Deutscher Bundestag
Enquete-Kommission
Internet und digitale Gesellschaft
Ausschussdrucksache
17(24)034
TOP 1c am 4.7.2011
30.6.2011

Projektgruppe Datenschutz und Persönlichkeitsrechte

Endgültig abgestimmte gemeinsame Vorschläge für das Kapitel 3 – Handlungsempfehlungen - der Fraktionen der SPD, Bündnis 90/die Grünen und der Linken

I. Hintergrund und Ausgangslage

Maßgeblicher Ausgangspunkt für die Notwendigkeit datenschutzrechtlicher Reformen waren und sind die tiefgreifenden Veränderungen der Informations- und Kommunikationstechnologien und die damit einhergehenden Veränderungen der Angebote und Dienste, des Nutzungsverhaltens und insbesondere des Verhaltens der datenverarbeitenden Stellen. Die letzte größere Reform des Datenschutzrechts erfolgte Ende der 90er Jahre zu einer Zeit, als beispielsweise das Internet sich noch in einer ersten Aufbruchsphase befand, andere Anwendungen und Technologien zur Anwendung kamen und es bei Weitem nicht die heutigen Nutzerzahlen aufwies. Grundlegende und nach wie vor geltende Regelungselemente des Datenschutzrechts basieren auf der Vorstellung der Großrechnertechnologie und der Rechenzentren der 70er Jahre.

Mittlerweile hat sich eine wesentlich veränderte Informations- und Kommunikationsgesellschaft herausgebildet. Das weltweite Internet ist zur zentralen Kommunikationsinfrastruktur moderner Nationalstaaten aufgerückt. Zu den prägenden Entwicklungen auf der technischen Seite wie auch auf der Seite der Anwender zählen etwa – unter stetiger Reduktion der Kosten - weiter ansteigende Rechnerkapazitäten, Miniaturisierung, verbesserte Chip- und Mikroprozessortechnologien, die Ausweitung der Netztechnologie, Profiling-Technologien sowie die mobilen Anwendungen. Die heute zentralen Angebote des Internet, welche unter dem Schlagwort Web 2.0 zusammengefasst werden, sind durch interaktive Dienste gekennzeichnet. Damit gewinnen der „User“ und sein Verhalten, vor allem seine eigene Datenverarbeitungspraxis, an Bedeutung.

Geprägt werden das Internet wie auch der Mobilfunkmarkt zudem durch oligopolistische Strukturen, sodass einige wenige Unternehmen maßgeblichen Einfluss auf zentrale Entwicklungen ausüben. Die Verarbeitung von Daten und Informationen insbesondere zum Zweck der personalisierten Werbeansprache strukturiert die Geschäftskonzepte der größten Webunternehmen. Quantität wie auch Qualität der Datensammlungen in den Händen privater Stellen haben in den vergangenen Jahren exponentiell zugenommen und sind u. a. auch für staatliche Stellen von weiter wachsendem Interesse. Das belegen die Debatten um die Einführung verpflichtender Speicherungen von Telekommunikationsverkehrsdaten, von Finanztransaktionsdaten wie auch von Flugpassagierdaten.

In wichtigen gesellschaftlichen Bereichen wie dem Internet, der Telekommunikation, bei Mobilität und Verkehr, den öffentlichen Räumen des täglichen Lebens oder bei Finanz- und Geldgeschäften hat die Digitalisierung dazu geführt, dass das Verhalten von Bürgern registriert, gespeichert und zumindest nachträglich für zunehmend länger zurückliegende Zeiträume nachvollzogen werden kann. Zudem steht die Gesellschaft erst heute, allerdings

nun tatsächlich vor dem Eintritt in das bereits 2000 im damaligen Modernisierungsgutachten[1] etwas vorschnell prognostizierte Ubiquitous Computing, die sogenannte allgegenwärtige Datenverarbeitung. Darauf deuten zunehmend geodatengestützte Anwendungen, erste marktgängige Nutzungen von RFID-Chips, die weit verbreitete Videoüberwachung, die Telematik im Automobilsektor oder auch das in Zukunft realisierte Smart Grid/ Metering im Energiesektor hin. Damit steht der Datenschutz heute vor der Situation, dass ganze Infrastrukturen erfassbar und auswertbar werden. Eine verkürzte, allein auf die Vorstellung eines eigentumsanalogen Verfügungsrechts verengte Schutzperspektive wird dieser veränderten Risikolage nicht gerecht. Umfang und Qualität der Datenverarbeitung haben vielmehr massive, auch gesamtgesellschaftliche Auswirkungen. Die damit verbunden überindividuellen Risiken etwa des Missbrauchs von Daten, des damit verbundenen breiten Vertrauensverlustes bei Nutzern sowie der möglichen Vermeidung der Nutzung ganzer Kommunikations-Infrastrukturen sind konzeptionell bislang nicht hinreichend berücksichtigt.

Der Reformstau im Bereich des Datenschutzes ist weitgehend unbestritten. Die Modernisierung des Datenschutzes führte bereits1998 zur Befassung des Deutschen Juristentages, der weitreichende Änderungsvorschläge unterbreitete. Die damalige Bundesregierung beabsichtigte eine zweistufige und grundlegend ansetzende Reform. Realisiert wurde lediglich die erste Stufe in Gestalt der Umsetzung der dringlichsten Anforderungen der EG-Datenschutzrichtlinie 95/46. Der durch ein umfangreiches wissenschaftliches Gutachten[2] vorbereitete zweite Reformschritt konnte nicht mehr verwirklicht werden. Seit 2009 hat auch die Europäische Kommission die Reform der Datenschutzrichtlinie angekündigt, Konsultationen in den Mitgliedstaaten durchgeführt sowie Ende 2010 erste Eckpunkte einer Reform vorgelegt, die neben dem Bereich der Privatwirtschaft auch eine Harmonisierung der staatlichen Datenverarbeitung, insbesondere bei den Polizei- und Justizbehörden der Mitgliedstaaten, herbeiführen soll.

Die gesellschaftliche Reaktion auf die genannten Veränderungen fallen in Deutschland recht deutlich aus. In Umfragen wünscht sich eine deutliche Mehrheit der Bundesbürger einen verbesserten Schutz ihrer Daten. Die Ausweitung des Internethandels gilt durch Vertrauensdefizite in der Bevölkerung zumindest als belastet. Denn viele Bürger fürchten sich vor dem Missbrauch ihrer personenbezogenen Daten, besonders bei der Nutzung des Internet. Anstrengungen beim Datenschutz hingegen können die Akzeptanz für neue Technologien erhöhen und das Vertrauen in deren Nutzung stärken.

Eine Gruppe von besonders internetaffinen Nutzern hat eine länderübergreifende „Postprivacy“-Debatte angestoßen, die den Wert des Datenschutzes im Internetzeitalter neu thematisiert. Kernaussage ist dabei die eher empiristische These vom Kontrollverlust von Daten im Internet. Weil es im Kontext des Internet faktisch nicht mehr möglich sei, im Wege

[1] Roßnagel, Alexander / Pfitzmann, Andreas / Garstka, Hansjürgen (2002): Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern.

[2] Roßnagel, Alexander / Pfitzmann, Andreas / Garstka, Hansjürgen (2002): Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern.

des Selbstschutzes eigene Daten vor der Weiterverarbeitung durch Dritte zu schützen, habe sich der Datenschutz überlebt und werde einer neuen Kultur der Transparenz weichen. Dem wird in der öffentlichen Debatte allerdings entgegengehalten, es handele sich um einen Fehlschluss, weil aus dem so beschriebenen Sein allein kein Soll ableitbar sei. Auch gilt die These vom Kontrollverlust schon deswegen als wenig zielführend, weil sie ein verkürztes Schutzprogramm des Datenschutzes beschreibt, bei dem aufgrund der Fehlvorstellung eines ausschließlich individuellen Verfügungsrechts primär Elemente des Selbstdatenschutzes dem Datenschutz zugerechnet werden. Allerdings besteht Datenschutz längst aus einer Vielzahl von weit darüber hinausgehenden Schutzvorkehrungen und Maßnahmen.

