Projektgruppe „Datenschutz, Persönlichkeitsrechte“

2.2. Datenschutz im öffentlichen Bereich (STAND: 15.3.)

Streitige Passagen sind kursiv gefasst.

2.2.1 Datenschutz in öffentlichen Einrichtungen

2.2.1.1. Einführung

Das deutsche Datenschutzrecht beruht seit seinen Anfängen auf einer Unterscheidung zwischen Datenschutz im Bereich öffentlicher Einrichtungen und dem Datenschutz bei nicht öffentlichen Stellen, insbes. in der Privatwirtschaft. Diese Differenzierung, die sich auch in der Struktur des Bundesdatenschutzgesetzes niedergeschlagen hat, findet ihren Ausgangspunkt in der Konzeption des Rechts auf informationelle Selbstbestimmung als eines individuellen Abwehrrechts gegenüber staatlichen Eingriffen. In diesem Zusammenhang wird darauf hingewiesen, dass die grundrechtlichen Grenzen für staatliche Datenverarbeitung enger sind als im nichtöffentlichen Bereich. Die öffentliche Gewalt wird durch die Grundrechte verpflichtet und kann sich nicht auf eigene entgegenstehende Grundrechte berufen. Zwischen staatlichen und nichtstaatlichen Gefährdungen der informationellen Selbstbestimmung besteht daher weiterhin ein Unterschied. [Fußnote: vgl. auch Di Fabio, Udo, in : Maunz/Dürig, Grundgesetz, Kommentar, 58. Ergänzungslieferung 2010, Art. 2, Rn. 190.] Die Europäische Datenschutzrichtlinie kennt diese Zweiteilung jedoch nicht. Das deutsche Recht sieht derzeit zumindest teilweise eine Gleichstellung öffentlicher und privater Datenverarbeitung vor, etwa für Telemedien. [Fußnote: Vgl. § 1 Abs. 1 Satz 2 TMG.]

Da das Grundgesetz keine zentrale Kompetenznorm für die Gesetzgebung im Bereich des Datenschutzes enthält, ergibt sich die Zuständigkeit für die Gesetzgebung als Teil der Regelungskompetenz für das jeweilige Verwaltungsverfahren aus den Sachkompetenzen der Art. 73 und 74 GG. [Fußnote: Kühling, Jürgen / Seidel, Christian / Siviridis, Anastasios: Datenschutzrecht, 2008, S. 74.]Bundesgesetze können daher den Datenschutz nur für Bereiche der Gesetzgebung des Bundes regeln. Entsprechendes gilt für Landesgesetze.

Neben der Unterscheidung datenschutzrechtlicher Bestimmungen für den privaten und öffentlichen Bereich ergibt sich also noch eine weitere Differenzierung zwischen bundes- und landesrechtlichen Normen. Dieses Nebeneinander bundes- und landesrechtlicher

Vorschriften kennzeichnet besonders den öffentlichen Bereich, da im privaten Bereich im Rahmen der konkurrierenden Gesetzgebungskompetenz nach Art. 74 Nr. 11 GG („Recht der Wirtschaft“) viele Bereiche - einschließlich der jeweiligen datenschutzrechtlichen Aspekte - durch Bundesgesetze geregelt sind, so dass für den privaten Bereich wenig Regelungsmöglichkeiten für die Länder verbleiben. [Fußnote: Kilian, Wolfgang / Weichert, Thilo, in: Kilian/Heussen (Hrsg.),Computerrechts-Handbuch, 28. Ergänzungslieferung, 2010, 1. Abschnitt, Teil 13, Punkt I., Rn. 3.]

