erkennbar sein, von welcher verantwortlichen Stelle personenbezogene Daten erhoben werden. Wenn Daten weitergegeben oder von anderen genutzt werden, soll unter Berücksichtigung der technisch vorhandenen Möglichkeiten und unter Wahrung des Betriebs- und Geschäftsgeheimnisses eine Rückverfolgbarkeit für den Betroffenen geschaffen werden. Dies könnte die Geltendmachung der Rechte auf Auskunft, Löschung, Sperrung oder Widerspruch weiter erleichtern.

Die Enquete-Kommission empfiehlt zudem eine Befassung des Deutschen Bundestages über die Ausübung und weitere Stärkung von Betroffenenrechten im Bundesdatenschutzgesetz (vgl. §§ 33 ff. BDSG), insbesondere ob verantwortliche Stellen zu einer besseren und verständlicheren Information der Betroffenen über die Verwendung der Daten bei der Erhebung verpflichtet werden können und ob eine effektivere Ausgestaltung der bereits vorhandene Rechte auf Auskunft, Löschung, Sperrung oder Widerspruch (vgl. § 4 Abs. 2 und 4 BDSG) denkbar ist. Dabei sollte dem Einsatz moderner Technologien (etwa dem Recht auf elektronische Auskunft über die gespeicherten Daten und einem elektronischen Widerspruchsrecht) besondere Bedeutung zukommen. Denn die Geltendmachung der Betroffenenrechte sollte auf die gleiche Art möglich sein, wie in die Datenerhebung eingewilligt wurde, bei Angeboten im Internet konsequenterweise auch elektronisch.

XVI. Datenbrief

Die Enquete-Kommission empfiehlt dem Deutschen Bundestag, ein Datenbrief-Konzept nicht weiter in Erwägung zu ziehen. Der Datenbrief entspräche nicht dem Grundsatz der Datensparsamkeit (vgl. § 3a BDSG). Für die Zustellung des Datenbriefes wären zumindest die Adresse des betroffenen Nutzers oder andere Kontaktdaten erforderlich, die für den eigentlich in Anspruch genommenen Dienst eventuell gar nicht anfallen würden. Die Daten des Betroffenen müssten möglicherweise zentral – mit erhöhtem Aufwand für die Datensicherheit – in einer Datenbank geführt und laufend aktualisiert werden. Das Risiko besteht, dass selbst sensible Daten des Betroffenen an unberechtigte Dritte gelangen. Der bürokratische Aufwand aller Beteiligten steht in keinem Verhältnis zum erwarteten Nutzen.

XVII. Anonyme Bezahlsysteme

Mit dem technischen Fortschritt nimmt auch der elektronische Zahlungsverkehr im Internet zu. Zunehmend werden mehr und mehr alltägliche Einkäufe im Inter-

net abgewickelt. Hierbei fallen auch eine Vielzahl personenbezogener Daten an. Die Einführung eines digitalen Bargeldes könnte jedoch zu einer Reduzierung der personenbezogenen Daten im Zahlungsverkehr des Internets führen. Darüber hinaus würde eine Einführung des digitalen Bargelds, eine Annäherung an alltägliche Barzahlungsgeschäfte in der „realen Welt“ fördern. Sie bietet allerdings auch Risiken, da ein weitestgehend anonymer Zahlungsverkehr zugleich eine Erleichterung für die Begehung von Straftaten sein könnte und damit das Internet als Tatmittel missbraucht würde. Internationale Lösungen sollten daher dann unterstützt werden, wenn sie Chancen und Risiken eines solchen Bezahlungssystems in einen angemessenen Ausgleich setzen. Die Enquete-Kommission regt daher die Bundesregierung an, entsprechende Forschungsvorhaben, die sich mit der Einführung eines digitalen Bargelds auseinandersetzen, positiv zu begleiten.

XVIII. Technischer Datenschutz

Datenschutz lässt sich in der Praxis nur dann sicherstellen, wenn die informationstechnischen Systeme im öffentlichen und nicht-öffentlichen Bereich gegen unberechtigten Zugriff und missbräuchliche Nutzung von innen und außen geschützt sind. Die hierfür einschlägigen Schutzregelungen (z.B. Anlage zu § 9 BDSG) stammen aus einer Zeit, als Datenverarbeitung durch Großrechner in abgeschotteten Rechenzentren gekennzeichnet war.