Die massive Zunahme der Verarbeitung personenbezogener Daten in einem zunehmend unübersichtlicheren Feld von Akteuren fordert vom Gesetzgeber eine konsequente Neuausrichtung des Regelungsfeldes. Der bestehende ordnungsrechtliche Regelungsansatz, wie er insbesondere im Bundesdatenschutzgesetz sowie dem Telemediengesetz und Telekommunikationsgesetz zum Ausdruck kommt, ist nicht grundsätzlich obsolet geworden. Ein allgemeiner Rückzug auf Selbstregulierungen, wie er zum Teil etwa mit Blick auf Fragen des Internetdatenschutzes vorgeschlagen wird, verfehlt jedoch die Vorgaben der verfassungsgerichtlichen Rechtsprechung zur mittelbaren Drittwirkung sowie den grundrechtlichen Schutzpflichten. Andererseits bedarf es einer sachgerechteren Beurteilung und Behandlung von Datenschutzfragen "vor Ort" bei den verarbeitenden Stellen selbst. Dem entspricht eher die Orientierung an Konzepten regulierter Selbstregulierung bzw. Ko-Regulierung. Es bedarf auch weiterhin klarer Vorgaben hinsichtlich der Zulässigkeit bestimmter Datenverarbeitungen, verbunden mit eben so deutlichen Regelungen zu den Konsequenzen von Verstößen. Die Durchsetzung dieser Regelungen muss durch ein unabhängiges und effizientes Aufsichtssystem gewährleistet sein. Nicht zuletzt das Bundesverfassungsgericht sieht dieses Ordnungssystem als maßgeblich an, weil der Umgang mit personenbezogenen Daten und Informationen zu einem großen Teil dem Schutzbereich insbesondere des Grundrechts auf informationelle Selbstbestimmung unterfällt.
Hinsichtlich der Zielsetzung des Datenschutzes ist bedeutsam, dass nicht eines, sondern eine Vielzahl unterschiedlicher Schutzerfordernisse unter diesem Begriff versammelt werden.

Daten und Informationen

Sachangemessene Regelungen bedürfen einer differenzierten begrifflichen Beschreibung. Die bisherige Einsetzung der Begriffe Daten und Informationen greift zu kurz. Daten sind Zeichen, die auf Datenträgern vergegenständlicht festgehalten werden und als Informationsgrundlagen dienen. Informationen selbst hingegen werden als Sinnelemente erst in bestimmten sozialen Verwendungszusammenhängen durch aktive Deutungsleistungen (sozialer Kontext) erzeugt und genutzt[3]. Mit der Unterscheidung wird die im Datenschutz durchaus bekannte „Kontextabhängigkeit“ für die Bewertung der mit Datenverarbeitungen verbundenen Risiken besser herausgearbeitet. In der Folge wird es möglich, zusätzliche Anknüpfungspunkte für präzisere Schutzmaßnahmen zu formulieren. Zukünftig sollte die

[3] zum Gesamtkonzept vgl. M. Albers

Unterscheidung von Daten und Informationen deshalb vom Gesetzgeber besser herausgearbeitet werden.

Anwendungsbereich/Personenbezug

Bei der Reform des Datenschutzes ist zu berücksichtigen, dass der grundlegende Ansatz des Datenschutzrechts, nämlich die Personenbezogenheit eines Datums, in der digitalen Welt weiterentwickelt werden muss. Zwar ist auch im Internet nicht jedes Datum personenbezogen, doch grundsätzlich sind alle Daten personenbeziehbar. Es gibt kein belangloses Datum mehr. Denn durch die Verknüpfung mit anderen Daten kann ein Personenbezug jederzeit hergestellt werden. Das bedeutet vor allem, dass Daten nicht von vornherein aus dem Schutz herausfallen dürfen. Es kommt mehr denn je darauf an, einen abgestuften gefährdungsabhängigen Schutz zu entwickeln, damit der Anwendungsbereich nicht beliebig weit geöffnet und damit konturlos wird.

Die technischen Möglichkeiten der Verkettung verschiedener Datensätze waren nie so ausgereift wie heute. Dem muss die zukünftige gesetzgeberische Gestaltung Rechnung tragen.

Abwehr- und Schutzkomponente

Datenschutz beinhaltet verfassungsrechtlich gesehen weit mehr als eine bloße Abwehr von Eingriffen in das Recht auf informationelle Selbstbestimmung. Die Schutzkomponenten betreffen nicht nur das Verhältnis zum Staat, sondern aufgrund konkreter Gefahren der personenbeziehbaren Datenverarbeitung auch den Bereich der Privatwirtschaft. Im Sinne der Gewährleistung einer freien Persönlichkeitsentfaltung der Bürgerinnen und Bürger beinhaltet die Schutzkomponente des Datenschutzes deshalb auch eine staatliche Verpflichtung, Maßnahmen zu treffen, die gewährleisten, dass die Daten des Einzelnen wirksam geschützt sind und dass er über die Verarbeitung dieser Daten informiert wird.

II. Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme/Grundrecht auf informationelle Selbstbestimmung

Angesichts der Bedeutung des Schutzes der personenbezogene Daten für nahezu alle Lebensbereiche und der wegweisenden Rechtsprechung des Bundesverfassungsgerichtes, insbesondere mit Blick auf die zukünftige technische Entwicklung, empfiehlt die Enquete-Kommission dem Deutschen Bundestag, zu prüfen,

1. ob die vom Bundesverfassungsgericht geschaffenen Grundrechte auf informationelle Selbstbestimmung sowie auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in den Grundrechtekatalog als eigenständig formulierte Grundrechte aufgenommen werden sollten.

2. ob es der Fortentwicklung des Post- und Fernmeldegeheimnisses hin zu einem übergreifenden Rechts auf Schutz des Kommunikationsgeheimnisses bedarf.

III. Grundprinzipien des Datenschutzrechts/Änderungsbedarf BDSG (Modernisierung, Vereinfachung, Sprache)

Die Grundprinzipien des deutschen Datenschutzes wurden in Kapitel 2.1 durch die Enquete-Kommission dargestellt. Wie die Enquete-Kommission in ihrer Beschreibung jedoch feststellt, werden diese Prinzipien in vielen Konstellationen nicht beachtet bzw. nachrangig zu anderen Interessen gestellt.
Die Enquete-Kommission gibt deshalb dem Deutschen Bundestag nachfolgende Handlungsempfehlungen:

Die Enquete-Kommission empfiehlt,

1. die ins Stocken gekommene Modernisierung des unübersichtlichen Datenschutzrechtes fortzusetzen. Das Ziel der Modernisierung muss eine deutliche Vereinfachung und Integration datenschutzrechtlicher Bestimmungen sein, wobei das bestehende Schutzniveau nicht abgesenkt werden darf. Dieses Ziel wird nur dann verwirklicht werden können, wenn das bestehende Datenschutzrecht um neue Datenschutzinstrumente ergänzt wird. Hierbei wird der Implementierung eines Datenschutzes durch Technik große Bedeutung zukommen.

2. zu überprüfen, inwieweit es einer Weiterentwicklung der Grundbegriffe und der bestehenden Dogmatik des Datenschutzrechts bedarf, insbesondere im Hinblick auf eine bessere Abgrenzung der Begriffe Daten, Informationen und Wissenskontext sowie der sich daraus ergebenden Konsequenzen. Dies ist geboten, weil ein allein auf Daten bezogenes und individualistisches Verständnis des Datenschutzrechts unsachgerecht schutzverkürzend wirken kann.

3. ein allgemeines, nicht subsidiäres Gesetz für einen modernen Datenschutz zu erarbeiten, das unter Vermeidung von Doppelregelungen eine klare Abgrenzung zwischen allgemeinen und bereichsspezifischen Regelungen erlaubt. Wenn möglich, soll es zu einem Verzicht, jedenfalls zu einer Reduzierung bereichsspezifischer Regelungen führen. Das Gesetz soll darüber hinaus auch allgemeine Regelungen zur Technikgestaltung, zur Datensicherung, zur Datenschutzorganisation, zur Datenschutzkontrolle und zur Selbstregulierung enthalten und weitaus stärker auf die bereits im Gesetz verankerten Grundprinzipien Datensparsamkeit und Datenvermeidung setzen.

4. bei der Erarbeitung eines allgemeinen Datenschutzgesetzes die zur Verwirklichung der informationellen Selbstbestimmung wesentlichen Schutzziele, wie: Datensparsamkeit und Datenvermeidung, Datensicherheit, Zweckfestlegung und –bindung, Systemdatenschutz, Transparenz, Gestaltungsrechte (Auskunfts-, Widerspruchs-, Benachrichtigungs-, Korrektur- und Löschungsrechte), Nichtverkettbarkeit (als technische Sicherung der Zweckbindung) und

Intervenierbarkeit (als technische Gestaltung von Verfahren zur Ausübung der Betroffenenrechte)[4] als übergreifende Grundprinzipien voranzustellen.