Darüber hinaus sind in vielen Fallkonstellationen Fragen der Spezialität und Subsidiarität von Normen zu beantworten. So haben etwa nach § 1 Abs. 3 BDSG andere datenschutzrechtliche Vorschriften des Bundes Vorrang vor dem BDSG. Vollziehen Landesbehörden Bundesrecht, gelten auf Grund einer weiteren Subsidiaritätsregelung (§ 1 Abs. 2 Nr. 2 BDSG) statt des BDSG die Landesdatenschutzgesetze, dies jedoch nur, soweit das zu vollziehende Bundesrecht (z. B. SGB, StVG) keine datenschutzrechtlichen Bestimmungen enthält. [Fußnote: Bergmann, Lutz / Möhrle, Roland / Herb, Armin: Datenschutzrecht, Stand April 2010, Ziff. 3.3.2.2.] Ganz überwiegend gilt auch für die Landesdatenschutzgesetze der Grundsatz der Subsidiarität gegenüber anderen datenschutzrechtlichen Regelungen. [Fußnote: Gola, Peter / Schomerus, Rudolf: BDSG, Kommentar, 2010, § 1, Rn. 33.]
Vielfach wird daher ein unübersehbares „Dickicht des bereichspezifischen Datenschutzes“ [Fußnote: Bergmann, Lutz / Möhrle, Roland / Herb, Armin: Datenschutzrecht, Stand April 2010, Ziff. 4.1.2.]beklagt. Im Ergebnis hat dies dazu geführt, dass im Bereich öffentlicher Einrichtungen das BDSG nicht das zentrale Regelungsinstrument darstellt. [Fußnote: Bergmann, Lutz / Möhrle, Roland / Herb, Armin: Datenschutzrecht, Stand April 2010, Ziff. 3.2.7.]

Die deutliche Unterscheidung zwischen Datenschutz im öffentlichem und privatem Bereich gilt auch für die Organisation der Aufsicht und Kontrollorgane. Während Bundes- und Landesdatenschutzbeauftragte die jeweilige Kontrolle über Bundes- und Landesverwaltung ausüben, wird die Kontrolle im privaten Bereich ausschließlich auf Länderebene, teilweise durch die Landesdatenschutzbeauftragten, teilweise durch gesonderte Aufsichtsbehörden, ausgeübt. Gesonderte Kontrolleinrichtungen gibt es im etwa Bereich der Kirchen und öffentlich-rechtlicher Rundfunkanstalten.

Der Datenschutzaufsicht kommt für die Verwirklichung eines effizienten Datenschutzes eine herausragende Rolle zu. Stärkung der Aufsichtsbehörden bedeutet somit zugleich eine Verbesserung des Datenschutzes. Vor dem Hintergrund der jüngsten Rechtsprechung des EuGH (Urteil vom 9.3.2010 C-518/07 [1]) ist es zwingend not-

wendig, die völlige Unabhängigkeit der Datenschutzaufsicht zu gewährleisten. Durch die Entscheidung des Europäischen Gerichtshofs könnte auch ein gesetzgeberisches Handeln auf Bundesebene erforderlich sein. Ein entsprechender Auftrag zur Prüfung ist bereits durch die fraktionsübergreifende Entschließung vom 16.12.2010 erteilt worden. [Fußnote: BT-Drs. 17/4179, S. 5.]Die europäische Datenschutzrichtlinie gibt vor, dass die Datenschutzaufsicht rechtlich, organisatorisch und finanziell unabhängig sein muss. Hierbei unterscheidet die Richtlinie nicht zwischen öffentlichem und privatem Bereich.

2.2.1.2. Das Bundesdatenschutzgesetz (BDSG)

Das BDSG ist ein Schutzgesetz, das natürliche Personen schützen soll. Verstöße dagegen können Schadenersatzansprüche begründen. Allerdings begrenzt das BDSG die Möglichkeit einer verschuldensunabhängigen Haftung für Datenschutzverstöße auf die öffentlichen Einrichtungen (§§ 7, 8 BDSG).

Das Datenschutzgesetz ist daneben ein Eingriffsgesetz, mit dem Eingriffe in das Grundrecht auf informationelle Selbstbestimmung gerechtfertigt werden. Die konkreten Eingriffsnormen bzw. Eingriffe müssen durch ein überwiegendes Allgemeininteresse gerechtfertigt sein. Sie müssen zudem den Grundsätzen der Verhältnismäßigkeit und der Normenklarheit genügen und Schutzvorkehrungen zum Zwecke der Datensicherheit und der Sicherheit der Betroffenenrechte vorsehen.

