Berufsbegleitender Masterstudiengang
Informationsrecht (LL.M.)

Center für lebenslanges Lernen

Prof. Dr. Dirk Heckmann
Prof. Dr. Dr. Volker Boehme-Neßler

eGovernment und IT-Vergabe

Carl von Ossietzky Universität Oldenburg, 2017

Impressum

Autor: Prof. Dr. Dirk Heckmann
4. Aufl. bearbeitet von
Prof. Dr. Dr. Volker Boehme-Neßler

Herausgeber: Center für Lebenslanges Lernen (C3L),
Carl von Ossietzky Universität Oldenburg

Auflage: 9. Auflage, Erstausgabe 2007

Layout: Andreas Altvater, Franziska Vondrlik

Oldenburg, Oktober 2017

Prof. Dr. Dirk Heckmann

Dirk Heckmann (*1960) absolvierte sein Jura-Studium an der Universität Trier. 1991 promovierte der Carl-von-Rotteck-Preisträger am Institut für Öffentliches Recht an der Universität Freiburg. Dort habilitierte er sich vier Jahre später in den Fächern Öffentliches Recht und Rechtstheorie. Seit 1996 hat Heckmann den Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht an der Universität Passau inne.

Beim Akkreditierungs-, Certifizierungs- und Qualitätssicherungsinstitut ACQUIN e.V. ist er seit 2001 im Fachausschuss tätig, von 2001-2004 agierte er zudem bei der Virtuellen Hochschule Bayern als Fachratssprecher. 2003 wurde der gebürtige Remscheider zum Richter am Bayerischen Verfassungsgerichtshof in München, 2007 zum Vorsitzenden des Wissenschaftlichen Beirats der Europäischen EDV-Akademie des Rechts und zum Mitglied des Vorstands der Deutschen Gesellschaft für Recht und Informatik gewählt.

Seit 2005 ist Dirk Heckmann Direktor der Forschungsstelle für Rechtsfragen der Hochschul- und Verwaltungsmodernisierung (ReHMo). Mit seinem Team betreut er den interdisziplinären und praxisorientierten Studiengang zum „IT-Juristen“ an der Universität Passau. 2006 wurde der Sicherheitsrechtsexperte in den Gründungssenat der Deutschen Hochschule der Polizei berufen. Als stv. Leiter des 2006 errichteten interdisziplinären Instituts für IT-Sicherheit und Sicherheitsrecht an der Universität Passau betreibt er Grundlagenforschung im Bereich der Rechtsinformatik und des IT-Sicherheitsrechts. Für die Deutsche Anwaltakademie ist er in der Ausbildung zum Fachanwalt für IT-Recht tätig. Seit 2009 leitet er das Center for IT-Compliance and Trust am Deutsche Telekom Institute for Connected Cities der Zeppelin University Friedrichshafen.

Dirk Heckmanns Forschungs- und Beratungsschwerpunkte liegen im Bereich IT-Sicherheit, Sicherheitsrecht und Rechtssicherheit – vor allem dort, wo Rechtsfragen des E-Governments, E-Procurement, E-Learning, E-Health, E-Banking, der IT-Vergabe und des IT-Outsourcing berührt werden – sowie auf dem Gebiet der juristischen Modellierung elektronischer Geschäftsprozesse und der Entwicklung integrierter Datenschutz- und Datensicherheitskonzepte.

Aus Heckmanns Feder stammen fast 100 Publikationen (Lehrbücher, Lexika, Kommentare und Fachaufsätze). Er ist Verfasser zahlreicher Rechtsgutachten zu Fragen des IT-Rechts, Datenschutzrechts, Verfassungs-, Vergabe- und Wettbewerbsrechts und Sicherheitsrechts für Unternehmen, Ministerien und Parlamente sowie Herausgeber des „juris-Praxisreports IT-Recht“ und der „Schriften zum Recht der Inneren Sicherheit“. 2009 erschien der von ihm herausgegebene und maßgeblich mitverfasste juris Praxiskommentar Internetrecht in der 2. Auflage.

Prof. Dr. Dr. Volker Boehme-Neßler

Volker Boehme-Neßler ist Inhaber des Lehrstuhls für Öffentliches Recht, Europarecht, Rechtstheorie, Informations- und Telekommunikationsrecht an der Carl von Ossietzky Universität Oldenburg. Studium in Berlin und Heidelberg. Dr. iur utr. 1993 in Heidelberg, Dr. rer.pol. 1997 in Berlin, Habilitation 2008 in Kassel. Rechtsanwalt in Berlin und Wiesbaden 1993 – 1998. Professor für Öffentliches Recht an der Hochschule für Technik und Wirtschaft Berlin 1998 – 2014. Forschungsschwerpunkte u.a.: Digitalisierung des Rechts und E-Government. Zahlreiche Veröffentlichungen zu diesen Bereichen.