5. dass die allgemeinen Datenschutzgrundsätze gleichermaßen für den öffentlichen und für den nicht öffentlichen Bereich gelten sollten.

6. den Zweckfestlegungs- bzw. Zweckbindungsgrundsatz in Verbindung mit dem Erforderlichkeitsgrundsatz durch eine eigene Norm hervorzuheben und zu konkretisieren. Dabei sollten auch Vorgaben für die Änderung bei Zweckfestlegung und Zweckbindung klar geregelt sein. In diesem Zusammenhang müssen Regelungen erarbeitet werden, nach denen es Nutzerinnen und Nutzern möglich ist, auch in der vernetzten Welt die Kontrolle über die Verwendung ihrer persönlichen Daten ausüben zu können.

7. zu prüfen, inwieweit Sanktionen bei Verstößen gegen den Zweckfestlegungs- bzw. Zweckbindungsgrundsatz eingeführt werden sollten. Den Aufsichtsbehörden muss ermöglicht werden, gegen Unternehmen, die nachgewiesenermaßen anlasslos oder zweckwidrig Daten erheben, speichern, verarbeiten und nutzen, wirkungsvolle Sanktionen zu verhängen. In diesem Zusammenhang ist die bereits im BDSG verankerte Löschungspflicht zu betonen. Ein Verwertungsverbot für Daten, die durch rechtswidrige Änderung des ursprünglichen Erhebungszwecks erlangt worden sind, sollte gesetzlich verankert werden. Regelungsbedarf besteht etwa im Hinblick auf die Verwertung von unrechtmäßig erlangten Daten in Gerichtsprozessen.

8. dass die Informationspflichten privater Anbieter gegenüber Nutzerinnen und Nutzern erweitert und die Auskunftsansprüche der Nutzerinnen und Nutzern gegenüber Anbietern gestärkt werden.

9. die Informationspflichten sowohl öffentlicher als auch nicht-öffentlicher Stellen gegenüber den Betroffenen bei Datenpannen zu erweitern.

10. dass, um Unsicherheiten bei der Festlegung der Verantwortlichkeit von vornherein zu vermeiden, die Formulierung „Daten verarbeitende (bzw. speichernde) Stelle“ dem Wortlaut der Europäischen Richtlinie angepasst wird („die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“). Darüber hinaus bedarf es einer gesetzlichen Klärung für die zunehmenden Konstellationen, bei denen eine Vielzahl von Beteiligten die Datenverarbeitung durchführen.

11. die Informationspflichten darüber hinaus wie folgt zu erweitern:

[4] Konferenz der Datenschutzbeauftragten des Bundes und der Länder „ Ein modernes Datenschutzrecht für das 21. Jahrhundert“

a. durch klare und eindeutige Offenlegung der Verantwortlichkeit für die Datenverarbeitung bei mehreren Stellen gegenüber den Betroffenen;

b. durch “prominente“ Platzierung der datenschutzrechtlich verantwortlichen Stelle und der zuständigen Datenschutzbehörde;

c. durch eine Verpflichtung der verantwortlichen Stelle, Herkunft und Empfänger von Daten zu dokumentieren sowie Datenbankzugriffe zu protokollieren, wenn personenbezogene Daten an Dritte weitergegeben werden;

d. durch eine gesetzliche Festschreibung zur Vermeidung von Medienbrüchen bei der Ausübung des Widerspruchsrechts. Die Ausübung des Widerspruchsrechts wird von den Anbietern bisweilen absichtlich erschwert. Häufig lassen sie einen Widerspruch gegen die Datenerhebung nur schriftlich zu, während die Einwilligung in die Erhebung durchaus auf elektronischem Wege erteilt werden kann.

12. das sogenannte „Kopplungsverbot“ auch auf–solche Unternehmen und Dienste auszuweiten, die keine marktbeherrschende Stellung haben. Nach geltender Rechtslage darf der Abschluss eines Vertrages (etwa bei der Nutzung von Internetdiensten) nicht an eine Einwilligung gekoppelt werden, die eine über die Diensterbringung hinausgehende Datenerhebung und –nutzung erlaubt. Dies gilt allerdings nur für solche Unternehmen, die eine marktbeherrschende Stellung innehaben.

13. eine Befassung des Deutschen Bundestages über die Ausübung und Stärkung von Betroffenenrechten im Bundesdatenschutzgesetz (vgl. §§ 33 ff. BDSG). Dabei sollte dem Einsatz moderner Technologien (etwa dem Recht auf elektronische Auskunft über die gespeicherten Daten und einem elektronischen Widerspruchsrecht) besondere Bedeutung zukommen. Die Auskunftsrechte der Betroffenen sind zu vereinfachen und bürgerfreundlicher auszugestalten,

a. durch entsprechende Bereitstellung technischer Mittel, die die Wahrnehmung der Rechte vereinfachen;

b. durch eine allgemeine Einführung eines Rechts auf elektronische Auskunft, u. a. auch im Hinblick auf die Verknüpfung bzw. Zusammenführung von Daten sowie die über den eigentlichen Zweck der Erhebung hinausgehende Nutzung;

c. durch eine Verpflichtung der Anbieter, Nutzer über Änderungen der für das betreffende Angebot geltenden Datenschutzbedingungen effektiv zu informieren.

14. Konzepte wie den vom Chaos Computer Club (CCC) vorgeschlagenen „Datenbrief“, der Unternehmen verpflichtet, in regelmäßigen Abständen Bürgerinnen und Bürger über ihre bei den Unternehmen gespeicherten persönlichen Daten zu unterrichten, in die Überlegungen für eine Stärkung der informationellen Selbstbestimmungsrechte einzubeziehen. Der Datenbrief ist kritisch zu bewerten, wenn und soweit damit eine eigene Sammlung und Zusammenführung von Daten zu Personen verbunden ist und ein nicht zu bewältigender Aufwand für die betroffenen Unternehmen droht. Diesen Problemen muss in der Ausgestaltung eines Konzeptes wie des Datenbriefs Rechnung getragen werden.

15. dass das Auskunftsrecht sich auch auf Datenverkettungen beziehen sollte. Welche persönlichen Daten bei einem bestimmten Anbieter mit anderen verknüpft werden und nach welchen Selektionskriterien dies geschieht, kann der datenschutzbewusste Nutzer derzeit nicht in Erfahrung bringen.

16. sicherzustellen, dass Betroffene, deren personenbezogene Daten an Dritte übermittelt werden, über den tatsächlichen Empfänger ihrer Daten informiert werden müssen. Wenn personenbezogene Daten an Dritte übermittelt werden, muss der Betroffene bislang lediglich über die „Kategorien von Empfängern“ unterrichtet werden. Er erfährt jedoch nicht, wer seine Daten tatsächlich bekommen hat. Dieser Missstand wäre mit einer schlichten Formulierungsänderung im Gesetz leicht zu beheben. Verstöße gegen diese Regelung könnten zudem mit einem Bußgeld belegt werden.

17. die Formulierung einer einheitlichen allgemeinen technikunabhängigen Vorschrift zur transparenten Datenerhebung, -verarbeitung und –nutzung, die u. a. folgende Punkte regelt:

a. grundsätzliches Verbot der unbemerkten Datenerhebung mit Sanktionen im Falle des Verstoßes;

b. Informationspflicht gegenüber den Betroffenen über Funktionsweise und Art der Datenerhebung, Identität der verantwortlichen Stelle, Rechte der Betroffenen und einer Datenschutzerklärung.

18. die Schaffung einer allgemeinen, technikunabhängigen Regelung zur Verarbeitung personenbezogener Lokalisierungsdaten unter Verpflichtung der Lokalisierungsdienstanbieter, die konkrete Ortung des Betroffenen durch ein Signal anzuzeigen, sowie innerhalb von Trackings-Systemen, die Einwilligung des Betroffenen vorzusehen. Der europäischen Datenschutzrichtlinie für die elektronische Kommunikation 2002/58/EG zufolge ist für die Verarbeitung von Positionsdaten aus GSM/UMTS (Handys), bei denen es sich stets um Tracking-Systeme handelt, ausdrücklich eine Einwilligung des Betroffenen erforderlich. Bislang ist diese Vorgabe der Richtlinie jedoch nicht in das Bundesdatenschutzgesetz aufgenommen worden. Das Gesetz ist in diesem Punkt deshalb bislang nicht europarechtskonform. Bei der

Ausgestaltung ist auf Technikneutralität zu achten. Ferner muss es Betroffenen ermöglicht werden, im Rahmen der technischen Möglichkeiten eine Ortung der eigenen Person zu verhindern. Positionsdaten sollten in die Kategorie der besonders schützenswerten („sensitiven“) Daten ins BDSG aufgenommen werden.