Nach dem BDSG gilt – wie im gesamten Datenschutzrecht - wegen des mit der Datenverarbeitung verbundenen Grundrechtseingriffs und dem Gesetzesvorbehalt das Verbot mit Erlaubnisvorbehalt (§ 4 Abs. 1 BDSG). Das heißt, Datenverarbeitung ist nur dann zulässig, wenn entweder eine Rechtsvorschrift dies ausdrücklich vorsieht oder der Betroffene ausdrücklich eingewilligt hat.
Hierbei sind im Sinne der Rechtsprechung des Bundesverfassungsgerichts besonders hervorzuheben:

- die Zweckbindung für die Verwendung personenbezogener Daten,
- eine strikte Beschränkung der Datenverarbeitung und -nutzung auf das Erforderliche,
- die größtmögliche Selbstbestimmung der Betroffenen sowie
- die Transparenz der Datenverarbeitung.

Nur bei Beachtung dieser Anforderungen ist der notwendige Schutzzweck für ein modernes Datenschutzrecht gewährleistet.

Über das BDSG hinaus finden sich weitere Datenschutzregelungen mit Relevanz für den staatlichen Bereich in dem Bundespersonalvertretungsgesetz (BPersVG) sowie den jeweiligen Landespersonalvertretungsgesetzen, dem Betriebsverfassungsgesetz (BetrVG), den jeweiligen Landesvorschriften zum Datenschutz, den sozialrechtlichen Vorschriften (SGB), dem Telekommunikationsgesetz (TKG) und dem Telemediengesetz (TMG) sowie diversen EU- und UN-Richtlinien betreffend personenbezogene Daten.

Durch die engen Vorgaben zu Eingriffen in das Recht auf informelle Selbstbestimmung nimmt der Staat in Fragen des Datenschutzes eine Vorbildfunktion für nichtstaatliche Akteure ein.

Wenn durch die Politik allerdings immer weitere Einschränkungen des Datenschutzes zur vorgeblichen Bekämpfung von Kriminalität oder Terrorismusabwehr vorgenommen werden, sinkt sogleich die Möglichkeit, glaubwürdig Einfluss auf den Umgang von nichtstaatlichen Akteuren mit persönlichen Daten zu nehmen. Hier sei exemplarisch auf den sprunghaften Anstieg der Kontoabfragen durch Finanz- und Sozialverwaltungen in den letzten Jahren hingewiesen, die im direkten Zusammenhang mit Erweiterungen der Zugriffsmöglichkeiten mindestens auf so genannte Stammdaten bei Banken und Sparkassen zurückgehen. So droht der Vorbildcharakter des Staates verloren zu gehen.

Absatz streitig

Auch wenn es im staatlichen Bereich einige Spezifika bezüglich des Beschäftigtendatenschutzes gibt, wird an dieser Stelle nicht darauf eingegangen. Vielmehr wird das Thema Beschäftigtendatenschutz übergreifend, sowohl für den privaten als auch den öffentlichen Sektor, Gegenstand des Kapitels 2.3. sein.

2.2.1.3. Staatliche Datenverarbeitung im Wandel

Die Anfänge der Datenschutzbewegung in Europa wie auch in den USA wandten sich gegen als übermächtig und bedrohlich empfundene Datenerhebungsprojekte staatlicher Stellen.

Hinter diesen Projekten stand die zunehmende Computerisierung der Verwaltung, die neue Möglichkeiten einer Zusammenführung und Auswertung von personenbezogenen Daten erstermöglichte. Die geplante Volkszählung zu Beginn der 80er Jahre und das daraufhin 1983 ergangene Volkszählungsurteil des Bundesverfassungsgerichts etablierten dann endgültig die bis dahin noch streitigen rechtlichen Grundprinzipien des Datenschutzes.

Nachfolgend haben Gesetzgeber und Verwaltung in der Verfolgung ihrer Aufgaben weiterhin Instrumente und Verfahren vorangetrieben, die zumindest mit Blick auf den Datenschutz erhebliche Prob-

leme aufgewiesen haben. Dies gilt in zunehmendem Maße auch für Vorhaben auf europäischer Ebene. Die Vielzahl an Entscheidungen des Bundesverfassungsgerichts zu Bundes- und Landesgesetzen (z. B. G 10-Entscheidung, Großer Lauschangriff, Online-Durchsuchung, Rasterfahndung, KFZ-Kennzeichenerfassung, Vorratsdatenspeicherung)markiert dabei einen aktuellen Stand des Datenschutzes im öffentlichen Bereich, der auf den Widerstreit zwischen den von staatlichen Stellen in Anschlag gebrachten öffentlichen Interessen einerseits, sowie dem insbesondere vom Bundesverfassungsgericht betonten verfassungsrechtlichen Persönlichkeitsrecht andererseits, hinweist.