INHALTSVERZEICHNIS

I. E-GOVERNMENT 8

1. Grundlagen 8

1.1 Begriff und Funktionen des E-Government 8

1.2 Grundbausteine des E-Government 10

2. Verfassungsrechtliche Rahmenbedingungen des E-Governments 17

2.1 IT-Zusammenarbeit von Bund und Ländern (Art. 91c GG) 17

2.2 Grundrechtsschutz der Vertraulichkeit und Integrität Informationstechnischer Systeme 19

2.3 Grundrecht auf IT-Abwehr 23

2.4 Grundrecht auf IT-Einsatz - Die Pflicht zur barrierefreien Ausgestaltung staatlicher Internetangebote 25

2.5 E-Democracy 25

3. Einfachgesetzliche Vorgaben 28

3.1 Allgemeiner rechtlicher Rahmen 28

3.2 E-Government-Gesetz auf Bundesebene 29

3.3 E-Government-Gesetze der Länder 30

3.4 Das BSI-Gesetz 30

3.5 Das De-Mail-Gesetz: Vertrauen im E-Government 31

4. Grundzüge des elektronischen Verwaltungsverfahrens 32

4.1 Zugang zur elektronischen Kommunikation (§ 3a Abs. 1 VwVfG) 32

4.2 Elektronische Formen (§ 3a Abs. 2 VwVfG) 44

4.3 Elektronische Formate (§ 3a Abs. 3 VwVfG) 47

4.4 Elektronischer Verwaltungsakt (§ 37 VwVfG) 48

4.5 Elektronische Bekanntgabe (§ 41 VwVfG) 53

4.6 Elektronisches Verfahren über eine einheitliche Stelle (§ 71a VwVfG ff.) 64

II. IT-VERGABE 75

1. Vergaberecht im Überblick 75

1.1 Einführung 75

1.2 Systematik und Grundstrukturen des Vergaberechts 81

1.3 Grundprinzipien des Vergaberechts 93

1.4 Kernelemente eines prototypischen Vergabeverfahrens (am Beispiel einer Softwarebeschaffung) 101

1.5 Grundzüge des Vergaberechtsschutzes 106

2. Vergabebedürftigkeit von IT-Leistungen 114

2.1 Ausgangslage 115

2.2 Checkliste zur Vergabebedürftigkeit 115

2.3 Öffentlicher Auftraggeber 116
2.4 Finanzwirksame Maßnahme 117
2.5 Beschaffung von Waren- oder Dienstleistungen 118
2.6 Entgeltlicher Vertrag 123
2.7 Mit Unternehmen 124
2.8 Am Markt 127
3. Rechtskonformes IT-Vergabeverfahren 131
3.1 Ausgangslage 131
3.2 Checkliste zum rechtskonformen Vergabeverfahren 131
3.3 Nationale oder EU-weite Vergabe 133
3.4 Wahl der geeigneten Vergabeart 134
3.5 Rechtskonforme Leistungsbeschreibung, technische Anforderungen 136
3.6 Bekanntmachung und Informationsübermittlung 142
3.7 Angebotswertung und Zuschlag 143
4. Rechtsfragen der E-Vergabe 147
4.1 Begriff der E-Vergabe 147
4.2 Politische Vorgaben 147
4.3 Rechtsgrundlagen 148
4.4 Digitalisierung des Vergabeverfahrens 149
4.5 Maßstäbe der Vergaberechtskonformität 155

III. WIEDERHOLUNGSFRAGEN MIT MUSTERLÖSUNGEN 159

IV. SCHLÜSSELWORTVERZEICHNIS 187

V. AUSGEWÄHLTE ENTSCHEIDUNGEN 200

VI. HINWEIS AUF INTERNETADRESSEN 203

VII. LITERATUR: 205

KAPITEL I:
E-GOVERNMENT

Lernergebnisse des Kapitels

Die Studierenden sollen

- sich das Verhältnis von Verwaltungsmodernisierung und Einsatz neuer Medien in der öffentlichen Verwaltung bewusst machen;
- die maßgeblichen Rechtsgrundlagen des sog. elektronischen Verwaltungsverfahrens kennenlernen und diese sachadäquat anzuwenden lernen;
- ein Problembewusstsein für solche Rechtsfragen entwickeln, die sich aus dem IT-Einsatz im Verwaltungsverfahren ergeben;
- sich mit den wesentlichen technologischen Aspekten vertraut machen, die zu einer Neuorganisation der öffentlichen Verwaltung durch die deutsche und europäische IT-Politik führen.