19. für die Betroffenen eine Anspruchsnorm mit Sanktionierung bei Nichtbeachtung zu schaffen, die die verantwortliche Stelle dazu verpflichtet, ihre Systeme und Verfahren so auszurichten, dass nur Daten erhoben werden, die auch erforderlich sind.

20. entsprechend der europäischen Datenschutzrichtlinien gleiche Regeln für öffentliche und nicht-öffentliche Stellen zu schaffen und dabei verbindliche datenschutzrechtliche Mindeststandards festzuschreiben. Dies begründet sich in dem als zunehmend problematisch erscheinenden Umgang mit öffentlich zugänglichen personenbezogenen Daten. Darf beispielsweise die Polizei Daten über Demonstrationsteilnehmer in sozialen Netzwerken recherchieren und unbeschränkt miteinander verknüpfen? Personenbezogene Daten, welche aus „allgemein zugänglichen Quellen“ stammen oder vom Betroffenen „zur Veröffentlichung vorgesehen“ sind, dürfen nach derzeitiger Rechtslage erhoben werden. Aufgrund der besonderen Gefahren, die die Erhebung solcher Daten allein schon durch die Möglichkeit der nachfolgenden Verkettung mit sich bringt, erscheint dies unbefriedigend. Die Privilegierung öffentlich zugänglicher Daten sollte auf solche Verwendungen eingeschränkt werden, die im offensichtlichen oder erklärten Interesse des Betroffenen liegen bzw. diesem nicht widersprechen.
Die Unterscheidung zwischen öffentlichen und nicht-öffentlichen Regeln im Datenschutz ist nicht mehr zeitgemäß. Zur Einhaltung datenschutzrechtlicher Mindeststandards für den öffentlichen und nicht-öffentlichen Bereich sollten effektive und abschreckende Sanktionen festgelegt werden. Hilfreich wäre hier eine umfassende verschuldensunabhängige Haftung öffentlicher wie nicht-öffentlicher Stellen, etwa durch pauschalisierten Schadensersatz. Hierdurch könnte insbesondere die Problematik der Bezifferbarkeit des Schadens gelöst werden. Auch würde der Ersatz von immateriellen Schäden dadurch erleichtert. Ebenfalls angebracht scheint eine Erweiterung der Bußgeldtatbestände, insbesondere für unbefugte Datennutzung und unzulässige Beobachtung (Videoüberwachung).

IV. Anonymität und Pseudonymität

Die Enquete-Kommission hat in ihrer Bestandsaufnahme festgestellt, dass auch eine anonyme und pseudonyme Nutzung des Internets zur Ausübung des Rechts auf informationelle Selbstbestimmung gehören kann.

Deshalb empfiehlt die Enquete-Kommission dem Deutschen Bundestag,

1. durch gesetzgeberische Maßnahmen zur Stärkung der Möglichkeit der anonymen Nutzung elektronischer Medien den Datenschutz zu verbessern.

2. die allgemeine gesetzliche Verpflichtung, die die Dienstleister verpflichtet, anonyme und pseudonyme Nutzungsmöglichkeiten von Internetdiensten anzubieten, weiter zu stärken. Verstöße gegen die Möglichkeit und Wahrung von Pseudonymität und Anonymität sollten ferner sanktioniert werden können.

V. Technischer Datenschutz

Die Enquete-Kommission hat in ihrer Beschreibung festgestellt, dass die aktuellen Rechtsnormen oft nicht mehr geeignet sind, Datensicherheit und Datenschutz zu gewährleisten, weil sie nicht mehr zeitgemäß und nicht technikneutral formuliert sind. Die Enquete-Kommission hat auch festgehalten, dass eine technikneutrale Formulierung z. B. anhand von Schutzzielen – wie dies die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt – geeignet sein kann, gesetzliche Normen trotz der ständigen technischen Weiterentwicklung beständiger zu gestalten.

Die Enquete-Kommission empfiehlt deshalb dem Deutschen Bundestag:

1. die technischen und organisatorischen Maßnahmen (i. S. d. Anlage zu § 9 BDSG) zu reformieren, indem die Definitionen der elementaren Schutzziele aufgenommen werden, so dass sich daraus einfache, flexible und praxistaugliche Maßnahmen ableiten lassen.

2. Bei der Definition der Schutzziele sollten folgende Punkte beachtet werden:

   a. Die Schutzziele sollten einfach, verständlich, praxistauglich und technologieunabhängig formuliert sein.

   b. Maßgabe bei der Definition sollten in erster Linie die Vorgaben des Datenschutzes sein, nicht Vorgaben zur IT-Sicherheit.

   c. Die Umsetzung muss frühzeitig ansetzen und durch entsprechende Maßnahmen (wie etwa Risikoanalysen und Sicherheitskonzepte, die vor Freigabe des Verfahrens vorgelegt und fortgeschrieben werden müssen) abgesichert werden.

VI. Datenschutz für Kinder und Jugendliche

Die Enquete-Kommission stellt fest, dass es verschiedene schutzwürdige Gruppen im Bereich des Datenschutzes gibt. Dabei ist besonders die Gruppe der Kinder und Jugendlichen hervorzuheben, weil sie aufgrund ihrer (noch) nicht ausreichenden Einsichtsfähigkeit in der digitalen Informationsgesellschaft besonders schutzwürdig sind.

Die Enquete-Kommission empfiehlt deshalb dem Deutschen Bundestag,

1. mit klaren gesetzlichen Regelungen festzulegen, ab wann und unter welchen Voraussetzungen Minderjährige eigenständig einwilligen und ihre Betroffenenrechte wahrnehmen können.

2. allgemein gesetzlich festzulegen, dass bei Angeboten für Kinder und Jugendliche die Erhebung von personenbezogene Daten auf das erforderliche Mindestmaß für die Dienstleistung beschränkt bleiben muss. Zuwiderhandlungen bzw. Verstöße müssen besonders stark sanktioniert werden.

3. zu prüfen, inwieweit darüber hinaus spezielle Datenschutzregelungen für Kinder und Jugendliche getroffen werden müssen, z. B. im Hinblick auf den Bereich der sozialen Netzwerke oder bei Kaufangeboten~~,~~ wie Online-Spielen, Klingeltönen etc.

4. Anbieter von Online-Diensten, die von Kindern und Jugendlichen genutzt werden, dazu zu verpflichten, die Hinweise zum Datenschutz so verständlich zu machen, dass Kinder und Jugendliche diese auch verstehen. So könnten beispielsweise die AGB~~s~~ und die Datenschutzerklärungen neben den juristisch verbindlichen Textversionen in leicht verständlichen Versionen angeboten werden.

5. auf die Einführung eines allgemein gültigen Datenschutzgütesiegels hinzuwirken, speziell zur Orientierung für Kinder und Jugendliche, wie es der Bundesbeauftragte für den Datenschutz bereits gefordert hat. Dies könnte z. B. durch die Stiftung Datenschutz vergeben werden.

6. sich für eine Stärkung der Medienkompetenz durch Bildungsangebote, etwa der Stiftung Datenschutz, einzusetzen. Es ist notwendig, das Bewusstsein für den Schutz eigener und fremder Daten bei Kindern und Jugendlichen zu entwickeln und zu fördern.

7. Anbieter von Internetdiensten zu verpflichten, etwaig~~e~~ erstellte Persönlichkeitsprofile zu löschen und die über die Kinder bekannten Informationen umgehend zu anonymisieren, sobald diesen Anbietern das Alter eines minderjährigen Kindes bekannt wird.

8. Anbietern von Internetdiensten die Weitergabe und den Weiterverkauf von Daten von Kindern und Jugendlichen und Profilen von minderjährigen Nutzerinnen und Nutzern zu untersagen.