Die Auseinandersetzung beschränkt sich dabei nicht auf den Sicherheitsbereich, sondern findet ihre Fortsetzung auch in anderen Bereichen der öffentlichen Verwaltung, so etwa in den aktuellen Auseinandersetzungen um Grenzen zulässiger Datenerhebung bei Hartz-IV-Empfängern oder die Ausweitung staatlicher Kontodatenzugriffe.

2.2.1.4 Herausforderungen für das Datenschutzrecht in öffentlichen Einrichtungen

Die Informationsverarbeitung öffentlicher Stellen stellt besondere Herausforderungen an den Datenschutz, denn:

- viele staatliche und kommunale Aufgaben, z.B. in Steuerverwaltung, Justiz, Sicherheit, Sozialhilfe und Gesundheitswesen, erfordern naturgemäß die Erfassung und Verarbeitung personenbezogener Daten, die einen besonderen Schutzbedarf aufweisen können;
- die mit der Informationsverarbeitung einhergehenden Fachaufgaben, insbesondere in der Eingriffsverwaltung, sind gesetzlich legitimiert;
- die vollständige Durchdringung der öffentlichen Verwaltung mit IT hat zur Konsequenz, dass die öffentliche Verwaltung in ihrer Gesamtheit über ein fast lückenloses Datenprofil aller Bürger verfügt.

Datenschutz im öffentlichen Bereich muss vor diesem Hintergrund sicherstellen, dass

- die Informationsverarbeitung und die damit verbundene Einschränkung des informationellen Selbstbestimmungsrechtes in jedem Anwendungsfall rechtlich legitimiert und angemessen ist (Erforderlichkeitsgrundsatz),

- die personenbezogenen Daten nur zu dem Zweck verwendet werden, für den sie erfasst wurden (Zweckbindungsgrundsatz),
- betroffene Bürger wissen, welche öffentliche Stellen welche Daten über sie gespeichert haben (Transparenzgrundsatz), und
- nur solche personenbezogenen Daten *von Bürgern und Beschäftigten* erfasst und gespeichert werden, die zur Erledigung der jeweiligen Aufgabe unbedingt erforderlich sind (Datenvermeidungs- und Datensparsamkeitsgrundsatz).

kursiv gefasste Ergänzung streitig

Die bereichsspezifischen Regelungen zum Datenschutz sollen nicht nur einer materiellen Verletzung dieser Grundsätze vorbeugen, sondern darüber hinaus auch vermeiden, dass die persönlichen Grundrechte durch ein diffuses Gefühl totaler staatlicher Überwachung [Fußnote: BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 212.] eingeschränkt oder beeinträchtigt werden.

Gerade um diesem diffusen Gefühl totaler staatlicher Überwachung entgegenzutreten, wird diskutiert, ob und wie Auskunftsrechte für Bürgerinnen und Bürger und Auskunftspflichten staatlicher Stellen, etwa im Zusammenhang mit den Informationsfreiheitsgesetzen der Länder und des Bundes, überprüft und gegebenenfalls ausgebaut werden sollten.

Absatz streitig

Regelmäßig lassen sich zum Teil deutliche Modifikationen der zulässigen Datenerhebungen erreichen, aber ein grundsätzlicher Verzicht auf „Datensammelprojekte“ wird politisch oftmals nicht erreicht. Stattdessen kam und kommt ein Schutzprogramm des Datenschutzes zur Anwendung, das zu großen Teilen mit der technischen Entwicklung nicht mehr Schritt gehalten hat und deshalb oftmals nicht zu passen scheint. Dementsprechend wird auch im Bereich der öffentlichen Verwaltung von massiven Vollzugsdefiziten hinsichtlich des Datenschutzes gesprochen, obwohl dort eine längere Tradition des Umganges mit diesem Recht sowie eine weitaus selbstverständlichere Bindung an das Gesetz besteht. Auch das Aufsichtssystem des Datenschutzes wirft insoweit Fragen auf, als die fehlende Unabhängigkeit der in Landeszuständigkeit erfolgenden Datenschutzaufsicht vom EuGH gerügt wurde, aber bis heute folgenlos geblieben ist.
Beim Betrieb bestehender oder der Einführung neuer IT-Infrastrukturen in öffentlichen Einrichtungen ergeben sich eine Vielzahl datenschutzrechtlicher Fragestellungen.