Beispielsweise kommen im Zuge des eGovernment längst Online-Verfahren zum Einsatz, bei denen Bürger selbst auf die IT-Systeme der Verwaltung zugreifen. Durch diese Entwicklung und die fortschreitende Vernetzung der Verwaltungssysteme untereinander wird es zunehmend schwieriger, das Regelwerk auf neue Technologien und vernetzte Infrastrukturen anzuwenden. Die Enquete-Kommission hält es für erforderlich zu prüfen, ob die technisch-organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes (Anlagen zu § 9 BDSG und entsprechende Regelungen in den Datenschutzgesetzen der Länder) durch technikneutrale Schutzziele ersetzt werden müssen, die dann durch dokumentierte Rahmen- und Verfahrenskonzepte umgesetzt und dem aktuellen Stand der Technik fortgeschrieben werden müssten.

XVIII. Datenschutz für Kinder und Jugendliche

Aktuelle Studien zeigen, dass viele Kinder und Jugendliche mit der Nutzung moderner Technik bereits sicher und selbstverständlich umgehen können. Dennoch hält die Enquete-Kommission auch für die Zukunft, ein verstärktes Bemühen um

Aufklärung und Bildung auch im Bereich des Datenschutzes für geboten. Vielversprechende Bildungsangebote staatlicher als auch nicht-staatlicher Organisationen liegen hierzu bereits vor. Es gilt daher, diese Angebote noch sichtbarer für die Nutzer zu machen. Die Enquete-Kommission sieht bei der Stärkung des Selbstdatenschutzes von Kindern und Jugendlichen auch die Länder aufgrund ihrer Zuständigkeit für den Bildungsbereich in der Pflicht.

Unternehmen, die Dienste im Internet anbieten, können die Einwilligungsfähigkeit von Minderjährigen bisher nur schwer überprüfen. Die Enquete-Kommission empfiehlt daher der Bundesregierung, die gesetzlichen Voraussetzungen der Einwilligungsfähigkeit von Minderjährigen zu überprüfen. In die vorzunehmende Prüfung sollte die bisher maßgebliche Einsichtsfähigkeit, aber auch die Möglichkeit einer festen Altersgrenze einbezogen werden. Dabei ist zu beachten, dass die Informations- und Kommunikationsrechte von Minderjährigen auch in Zukunft gewahrt bleiben.

XIX. Profilbildung

Die Enquete-Kommission empfiehlt dem Deutschen Bundestag zu prüfen, ob die Bildung bestimmter Profile gesetzlich zu regeln ist. Dabei könnten bestimmte Profilbildungen von einer ausdrücklichen gesetzlichen Regelung oder aber der Einwilligung des Betroffenen abhängig gemacht werden

Insbesondere durch Berechnungen, Vergleiche und statistische Korrelationssoftware können in bestimmten Fällen personenbezogene Daten, die Unternehmen im Rahmen von Internetdiensten erhoben haben zu umfassenden Profilen zusammengeführt und zu vielfältigsten Zwecken genutzt werden. Durch solche Profile können in einigen Bereichen Verhalten, Gewohnheiten und Neigungen eines Nutzers abgebildet und kategorisiert werden, ohne dass es dem Nutzer zuvor offen gelegt wird.

Es sind daher für bestimmte Profilbildungen eine gesetzliche Definition dieses Begriffs sowie Regelungen zum Umgang mit ihnen zu erwägen. Dabei ist zu berücksichtigen, dass nicht jede Verknüpfung von Informationen mit einer natürlichen Person zu einem schwerwiegenden Eingriff in das informationelle Selbstbestimmungsrecht führt und eine gesetzliche Regelung erfordert. Wichtig ist daher, für diese Fälle eine klare Unterscheidung zu treffen. Transparenz für Betroffene und Informationen über Umfang und Herkunft der Profildaten und die beabsichtigte Verwendung des Profils sind notwendig. Diese Ziele könnten auch mit Hilfe von Selbstverpflichtungen erreicht werden.