9. die Erhebung und Erstellung von Persönlichkeits-, Konsum- und Vorliebenprofilen von minderjährigen Nutzerinnen und Nutzern grundsätzlich zu untersagen.

Hinsichtlich weiterer entsprechender Handlungsempfehlungen wird auf die Projektgruppe Medienkompetenz der Enquete-Kommission verwiesen.

VII. Profilbildung

Die Enquete-Kommission stellt in ihrem Bericht fest, dass die Zusammenführung und Verknüpfung personenbezogener Daten zu Profilen (wie z. B. durch das sogenannte Behavioral Targeting) eine besondere Gefahr für das Persönlichkeitsrecht darstellen kann. Durch solche Techniken können das Verhalten, die Interessen und die Gewohnheiten eines Menschen vorhersehbar gemacht werden, was nicht zuletzt eine gezielte Manipulation ermöglicht, unabhängig davon, ob dies zu Werbe- oder sonstigen Zwecken erfolgt.

Aufgrund des Gefährdungspotentials empfiehlt die Enquete-Kommission dem Deutschen Bundestag,

1. die Schaffung einer gesetzlichen Definition der Profilbildung und deren grundsätzliches, gesetzlich verankertes Verbot mit einem allgemeinen Ermächtigungsvorbehalt sowie die Schaffung von gesetzlichen Ausnahmen, die nur zulässig sind, wenn sie dem besonderen Gefährdungspotential Rechnung tragen und/oder durch freiwillige, aktive und informierte Einwilligung der Betroffenen legitimiert sind. Diese Einwilligung setzt eine umfassende Information über Umfang und Herkunft der verwandten Daten, Zweck und Verwendung des Profils, die verantwortliche Stelle und die vorgesehene Löschungsfrist voraus. Die Einwilligung muss freiwillig und jederzeit widerrufbar sein. Der Widerruf muss die sofortige Löschung des Profils zur Folge haben, auch bei den Stellen, an die es übermittelt worden ist.

2. angesichts des umfassenden und weit verbreiteten Einsatzes von Instrumenten zum Zwecke des Behavioural Targeting, Initiativen, die eine anbieterunabhängige, aktive Information der Öffentlichkeit über Funktionsweisen, eingesetzte Techniken, mögliche Schutzmechanismen sowie die derzeitigen rechtlichen Regelungen zu unterstützen.

3. die Webseiten-Betreiber ebenso wie Werbewirtschaftsunternehmen zu verpflichten, - verständlich und leicht einsehbar - Informationen über die konkret eingesetzten Analyse-Techniken und die Möglichkeit einer begrenzten Einwilligung aufzuzeigen.

VIII. Veröffentlichung von Daten im Internet

Mit der Verbreitung von sog. Web 2.0 Anwendungen wird die Veröffentlichung von personenbeziehbaren Informationen insbesondere durch andere Privatpersonen im Rahmen der Nutzung z.B. von sozialen Netzwerken möglich. Mit dem Wegfall technischer Grenzen der Publizierbarkeit häufen sich Konflikte um Veröffentlichungen die gegen Persönlichkeitsrechte verstoßen können oder von den Betroffenen aus anderen Gründen abgelehnt werden.
Die Enquete-Kommission empfiehlt dem Deutschen Bundestag:

zu prüfen, ob durch ein allgemeines, auch gegenüber den Internetanbietern geltend zu machendes Widerspruchsrecht gegen personenbezogene Internetveröffentlichungen

eine wesentliche Verbesserung des Persönlichkeitsrechts der Betroffenen bewirkt werden kann.

IX. Cloud Computing

Die Enquete-Kommission stellt fest, dass das Cloud Computing zukünftig eine große Herausforderung für den Datenschutz darstellt. Deshalb ist es unerlässlich, dass sich die Bundesregierung auf internationaler und europäischer Ebene dafür einsetzt, Vereinbarungen und Standards zu erreichen, die einem hohen – möglichst deutschen bzw. europäischen Schutzniveau entsprechen.

Darüber hinaus empfiehlt die Enquete-Kommission dem Deutschen Bundestag,

1. gesetzliche Regelungen zu schaffen, die datenschutzrechtliche Mindeststandards dafür festlegen, unter welchen Umständen personenbezogene bzw. personenbeziehbare Daten ausgelagert werden dürfen. Die Nichteinhaltung dieser Mindeststandards muss sanktioniert werden,

2. weitere gesetzliche Regelungen zu schaffen, die Verantwortlichkeiten und entsprechende Dokumentationspflichten über die Auslagerung bzw. Weitergabe von Daten klar regeln,

3. die Anbieter von Clouds dazu zu verpflichten, Art und Ort der Datenverarbeitung offenzulegen sowie Angaben zu den Sicherungsmaßnahmen zu machen,

4. eine Möglichkeit zum Schutz in der gesetzlichen Festlegung zu schaffen, dass personenbezogene Daten nur auf deutschen und/oder europäischen Servern gespeichert werden dürfen, bei denen ein entsprechendes Datenschutzniveau sichergestellt ist.

X. Regulierte Selbstregulierung und Auditierung

Die Enquete-Kommission stellt fest, dass eine Selbstregulierung im Datenschutz eine wertvolle Ergänzung zu den gesetzlichen Regelungen darstellen kann, weil sie den gerade für den Internet-Bereich wichtigen Vorzug der Flexibilität und Anpassung an neue Gegebenheiten besitzt. Ein hohes Schutzniveau wird jedoch nur erreichbar sein, wenn die Selbstregulierung in einen gesetzlichen Rahmen eingebunden ist, es sich also der Sache nach um eine Ko-Regulierung handelt. Ein Beispiel bietet § 38 a Bundesdatenschutzgesetz, der aber bislang mangels Akzeptanz in der Privatwirtschaft noch nicht die beabsichtigte Wirkung entfalten konnte. Reine Selbstregulierungen bleiben sinnvoll und notwendig, wenn es sich unterhalb der gesetzlichen Regelungsziele um freiwillige zusätzliche Bemühungen der Industrie handelt.

Die Enquete-Kommission stellt darüber hinaus fest, dass Datenschutzaudits und Datenschutzgütesiegel ein wesentliches Instrument zur Vertrauensbildung im gegenseitigen Verhältnis von Bürgern, Unternehmen und Staat darstellen können.

Die Enquete-Kommission empfiehlt deshalb dem Deutschen Bundestag,

1. zu prüfen, wie die Integration von selbstregulativen Elementen in das Konzept des BDSG verbessert werden kann, ohne das Schutzniveau zu senken. Begründet wird diese Forderung damit, dass mit § 38 a Bundesdatenschutzgesetz zwar eine Norm mit explizit selbstregulativen Elementen existiert, die zwar im Grundsatz sowohl von den Unternehmen als auch von den Datenschutzbeauftragten begrüßt, jedoch in der Praxis kaum angewandt wird. Es wird vermutet, dass das an den nicht hinreichend konkret ausgestalteten Verfahren liegt.

2. ein Datenschutzauditgesetz gem. § 9 a BDSG zu verabschieden, welches den Unternehmen die Möglichkeit eines Audits auf freiwilliger Basis bietet und dessen Verfahren unbürokratisch, aber verbindlich ausgestaltet sein muss.

3. im Rahmen von Vergabegesetzen eine Verpflichtung öffentlicher Stellen zu verankern, solche auditierten bzw. zertifizierten Produkte bevorzugt einzusetzen. Soweit keine Vergabegesetze bestehen, ist im Rahmen der Ausschreibungen zu berücksichtigen, dass datenschutzrechtlich fortschrittliche Produkte bevorzugt eingekauft und/oder genutzt werden.

XI. Stiftung Datenschutz

Die Enquete-Kommission stellt fest, dass die geplante Stiftung Datenschutz, wenn die richtigen Vorgaben für die inhaltliche Ausgestaltung gefunden werden, als wirkungsvolle Plattform vorhandene Angebote zusammenführen und so ihrem geplanten Auftrag für Aufklärung und Information gerecht werden kann. Sie begrüßt daher im Grundsatz die von der Bundesregierung auf den Weg gebrachte Stiftung Datenschutz. Diese Stiftung kann u. a. Kriterien für die Zertifizierung von Diensten sowie für ein einheitliches Gütesiegel aufstellen und damit mehr Transparenz für Unternehmen und Bürger erwirken. 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. Neben der Festlegung von Kriterien nimmt sie die Vergabe von Gütesiegeln nach einem gesetzlich geregelten Verfahren vor.