alternativer Textvorschlag

Bei bisherigen Gesetzgebungsvorhaben konnten oft während des parlamentarischen Verfahrens noch Veränderungen hin zu einer Reduzierung der Menge an gesammelten, personenbezogenen Daten erreicht werden, jedoch nicht ein vollständiger Verzicht auf das

jeweilige Vorhaben. Gesetzliche Schutzprogramme für den Datenschutz können zudem vielfach mit der technischen Entwicklung nicht Schritt halten.
Beim Betrieb bestehender oder der Einführung neuer IT-Infrastrukturen in öffentlichen Einrichtungen ergeben sich daher eine Vielzahl datenschutzrechtlicher Fragestellungen.

Deren frühzeitige Einbeziehung in alle Projekte u.a. bei der Entwicklung der jeweiligen Hard- und Software ist unabdingbar. Die Umstellung bestehender Verwaltungsverfahren auf elektronische Basis birgt dabei auch Chancen für den Datenschutz. Die zukünftige Technik kann bereits frühzeitig nach den Geboten der Datensparsamkeit und -sicherheit gestaltet werden. [Fußnote: Bizer, Johann (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein): eGovernment: Chance für den Datenschutz, abrufbar unter: https://www.datenschutzzentrum.de/e-government/dud-200507.htm (Stand: 11.11.2010).]

Fragen des Datenschutzes in öffentlichen Einrichtungen werden vielfach unter den Stichworten „eGovernment und Datenschutz“ thematisiert. Als besondere Herausforderungen werden hierbei unter anderem beschrieben: [Fußnote: Vgl. Der Landesbeauftragte für den Datenschutz Niedersachsen: Herausforderungen für den Datenschutz bei eGovernment, abrufbar unter: http://www.lfd.niedersachsen.de/live/live.php?navigation_id=13010&article_id=56234&_psmand=48 (Stand: 11.11.2010).]

- Zunahme personenbezogener Daten, d. h. die gesamte Kommunikation Einzelner mit Behörden kann erfasst und analysiert werden; im Gegensatz dazu fallen etwa bei formlosen (fern-)mündlichen Anfragen bei einer Behörde üblicherweise keinerlei Daten an; [Fußnote: Vgl. hierzu auch Yildirim, Nuriye: Datenschutz im Electronic Government, 2004, S. 64.]
- Zunahme zentraler, bereichsübergreifender Datenbestände, etwa wenn Verwaltungsdienstleistungen unterschiedlicher Behörden oder Behördenbereiche an einer zentralen Stelle (etwa One-Stop-Government oder Lebenslagenkonzept) angeboten werden; beispielsweise durch den „einheitlichen Ansprechpartner“ nach der EU-Dienstleistungsrichtlinie, der als zentrale Anlaufstelle insbesondere für elektronische Behördendienste fungiert; [Fußnote: Vgl. hierzu auch Petersen, Christin: Einheitlicher Ansprechpartner und Datenschutz, LKV 2010, S. 344 ff.]
- Fragen der Datensicherheit im Rahmen der elektronischen Kommunikation mit dem Bürger, etwa Gefährdungen des internen IT-Systems durch Systemöffnung, Notwendigkeit der Authentisierung bei Übermittlung personenbezogener Daten;

- Fragen der internen Datensicherheit;
- datenschutzrechtliche Verantwortlichkeiten bei Zusammenarbeit mehrerer Stellen, gegebenenfalls auch von Bund, Ländern und Kommunen; [Fußnote: Vgl. hierzu auch Landesbeauftragter für den Datenschutz Baden-Württemberg (Hrsg.): Ein modernes Datenschutzrecht für das 21. Jahrhundert, Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. März 2010, S. 15.]
- Einschaltung (privater) technischer Dienstleister.