XX. Veröffentlichung von Daten im Internet

Bei der Veröffentlichung von personenbezogenen Daten im Internet sind in der Regel immer mehrere Grundrechte in einen angemessenen Ausgleich zu bringen. Neben dem Grundrecht auf informationelle Selbstbestimmung sind dies beispielsweise auch das Grundrecht auf Meinungsfreiheit und das Grundrecht auf Informationsfreiheit. Aber auch die Freiheit der Berichterstattung und das Informationsinteresse der Allgemeinheit können zu berücksichtigen sein. Gesetzliche Regelungen für diesen Bereich können daher mithin nur eine Konkretisierung verfassungsrechtlicher Grenzen darstellen. Die Enquete-Kommission empfiehlt daher der Bundesregierung, diesen Bereich weiterhin sorgfältig zu beobachten und den Schutz vor schwerwiegenden Eingriffen in das Persönlichkeitsrecht sicher zu stellen.

Widerspruchsrechte gegen bestimmte Veröffentlichungen im Internet, die vorrangig auf der Basis von Selbstverpflichtungen von Plattformbetreibern umgesetzt werden könnten, können ein wirksames Mittel zur Wahrung des Grundrechts auf informationelle Selbstbestimmung sein. Allerdings muss es auch hierbei zu einer angemessenen Berücksichtigung verschiedener, möglicherweise auch gegenläufiger, Interessen kommen. Dies muss durch entsprechende verfahrensrechtliche Regelungen abgesichert sein. Bereits bestehende Widerspruchsregelungen (vgl. § 35 Abs. 5 BDSG, Art. 14 der EU-Datenschutzrichtlinie) sind mit einzubeziehen.

XXI. Regulierte Selbstregulierung

Aus Sicht der Enquete-Kommission ist Selbstregulierung durch die Wirtschaft ein wichtiges Instrument im Datenschutz. Im Vergleich zur Gesetzgebung ist sie flexibler und kann schneller auf neue Entwicklungen reagieren. Selbstverpflichtungen der Wirtschaft können darüber hinaus das Datenschutzniveau heben, zum Beispiel durch Vorgaben zur Datenvermeidung und Datensparsamkeit. Dort, wo sich die Selbstregulierung im Interesse der Nutzer und der Unternehmen bewährt, ist dann ein Handeln durch den Gesetzgeber nicht notwendig.

Die zentrale Informations- und Widerspruchsstelle, wie sie der Datenschutz-Kodex für Geodatendienste vorsieht und von der – ohne eine zentrale Speicherung - Widersprüche an die jeweiligen Unternehmen weitergegeben werden, erleichtert es den Nutzern, ihr Widerspruchsrecht auszuüben. Für die Beilegung von Streitigkeiten über die Ausübung von Nutzerrechten kann auf dieser Grundlage

eine Schlichtungsstelle Datenschutz zur effektiven unbürokratischen Durchsetzung der gesetzlichen Rechte auf Löschung, Sperrung und Widerspruch beitragen. Diese könnte unter Beteiligung von Wirtschaft und Datenschutzverbänden realisiert werden.

XXII. Stiftung Datenschutz

Die Enquete-Kommission ist der Ansicht, dass die Errichtung einer Stiftung Datenschutz mit dem Auftrag, Produkte und Dienstleistungen auf Datenschutzfreundlichkeit zu prüfen, ein Datenschutzaudit zu entwickeln und Bildung im Bereich des Datenschutzes zu stärken, den Selbstdatenschutz durch Aufklärung verbessern kann. Sie begrüßt daher im Grundsatz die von der Bundesregierung geplante Stiftung Datenschutz.

Diese Stiftung kann u. a. Kriterien für die Zertifizierung von Diensten sowie für ein einheitliches Gütesiegel aufstellen und damit eine leicht nachzuvollziehende Vergleichbarkeit für Unternehmen und Bürger herstellen. Dadurch kann sich auch eine Erleichterung bei der Auswahl zwischen einer Vielzahl von Anbietern ergeben und zugleich das Vertrauen der Bürger in neue Technologien gestärkt werden. Für Unternehmen kann sie Anreize setzen, hohe datenschutzrechtliche Anforderungen einzuhalten.

Weitere Aufgaben können die Stärkung des Selbstdatenschutzes sowie Aufklärung und Bildung im Datenschutz sein.