Bei der Einrichtung der Stiftung Datenschutz ist darauf zu achten, dass vergleichende Tests nach verschiedenen Kriterien, unter Einschluss des Datenschutzes, auch bereits etwa durch die Stiftung Warentest durchgeführt werden, für Güter, Produkte und Dienstleistungen, die sich explizit an Endverbraucher richten. Eine klare Zuordnung der Zuständigkeit in diesem Bereich ist deshalb in der Satzung zu verankern. Eine Überschneidung der Zuständigkeiten

zwischen den beiden Stiftungen sollte vermieden werden. Vielmehr sollen diese sich in ihren Angeboten ergänzen.
Weitere Aufgaben können die Stärkung des Selbstdatenschutzes sowie Aufklärung und Bildung im Datenschutz sein.

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

1. Die Stiftung ist wirtschaftlich und organisatorisch, also finanziell und personell, unabhängig von den zu bewertenden Unternehmen zu organisieren. Personell ist darauf zu achten, dass bei der Besetzung der Gremien die zu prüfenden datenverarbeitenden Unternehmen zwar beteiligt werden, aber auf die Unabhängigkeit der Stiftung keinen Einfluss haben. Dies könnte z. B. durch die Einsetzung eines Beirats, der beratende Funktion hat, geschehen. Finanziell sollte die Bundesstiftung nicht allein vom Bundeshaushalt abhängig sein müssen. Bei der Annahme von Zuwendungen hat die Stiftung jedoch darauf zu achten, dass ihre Unabhängigkeit gewahrt bleibt.

2. In der Satzung ist das Verhältnis zu den Datenschutzbehörden zu klären. Es ist festzuhalten, dass diesen allein die Kontrolle über die Einhaltung der Gesetze obliegt und die Aufsichtstätigkeit nicht durch die Arbeit der Stiftung beeinflusst werden darf. Ebenso dürfen die von der Stiftung Datenschutz erteilten Audits und Gütesiegel keine rechtliche Bindungswirkung gegenüber den Datenschutzbehörden entfalten, d. h. die Aufsichtsbehörden müssen die entsprechenden Unternehmen dennoch anlassbezogen überprüfen dürfen.

3. Es ist in der Satzung zu regeln, wer die materiellen Standards für Zertifizierungsverfahren setzt. Dabei sind ein Höchstmaß an Transparenz sowie eine enge Kooperation mit den Datenschutzbehörden unabdingbar.

4. Die Vergabe von Audits kann durch die Stiftung Datenschutz aufgrund eines bundeseinheitlich gesetzlich festgelegten Auditierungsverfahrens erfolgen. Hierfür bedarf es eines Gesetzes i. S. v. § 9a BDSG. Dabei ist zu beachten, dass bereits existierende Audit-Verfahren (wie z. B. in Bremen oder Schleswig-Holstein) in die Ausgestaltung und Vergabe eingebunden werden.

5. Bei der Vergabe von Gütesiegeln durch die Stiftung ist darauf zu achten, dass ein einheitliches Gütesiegel entwickelt wird 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 (z. B. für 2 Jahre) zu erteilen und müssen turnusgemäß geprüft werden.

6. Im Bereich der Bildung darf die Stiftung Datenschutz nicht die Zuständigkeit der Länder verletzen. Die Länder sind deshalb mitentscheidend einzubeziehen. Schwerpunkt der Stiftungstätigkeit sollte deshalb die außerschulische Bildung sein.

7. Im Bereich der Aufklärung wird der Stiftung empfohlen, ein zentrales Infoportal oder ein virtuelles Datenschutzbüro (wie derzeit beim ULD Schleswig-Holstein praktiziert) zu schaffen.

8. Die Stiftung Datenschutz sollte perspektivisch auch im Bereich der Datenschutzforschung, insbesondere der Entwicklung und dem Ausbau von Instrumenten des technischen Datenschutzes, tätig werden. Mögliche Tätigkeitsfelder eröffnen sich sowohl im Bereich der Koordination der Forschungsmittelvergabe als auch für den Bereich eigener Forschungsanstrengungen.

XII. Schadensersatzansprüche

Im Ergebnis stellt die Enquete-Kommission fest, dass Handlungsbedarf im Bereich des Schadensersatzrechts besteht.

Die Enquete-Kommission empfiehlt deshalb dem Deutschen Bundestag,

1. bezugnehmend auf die Vorschläge der Konferenz des Bundes- und der Landesdatenschutzbeauftragten, eine Gefährdungshaftung auch gegenüber nicht-öffentlichen Stellen einzuführen.

2. einen pauschalierten Schadensersatzanspruch bei Datenschutzverstößen einzuführen, der die Problematik der Bezifferbarkeit des Schadens löst und des Ersatzes von immateriellen Schäden gegenüber allen datenverarbeitenden Stellen ermöglicht, unabhängig von nachweisbaren weiteren und höheren Schäden.

3. zu prüfen, ob nicht die Festlegung einer Mindest- und einer Höchstgrenze der Ersatzsumme erfolgen sollte.

XIII. Verbandsklage

Die Enquete-Kommission empfiehlt dem Deutschen Bundestag,

eine gesetzliche Regelung zu schaffen, die Verbraucherschutz- und Datenschutzverbänden eine „fremdnützige“ Klagebefugnis einräumt, ähnlich dem Instrument des Verbandsklagerechts. Eine solche Befugnis soll es den Verbänden ermöglichen, im Namen von Betroffenen und im Interesse der Allgemeinheit auch dann gegen Datenschutzverstöße vorzugehen, wenn die Betroffenen keine rechtlichen Schritte gegen den Rechtsverletzer einleiten.

XIV. Beschäftigtendatenschutz

Die Enquete-Kommission stellt fest, dass es im Bereich des Datenschutzes für Beschäftigte gesetzgeberischen Handlungsbedarf gibt. Hierbei sind insbesondere die Rechte der Beschäftigten bei Überwachung und Screening zu wahren. Darüber hinaus muss die datenschutzgerechte Ausgestaltung der gesetzlich vorgegebenen Verfahren zur Speicherung von personenbezogenen Daten, wie z. B. des elektronischen Entgeltnachweises ELENA, sichergestellt werden.

Die Enquete-Kommission empfiehlt deshalb dem Deutschen Bundestag, ein entsprechendes Gesetz unter Beachtung nachfolgender Kriterien zu beschließen:

1. Der Beschäftigtendatenschutz ist in einem eigenständigen Gesetz zu regeln. Die derzeit bestehenden Regelungen im BDSG sind nicht effektiv genug. Denn es finden die allgemeinen Regelungen des Datenschutzes auch auf das Beschäftigungsverhältnis Anwendung. Diese sind oft nicht explizit auf den Persönlichkeitsrechtsschutz der Beschäftigten zugeschnitten.

2. Eine eigenständige gesetzliche Regelung muss die dem Arbeitsverhältnis immanente Abhängigkeit der Beschäftigten zum Arbeitgeber aufgreifen und eine Generaleinwilligung für die Datenerhebung und -nutzung schon bei Aufnahme des Arbeitsverhältnisses, aber auch während des Arbeitsverhältnisses verhindern.

3. Das Gesetz muss die anlasslose Beobachtung und Überwachung von Beschäftigten am Arbeitsplatz, aber auch im privaten Umfeld verbieten. Dieses grundsätzliche Verbot muss die direkte Überwachung durch Beauftragte, Externe oder Mitarbeiter, aber auch die indirekte Überwachung durch Video- oder Tonaufnahmen umfassen. Auch biometrische oder ferngesteuerte Systeme (RFID, GPS oder Fernwartungssoftware auf Mitarbeiter- PCs) dürfen nicht über eng begrenzte Zwecke hinaus eingesetzt werden und bedürfen der Vorabkontrolle.

4. Bei der Nutzung von Internet und E-Mail ist dem Persönlichkeitsrecht der Beschäftigten in besonders hohem Maße Rechnung zu tragen. Es muss ein grundsätzliches Verbot des Zugriffs auf personenbezogene oder beziehbare Nutzerdaten bei der Verwendung dieser modernen Kommunikationsmittel festgelegt werden. Dieses Verbot darf nicht durch eine Generaleinwilligung der Beschäftigten – etwa mit Abschluss des Arbeitsvertrages - ausgeschlossen werden.