2.2.1.5 Cloud Computing in der öffentlichen Verwaltung

Cloud Computing als Möglichkeit, Speicherkapazitäten, Rechenleistung und Software bedarfsspezifisch über das Internet zu beziehen, könnte perspektivisch auch in öffentlichen Einrichtungen an Bedeutung gewinnen. Die gemeinsame Nutzung von Hard- und Software sowie Rechenkapazitäten, die auf verschiedenen Servern nachfrage- und einzelfallabhängig zur Verfügung gestellt werden, könnte auch für Behörden, Ministerien und kommunale Selbstverwaltungskörperschaften möglicherweise Sparpotentiale durch Senkung der Ausgaben für eigene Hard- und Software eröffnen. [Fußnote: Vgl. Schulz, Sönke: Cloud-Computing in der öffentlichen Verwaltung, MMR 2010, S. 75.]
Allerdings steht diese Form der Vernetzung behördlicher IT-Infrastrukturen, also der von unterschiedlichen Trägern der öffentlichen Verwaltung eingesetzten Hard- und Software, noch am Anfang. [Fußnote: Schulz, Sönke: Cloud-Computing in der öffentlichen Verwaltung, MMR 2010, S. 75.] Soweit ersichtlich, gibt es in Deutschland noch keine Nutzung von Cloud-Anwendungen durch öffentliche Stellen, wohl aber entsprechende Prüfungen. [Fußnote: Weichert, Thilo: Cloud Computing und Datenschutz, Punkt 12., abrufbar unter: https://www.datenschutzzentrum.de/cloud-computing/ (Stand: 11.11.2010).] Dabei wird davon ausgegangen, dass sich nur Modelle einer abgeschlossenen („privaten“) Cloud in alleiniger Verantwortung der öffentlichen Verwaltung als mögliche Option erweisen könnten. [Fußnote: Schulz, Sönke: Cloud-Computing in der öffentlichen Verwaltung, MMR 2010, S. 78.]
Daneben stehen andere Formen der Zusammenarbeit von öffentlichen Einrichtungen im IT-Bereich, etwa als „Shared Services Center“. Hierbei werden verwaltungsunterstützende Leistungen für die öffentliche Verwaltung zentral und gemeinschaftlich erbracht. Interne Dienstleistungen (etwa Personalverwaltung oder Gebäude-Management) werden also mittels gemeinsamer Nutzung von Ressourcen für mehrere Organisationseinheiten erbracht.
Die Bundesregierung strebt an, die Entwicklung und Einführung von Cloud Computing zu beschleunigen. Neben mittelständischen Unternehmen soll gerade der öffentliche Sektor frühzeitig von den

Chancen profitieren. Unter anderem die Bereiche Sicherung und Schutz von Daten sind an die spezifischen Anforderungen von Cloud Computing anzupassen. Datenschutz und Datensicherheit seien eine der hierbei sich ergebenden rechtlichen Herausforderungen. [Fußnote: IKT-Strategie der Bundesregierung „Deutschland Digital 2015“, November 2010, S. 12, abrufbar unter: . http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Technologie-und-Innovation/ikt-strategie-der-bundesregierung,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf (Stand: 15.11.2010).] Hierzu hat die Bundesregierung ein „Forschungsprogramm Sichere Internet-Dienste – Cloud Computing für Mittelstand und öffentlichen Sektor (Trusted Cloud)“ aufgelegt. [Fußnote: IKT-Strategie der Bundesregierung „Deutschland Digital 2015“, November 2010, S. 12, abrufbar unter: . http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Technologie-und-Innovation/ikt-strategie-der-bundesregierung,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf (Stand: 15.11.2010).]