Die Enquete-Kommission fordert daher die Bundesregierung bei Errichtung der Stiftung auf, folgende Punkte – die für eine wirkungsvolle Arbeit einer Stiftung Datenschutz mit vorstehendem Auftrag von großer Bedeutung sind – zu berücksichtigen:

1. Die Stiftung ist mit Distanz zu den zu bewertenden Unternehmen zu organisieren. Personell ist darauf zu achten, dass bei der Besetzung der Gremien Unternehmen oder Verbände zwar beteiligt werden, aber auf die Unabhängigkeit der Stiftung an sich keinen Einfluss haben. Dies könnte z. B. durch die Beteiligung in einem Beirat, der beratende Funktion hat, geschehen. Finanziell sollte die Stiftung nicht allein vom Bundeshaushalt abhängig sein. Bei der Annahme von Zuwendungen hat die Stiftung jedoch darauf zu achten, dass die Unabhängigkeit nicht gefährdet werden darf.

2. Bei der Entwicklung von Gütesiegeln durch die Stiftung ist darauf zu achten, dass es ein einheitliches Gütesiegel gibt und somit eine inflationäre Handhabung bei der Vergabe vermieden wird. Ebenso ist das Verfahren für die Vergabe transparent zu gestalten. Die Gütesiegel sind nur für eine bestimmte Zeit zu erteilen und müssen überprüfbar sein.

3. Im Bereich der Bildung sollte die Stiftung Datenschutz sowohl schulisch als auch außerschulisch tätig sein. Sofern sie im schulischen Bereich tätig wird, sollten durch eine Abstimmung mit den Ländern von Beginn an Zuständigkeitsverletzungen ausgeschlossen werden.

4. Im Bereich der Aufklärung wird der Stiftung empfohlen, ein zentrales Infoportal oder ein virtuelles Datenschutzbüro zu schaffen. Die Stiftung sollte hier auch eine koordinierende Funktion hinsichtlich bereits bestehender Bildungsinitiativen in diesem Bereich übernehmen.

5. Im Bereich der Datenschutzforschung wird angeregt zu prüfen, ob die Stiftung Datenschutz insbesondere bei der Entwicklung und dem Ausbau von Instrumenten des technischen Datenschutzes tätig werden kann. Mögliche Tätigkeitsfelder eröffnen sich sowohl im Bereich der Koordination der Forschungsmittelvergabe als auch für den Bereich eigener Forschungsanstrengungen.

XXIII. Schadensersatzansprüche im Datenschutzrecht

Die Enquete-Kommission empfiehlt dem Deutschen Bundestag, weiter zu beobachten, ob das Sanktionssystem im Datenschutzrecht weiterhin effektiven Schutz gewährleistet. Auch ein Wegfall von Antragserfordernissen bei bestimmten Straftaten im Bereich der Datenverarbeitung, die über individuelle Verstöße hinausgehen, kann zu einer Verbesserung in Betracht gezogen werden.

Wenn eine verantwortliche Stelle dem Betroffenen durch eine datenschutzrechtlich unzulässige oder unrichtige Verarbeitung seiner personenbezogenen Daten einen Schaden zufügt, macht sie sich schadensersatzpflichtig. Die Enquete-Kommission empfiehlt dem Deutschen Bundestag, zu evaluieren, inwieweit die Ansprüche praxistauglich sind und sich als Instrument neben Bußgeldern und Sanktionen etablieren. Falls Verbesserungen erforderlich erscheinen und Unterlassungs- und Beseitigungsansprüche nicht ausreichen, könnte unter anderem ein Ersatz immaterieller Schäden wie im öffentlichen Bereich auch für den nichtöffentlichen Bereich in die Überlegungen mit einbezogen werden.

XXIV. Beschäftigtendatenschutz

Die Enquete-Kommission begrüßt, dass die Bundesregierung ein Gesetz zur Regelung des Beschäftigtendatenschutzes auf den Weg gebracht hat. Die Regelungen sollten einen Ausgleich zwischen den Interessen der Arbeitnehmer und Arbeitgeber und damit insgesamt eine Verbesserung des Arbeitnehmerdatenschutzes beinhalten. Es sollten nur solche Daten verarbeitet werden die für das Arbeitsverhältnis erforderlich sind. Datenverarbeitungen, die sich beispielsweise auf für das Arbeitsverhältnis nicht relevantes außerdienstliches Verhalten oder auf nicht dienstrelevante Gesundheitszustände beziehen, müssen ausgeschlossen sein.