5. Ausgehend von dem Grundsatz, dass der Zweck des Datenschutzes darin besteht, die Einzelnen vor Missbrauch ihrer Daten zu schützen, können Ausnahmen nur für gesetzlich ausdrücklich geregelte Fälle vorgesehen werden. Dies ist insbesondere nur dann zuzulassen, wenn eine andere Aufklärung, insbesondere durch die Polizei oder die Staatsanwaltschaft, nicht möglich ist. Ausnahmen sind für Fälle des begründeten Verdachts einer Straftat oder der schwerwiegenden Schädigung des Arbeitgebers zuzulassen. Hierzu sind das Zustimmungserfordernis der Interessenvertretung oder,

sofern nicht vorhanden, die Einbeziehung einer neutralen Stelle (z.B. des Landesdatenschutzbeauftragten) erforderlich[5].

6. Es ist notwendig, das Fragerecht des Arbeitgebers bei der Einstellung und die Möglichkeit der Anordnung von ärztlichen Untersuchungen im Gesetz auf die durch die Rechtsprechung beurteilten Fälle zu beschränken. Die Anordnung von ärztlichen Untersuchungen bedarf der Zustimmung des Betriebsrates.

7. Vor der Erhebung von Beschäftigtendaten im Rahmen eines Einstellungsverfahrens ist über die Art der auszuübenden Tätigkeit und deren Einordnung in den Arbeitsablauf des Betriebs zu unterrichten.

8. Es bedarf einer Sonderregelung im Gesetz für den folgenden Fall: Sind Beschäftigte auch Kunden ihres Arbeitgebers, müssen die Daten des Kundenbereichs gesondert geführt und geschützt werden. Personalverantwortliche dürfen keinen Zugriff auf diese Kundendaten haben.

9. Es ist notwendig, dass seit Beginn 2010 in puncto Einmeldungen bereits angelaufenen, aber noch nicht im Wirkbetrieb befindlichen Verfahren des elektronischen Entgeltnachweises ELENA gesetzlich zu überarbeiten, wenn ein rechtmäßiger Betrieb hergestellt werden soll. Bei diesem Verfahren werden gegenwärtig monatlich Beschäftigtendaten eingemeldet und – angesichts des verhängten Moratoriums der Bundesregierung - anlasslos vier Jahre lang gespeichert. Ob dies den verfassungsrechtlichen Vorgaben entspricht, wird das Bundesverfassungsgericht noch entscheiden. Dem Deutschen Bundestag wird aufgegeben, im Rahmen des Gesetzgebungsverfahrens zu prüfen, ob die Datenerhebung und -speicherung im sogenannten ELENA-Verfahren mit der Rechtsprechung des Bundesverfassungsgerichts vereinbar ist.

10. Fälle des sog. Whistleblowings sind gesetzlich gesondert zu verankern und mit einem Maßregelungsverbot zu versehen[6].

11. Ein eigenständiges Beschäftigtendatenschutzgesetz muss die Rechtsposition des betrieblichen Datenschutzbeauftragten stärken, so z.B. durch eine weiter verbesserte Kündigungsschutzregelung

12. Die Mitbestimmungsrechte der Betriebsräte beim Datenschutz sind durch das Gesetz zu stärken.

13. Für die Daten von Mitgliedern des Betriebsrates und von Aufsichtsräten einen Immunitätsschutz für die Dauer ihrer Amtszeit zu prüfen bzw. darüber hinaus in

[5] (siehe hierzu: Däubler/Klebe/Wedde/Weichert, Kompaktkommentar zum BDSG, 2010, S. 558 ff.)

[6] ausführlich zur Thematik des Whistle-Blowings: Tinnefeld/Rauhofer, Whistleblower: Verantwortungsbewusste Mitarbeiter oder Denunzianten? DuD 2008, S.717 ff.

Anlehnung an die Vorschriften zum Sonderkündigungsschutz im Kündigungsschutzgesetz gelten.

14. Um die von Datenschutzverstößen betroffenen Beschäftigten in der Rechtsdurchsetzung zu stärken, muss das Gesetz eine Verbandsklagemöglichkeit vorsehen. Denn im bestehenden Arbeitsverhältnis wird eine Klage gegen den Arbeitgeber der Erfahrung halber nicht angestrengt. Hierzu ist die Gefahr von Repressalien zu groß.

15. In einem Beschäftigtendatenschutzgesetz ist ein konkreter Anspruch auf Schmerzensgeld für den in seinem Persönlichkeitsrecht verletzten Beschäftigten (z.B. entsprechend § 15 AGG) zu verankern.

16. In einem neuen Beschäftigtendatenschutzgesetz müssen die Ansprüche der Beschäftigten bei Verstößen gegen den Beschäftigtendatenschutz konkret, klar und verständlich geregelt werden. Es bedarf u. a. eines Unterlassungsanspruches gegenüber dem Arbeitgeber sowie eines Schadensersatzanspruches für Vermögensschäden und immaterielle Schäden bei Gesetzesverstößen.

XV. Sicherheitsbehörden und die Evaluierung von Eingriffsbefugnissen

Die Enquete-Kommission empfiehlt dem Deutschen Bundestag:

die bestehenden Aufgaben und Befugnisse von Sicherheitsbehörden und Diensten, die mit Grundrechtseingriffen verbunden sind, umfassend hinsichtlich ihrer Notwendigkeit, Wirksamkeit und Effizienz sowie ihrer grundrechtswahrenden Funktion unabhängig, auf wissenschaftlicher Grundlage und ergebnisoffen zu evaluieren. Dies betrifft insbesondere die verdeckten Ermittlungsmaßnahmen. Zwar bestehen in zahlreichen Gesetzen bereits Evaluierungsvorschriften, die jedoch in der Umsetzung diesen Ansprüchen zumeist nicht genügen.

XVI. Ubiquitious computing

Nach den Datenschutzkonzepten der 60er und 70er Jahre, denen die damalige Großrechnertechnologie zugrunde lag, bedarf es jetzt schlüssiger Antworten auf die weltweite Vernetzung von Rechnern in einem eigenen "virtuellen Sozialraum"des Internets. Gleichzeitig beginnt mit der vernetzten Digitalisierung von Infrastrukturen (z.B. im Bereich Verkehr oder bei Stromnetzen) und Alltagsgegenständen u.a. mit Sensoren wie den RFiDs (Beispiel des sogenannten. "intelligenten Kühlschrankes") bereits die nächste große Herausforderung, auf die es noch keine regulatorische Antwort gibt. Kennzeichen dieser unter dem Stichwort Ubiquitous Computing zusammengefassten Entwicklung ist die (oft “ad hoc“ erfolgende) Verknüpfung der körperlichen Alltagswelt mit der virtuellen Welt des Internets. Die mit Sensortechnik ausgestatteten Alltagsgegenstände nehmen Veränderungen ihrer Umwelt wahr, vernetzen sich mit vergleichbaren Gegenständen und reagieren kontextbezogen. Über die Verbindung mit den Besitzern der Gegenstände erfolgen zumindest mittelbar umfangreiche

personenbeziehbare Speicherungen von Daten auf Vorrat sowie Nutzerprofile. In der Summe können auf diese Weise verhältnismäßig dichte Überwachungsnetze hinsichtlich der sich in diesen interaktiven Umgebungen bewegenden Personen entstehen. Die bisherigen Grundprinzipien des Datenschutzes sind mit diesen Anwendungen kaum in Einklang zu bringen[7].

Die Enquete-Kommission empfiehlt im Hinblick auf die Entwicklungen der allgegenwärtigen Datenverarbeitung dem Deutschen Bundestag:

1. die beginnende tatsächliche Ausbreitung von Anwendungen des Ubiquitous Computing ständig sorgsam zu beobachten.

2. Der Grundsatz verpflichtender technischer Vorkehrungen (Privacy by Design) bei der Entwicklung und dem Einsatz von Produkten des Ubiqitous Computing muss mit Blick auf die Funktionsweise und die besonderen Risiken ggf. gesetzlich konkretisiert werden.

3. Einschränkungen, die sich hinsichtlich der Anwendbarkeit zentraler Grundsätze des bisherigen Datenschutzrechts ergeben, durch angemessene, ein vergleichbar hohes Schutzniveau gewährleistende anderweitige Vorgaben zu kompensieren.
4. dafür Sorge zu tragen, dass die eingesetzten Technologien zugleich für Nutzer die Möglichkeit einer kontinuierlichen Erläuterung und Abrufbarkeit ihres Status mit Blick auf z.B. Profilbildung oder Vernetzungsgrad mit anderen Anwendungen gewährleisten, da der Grundsatz der Transparenz angesichts der weitgehend im Hintergrund stattfindenden vielfältigen Datenverarbeitungen besondere Bedeutung gewinnt.