Datenschutzrechtlich wird die Nutzung cloud-basierter Dienste bei der Verarbeitung personenbezogener Daten zumeist als eine Auftragsdatenverarbeitung im Sinne des § 11 BDSG eingeordnet. Verantwortlich für die Einhaltung datenschutzrechtlicher Vorschriften ist weiterhin der Auftraggeber (§ 11 Abs. 1 BDSG). Dieser ist insbesondere verpflichtet, den Gegenstand des Auftragsverhältnisses schriftlich hinsichtlich diverser Einzelaspekte genau festzulegen (etwa die nach § 9 BDSG zu treffenden technischen und organisatorischen Schutzmaßnahmen oder die Berechtigung zur Begründung von Unterauftragsverhältnissen). Diese rechtlichen Vorgaben setzen der cloud-basierten Verarbeitung personenbezogener Daten bisher enge Grenzen. [Fußnote: vgl. Weichert, Thilo: Cloud Computing und Datenschutz, Punkt 6.1., abrufbar unter: https://www.datenschutzzentrum.de/cloud-computing/ (Stand: 11.11.2010); Schulz, Sönke: Cloud-Computing in der öffentlichen Verwaltung, MMR 2010, S. 78 f. Zum Cloud Computing vgl. im Übrigen unter 2.3.3.] Im Übrigen gelten insoweit ähnliche Überlegungen wie für die datenschutzrechtliche Beurteilung von Cloud Computing durch private Unternehmen. [Fußnote: Schulz, Sönke: Cloud-Computing in der öffentlichen Verwaltung, MMR 2010, S. 78.]

2.2.2 Mögliche Erweiterung des Grundgesetzes im Hinblick auf das Kommunikationsgeheimnis und/oder Grundrecht auf informationelle Selbstbestimmung

(Text folgt.)

2.2.3 Datensicherheit

Datenschutz lässt sich in der Praxis nur dann sicherstellen, wenn die informationstechnischen Systeme des öffentlichen Bereiches 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 im öffentlichen Bereich durch Großrechner in abgeschotteten Rechenzentren gekennzeichnet war. Die jüngere Rechtsprechung [Fußnote: Vgl. Bundesverfassungsgericht zur Online-Durchsuchung, BVerfGE vom 27. Februar 2008, Az. 1 BvR 370/07, abgedruckt in: NJW 2008, 822; sowie Bundesverfassungsgericht zur Vorratsdatenspeicherung, Urteil vom 2. März 2010, Az. 1 BvR 256/08, BVerfGE 121, 1.] stellt in ihren Entscheidungen zunehmend auch auf die Bedeutung der informationstechnischen Sicherheit bei der Verarbeitung der personenbezogenen Daten ab.

Im Zuge des E-Government kommen 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 technisch veraltete Regelwerk auf neue Technologien und vernetzte Infrastrukturen anzuwenden.

Weitere Gesichtspunkte und Fragen der Datensicherheit werden zu einem späteren Zeitpunkt im Schlussbericht der Enquete-Kommission im Kapitel „Zugang, Struktur und Sicherheit im Netz“ aufgegriffen.

2.2.4 Datenschutzaudit und Gütesiegel zum Zwecke der Vertrauensbildung

Datenschutz in öffentlichen Einrichtungen kann durch Auditierungsverfahren gefördert und erleichtert werden. Die Verleihung von Gütesiegeln sowie die Zertifizierung und Durchführung von Audit-Verfahren können wirkungsvolle, marktsteuernde Anreize für besseren Datenschutz geben. Ähnlich wie bei der technischen Betriebssicherheit (dem TÜV) können Normen und Verfahren einen integrierten technischen Datenschutz fördern und gewährleisten.Die in den Bundesländern eingerichteten Datenschutzauditverfahren sowie das europäische Güsesiegel (EuroPriSe) können als praktische Beispiele hierfür angeführt werden.

Dabei wird das Datenschutzkonzepts einer öffentlichen Stelle durch einen unabhängigen Gutachter förmlich geprüft und von einer anderen unabhängigen öffentlichen Stelle bestätigt.

Im Unterscheid zu einer allgemeinen Beratung erfolgt beim Datenschutzaudit ein mehr: Die Beratung bezieht sich auf die jeweils konkret vorgelegte Frage bzw. auf den unterbreiteten Sachverhalt. Ob die gegebenen Empfehlungen umgesetzt werden, bleibt offen und auch Veränderungen maßgeblicher Umstände werden nach Abschluss der Beratung nicht berücksichtigt. Das Audit hingegen ist auf eine dauerhafte Verbesserung der Datenschutzorganisation gerichtet. In Anlehnung daran könnte eine staatlich gestützte Datenschutzstiftung als Gütesiegelgarantie wirken und der Vertrauensbildung Vorschub leisten.