Der Einsatz von Informations- und Kommunikationstechnologie am Arbeitsplatz ist heute nicht mehr wegzudenken. Das Spannungsverhältnis zwischen den Interessen von Arbeitnehmern und Arbeitgebern muss vor allem beim Einsatz von webbasierten Kontrollinstrumenten und im Rahmen der gestatteten auch privaten Nutzung betrieblicher Telekommunikationsmittel praxisgerecht und rechtsklar ausgestaltet werden. Hierfür sollte eine eigenstände Regelung getroffen werden. Es muss jedoch auch Raum für Betriebsvereinbarungen und Einwilligungen als unmittelbares, gestalterisches Mittel von spezifischen Gegebenheiten vor Ort bleiben, wobei das aktuell bestehende Schutzniveau nicht unterschritten werden darf.

XXV. Datenschutz und „Internet der Dinge“

Mit der flächendeckenden Einführung des Internetprotokolls IPv6 wird die bisher vorhandene Beschränkung von IP-Adressen auf 4,3 Milliarden Adressen aufgehoben. Zukünftig stehen 340 Sextillionen Adressen allen Nutzern im Internet zur Verfügung. Schon heute zeichnet sich ab, dass sich hierdurch ein „Internet der Dinge“ oder auch „Smart Life“ entwickeln kann. Immer mehr elektronische Geräte (z. B. Garagen, Kühlschränke, Autos etc.) können über lokale oder auch überregionale Netzwerke verbunden und so elektronisch gesteuert werden. Diese technologische Weiterentwicklung stellt auch besondere Anforderungen an den Datenschutz, da für das Internet der Dinge insbesondere personenbezogene Verbrauchs- und Gewohnheitsdaten von besonderer Bedeutung sind. Die Enquete-Kommission regt daher an, bereits zu Beginn der Einführung von Smart Life-Anwendungen durch die Anbieter für eine Vertrauenskultur beim Nutzer zu werben. Dies setzt zunächst voraus, dass datenschutzrechtliche Grundsätze auch hier beachtet werden.

XXVI. Geodaten und Geolocating

Geodaten werden sowohl von öffentlichen Stellen (im Rahmen von INSPIRE) als auch von nicht-öffentlichen Stellen (z. B. Google Street View und Microsoft Streetside) erhoben und zum Teil im Internet der Öffentlichkeit zur Verfügung gestellt. Dabei ist zu beachten, dass Geodaten alleine keine personenbezogenen Daten sind. Durch ihre Personenbeziehbarkeit und die Möglichkeit, sie mit personenbezogenen Daten zu verknüpfen, können sie jedoch datenschutzrechtlich relevant werden. Zudem sind sie aufgrund ihrer zunehmenden Detailschärfe und vielseitigen Einsetzbarkeit eine beliebte, zumeist kostenlose, Informationsquelle, die sowohl von Unternehmen als auch von Privatpersonen genutzt und in bestehende Angebote integriert wird.

Durch die gestiegene Verbreitung der Geodatendienste haben sich vielfältige Abgrenzungsfragen der Personenbeziehbarkeit von Daten, aber auch zu weiteren Folgeproblemen, wie z. B. der nicht einvernehmlichen Löschung von Geodaten zu speziellen Objekten ergeben. Die Enquete-Kommission empfiehlt daher dem Deutschen Bundestag diese Problematik in seine Überlegungen über gesetzliche Änderungen des BDSG mit einzubeziehen.

Geolokalisationsdienste zeichnen sich demgegenüber dadurch aus, dass Daten über die Position des Nutzers von mobilen Geräten übertragen werden. Eine Auswertung dieser Daten erlaubt die Erstellung von umfassenden Bewegungsprofilen. Nach dem geltenden Recht sind solche Dienste nur mit Einwilligung des Nutzers zulässig (vgl. § 4a BDSG). Die Enquete-Kommission empfiehlt dem Deutschen Bundestag an dieser Regelung weiter festzuhalten und durch einen stringenten Vollzug der gesetzlichen Vorgaben sicherzustellen, dass die Nutzer vor einer Erhebung von personenbezogenen Daten hierüber auch umfassend informiert wurden. Dies gilt insbesondere für den Fall, dass die Daten nicht lediglich zur technischen Durchführung des Dienstes anfallen, sondern darüber hinaus genutzt werden sollen.

Berlin, den 30.06.2011