XVII. Videoüberwachung

Der Einsatz von Videoüberwachungstechnik in öffentlich zugänglichen Räumen breitet sich weiterhin aus. Damit verbunden sind massenhafte Bilderfassungen und Bildspeicherungen von völlig unbeteiligten Personen. Die tatsächlichen Einsatzbedingungen, beispielsweise die Frage des konkreten Zwecks, technische Möglichkeiten wie etwa das Zoomen oder die Frage, ob es sich um eine internetgestützte Bildübertragung handelt, bleiben für die Betroffenen weithin intransparent. Darüber hinaus fehlt es an einer hinreichenden und aktuellen Übersicht, in welchem Umfang vor allem städtische Räume bereits von Videoüberwachungen betroffen sind. Die Datenschutzbeauftragten der Länder haben in den vergangenen Jahren auf zahlreiche weitere Probleme des zunehmenden Kameraeinsatzes aufmerksam gemacht, darunter insbesondere das gewaltige Vollzugsdefizit hinsichtlich der Beachtung der gesetzlichen Vorschriften. Die bestehenden gesetzlichen Regelungen, insbesondere § 6 b Bundesdatenschutzgesetz, haben auch inhaltlich keine Einschränkung dieser Entwicklung bewirken können und bieten den Bürgern nur unzureichenden rechtlichen Schutz.

[7] vgl. dazu insgesamt Roßnagel, MMR 2005, S. 71.

Die Enquete-Kommission empfiehlt deshalb dem Deutschen Bundestag,

1. im Rahmen einer Reform insbesondere des Bundesdatenschutzgesetzes die Zulässigkeit der Bild-Erfassung öffentlich zugänglicher Räume enger zu begrenzen,

2. sachgerechte Regelungen für eine verbesserte Transparenz und Sicherheit beim Einsatz von Videotechnik auf den Weg zu bringen, darunter auch Maßnahmen zur laufenden Beobachtung und Erfassung der Gesamtentwicklung der Ausbreitung,

3. die Bundesregierung anzuhalten, im Rahmen der Erneuerung der EG-Datenschutzrichtlinie 95/46 auf zulässigkeitsbegrenzende Bestimmungen für den Einsatz von Videoüberwachungen zu drängen.

XVIII. Datenschutz auf technischer Ebene (deep-packet-inspection und IPv6)

Der Datenverkehr von Nutzern im Internet sollte einem vollständigen Telekommunikationsgeheimnis unterliegen. Die Kommunikation von Bürgerinnen und Bürgern untereinander, mit staatlichen Stellen oder mit privaten Unternehmen gehört, wenn sie nicht von den Betroffenen selbst öffentlich gemacht wird, zur schützenswerten Privatsphäre jedes Einzelnen. Netzwerkmanagementmaßnahmen, etwa mit Hilfe von so genannter Deep-Packet-Inspection (DPI), bei der die von Teilnehmern gesendeten und empfangenen Inhalte durchleuchtet bzw. auch auf der Inhaltsebene ausgelesen und analysiert werden, sind unter diesem Gesichtspunkt datenschutzrechtlich abzulehnen.

Durch die rasant ansteigende Zahl von Geräten, die am Internet angeschlossen sind bzw. darüber kommunizieren, ist bereits seit geraumer Zeit klar, dass der verwendbare Adressraum des IPv4-Protokolls ausgereizt und nicht zukunftsfähig ist. Die anstehende Einführung des IPv6-Protokolls in den Internet-Alltag bietet die Nutzung einer ungleich größeren möglichen Anzahl nutzbarer IP-Adressen im Internet. Mit Nutzung von IPv6 ist es daher technisch möglich jedem internetfähigen Endgerät eine dauerhafte einzigartige IP-Adresse zuzuweisen. Somit ist die Kommunikation eines einzelnen Endgerätes theoretisch über Jahre hinweg nachvollziehbar.

Die Enquete-Kommission empfiehlt dem Deutschen Bundestag:

1. Die Verwendung von Methoden zur inhaltlichen Analyse von (IP-) Datenpaketen (z.B. DPI) bzw. die Analyse selbst zu untersagen. Dies gilt für Eingriffe von staatlicher und nicht-staatlicher Seite gleichermaßen und muss technikneutral formuliert werden.

2. Internet-Zugangsanbieter zu verpflichten, ihren Kunden ohne Mehrkosten die Auswahl zwischen dauerhaft festen und wechselnden IP-Adressen für ihre Anschlüsse bzw. Endgeräte anzubieten.

XIX. Geolocation/Geodaten

Die Enquete-Kommission stellt fest, dass sich mit dem Entstehen der digitalen Gesellschaft zunehmend auch eine digitale Öffentlichkeit herausbilden wird. Zu dieser digitalen Öffentlichkeit gehört auch das Angebot und die Nutzung von Geoinformationen bzw. Geodiensten und -anwendungen im Internet, wie z. B. Kartierungs- und Lokalisierungsdienste wie Google-Street-View, Microsoft Street Side,, Facebook-Places, Quype etc.

Wie auch in der analogen Welt gilt es , die Öffentlichkeit und den öffentlichen Raum als eine Grundvoraussetzung einer demokratisch verfassten offenen Gesellschaft zu erhalten und gleichzeitig die Privatheit zu schützen. Das bedeutet auch, die grundrechtlich abgesicherten Positionen wie Wissenschafts-, Presse- und unternehmerische Freiheit mit anderen Grundrechten wie dem Persönlichkeitsrecht und dem Recht auf informationelle Selbstbestimmung in Einklang zu bringen. Die Enquete-Kommission hält fest, dass Selbstverpflichtungen der in diesem Bereich tätigen Unternehmen hilfreiche Instrumente darstellen, wenn Persönlichkeitsrechte betroffen sind, bedürfen Sie aber jedenfalls eines gesetzlichen Rahmens.

Sie nimmt Bezug auf die Forderungen der Beauftragten für den Datenschutz und die Informationsfreiheit des Bundes und der Länder und empfiehlt dem Deutschen Bundestag,

eine allgemeine und technikunabhängige Regelung zur Verarbeitung von personenbezogenen Geoinformationen/-daten zu schaffen, die sich an den jeweiligen Risiken orientiert. Hierbei sollten folgende Gesichtspunkte beachtet werden:

a. Es sollten Kriterien geschaffen werden, die festlegen, über welche Verfahren eine Interessenabwägung zwischen Persönlichkeitsschutz und Informationsinteresse vorgenommen werden kann und wonach eine klare Abgrenzung zwischen reinem Sachbezug oder Personenbeziehbarkeit möglich ist.
b. Es sollte geprüft werden, ob und inwieweit eine gesetzliche Verpflichtung zu schaffen ist, die die Tatsache der konkreten Ortung den Betroffenen in verständlicher Form anzeigt, z. B. durch ein akustisches Signal, sobald die/der Betroffene geortet wurde.
c. Ebenso ist eine Regelung zu schaffen, wonach beim Einsatz von Tracking-Systemen, also jede Form der Ortung durch Dritte, die Betroffene nicht beeinflussen können, die Einwilligung (nach dem Vorbild von § 98 TKG) vorgesehen wird.
d. Darüber hinaus ist eine Regelung zu schaffen, wonach Unternehmen, die grundsätzlich sachbezogene, aber personenbeziehbare Geoinformationen im Internet zur Nutzung oder zur Verarbeitung veröffentlichen, welche schutzwürdige entgegenstehende Interessen der Betroffenen berühren können, ein Widerspruchsrecht den Betroffenen (wie z. B. Eigentümern, Mietern etc.) anbieten müssen. Ein entsprechendes Recht muss gesetzlich festgeschrieben

werden und kann nicht allein durch eine Selbstverpflichtung der anbietenden Unternehmen geregelt werden.

e. Verstöße gegen entsprechende Regelungen müssen sanktioniert werden, wobei die Aufsicht hierüber den Datenschutzbeauftragten des Bundes und der Länder sowie den Aufsichtsbehörden über den Datenschutz im nicht-öffentlichen Bereich obliegen sollte.