I. E-GOVERNMENT

1. Grundlagen

Hinweis: Die nachstehenden Ausführungen stellen eine in der systematischen Darstellung stark gekürzte und um Beispiele, Schlüsselbegriffe und Wiederholungsfragen erweiterte Fassung des Kapitels „E-Government“ in *Heckmann*, juris Praxiskommentar Internetrecht, 2. Aufl. 2009, dar. Für vertiefte Informationen sei die Lektüre der erweiterten Kommentierung empfohlen.

1.1 Begriff und Funktionen des E-Government

Electronic Government ist inzwischen ein weit verbreitetes, globales Phänomen – und ein in allen Industriestaaten akzeptiertes Leitbild. Der verstärkte Einsatz von Informations- und Kommunikationstechnologie wird als Instrument gesehen, ein besseres Regieren und Verwalten zu ermöglichen.

E-Government lässt sich als Abwicklung geschäftlicher Prozesse im Zusammenhang mit Regieren und Verwalten (Government) mit Hilfe von Informations- und Kommunikationstechniken über elektronische Medien definieren. Es umfasst damit alle Aspekte des Regierens und Verwaltens (z.B. öffentliche Willensbildung, Entscheidungsfindung, Leistungserstellung und -erbringung, Partizipation usw.) solange und soweit sie durch IuK-Technologien unterstützt werden können. Darüber hinaus muss E-Government auch als Bestandteil einer umfassenden Verwaltungsmodernisierung gesehen werden. Denn Technik- und Medieneinsatz alleine machen die Verwaltung nicht „modern“, lösen nicht automatisch Effizienz-, Akzeptanz- und Kapazitätsprobleme. Die Entwicklung technischer Lösungen kann Probleme aber sichtbar machen, besonders wenn es um komplexe Zusammenhänge geht. Dann ist E-Government ein Motor der Verwaltungsmodernisierung, mag der vermeintliche Zwang zur multimedialen Hochrüstung der Verwaltung Impulse auch und gerade für die konventionelle Verwaltungsreform geben. Technische und administrative Innovation können sich gegenseitig befruchten. Diese Mischform von E-Government kann man als Blended Government bezeichnen. Blended Government erschöpft sich nicht in der simplen Verbindung von realen Verwaltungsvorgängen mit webbasierten Dienstleistungen. Darüber hinausgehend geht es um die Entwicklung des Gesamtkonzeptes eines interaktiven, service- und bürgerorientierten Dienstleistungsstaates, in dem der Bürger als Kunde der Verwaltung optimal bedient wird. Das kann in dem einen Fall mittels moderner Informations- und Kommunikationstechnik geschehen, in einem anderen Fall auch auf traditionelle Weise, nicht selten auch in kombinierter Weise, je nach Bedürfnissen, Ressourcen, Erwartungshaltung der Bürger und eigenem Anspruch der Behörde.

In Deutschland kommunizieren und arbeiten inzwischen alle Bereiche der Verwaltung – Bundesverwaltung, Landesverwaltung, Kommunalverwaltung – online, wenn auch in sehr unterschiedlichen Ausmaßen. Das erste E-Government-Gesetz Deutschlands in Schleswig-Holstein hat die vorstehenden Reformgedanken aufge-

nommen. Dort ist der Begriff E-Government (in § 2 Nr. 1 E-GovG SH) wie folgt definiert: „E-Government ist der Einsatz moderner Informations- und Kommunikationstechnik (IT) in öffentlichen Verwaltungen in Verbindung mit organisatorischen Veränderungen in den Geschäftsprozessen der öffentlichen Verwaltung zur Durchführung von Informations-, Kommunikations- und Transaktionsprozessen innerhalb und zwischen staatlichen Institutionen sowie zwischen diesen Institutionen und Bürgern bzw. Unternehmen." Eines der neuesten Gesetze zum Thema E-Government ist das Sächsische E-Government Gesetz (SächEGovG), das am 9. Juli 2014 verabschiedet wurde und die öffentlich-rechtliche Verwaltungstätigkeit elektronisch unterstützen soll.

Systematisch lassen sich mindestens drei Ebenen des Electronic Government unterscheiden. Es betrifft das Verhältnis der Verwaltung zum Bürger (Administration to Citizen-Electronic Commerce), die Beziehung der Verwaltung zur Wirtschaft (Administration to Business-Electronic Commerce) und die Vernetzung der einzelnen Verwaltungen untereinander (Administration to Administration-Electronic Commerce).

Der A2C-Electronic Commerce wird vom Leitbild der virtuellen Behörde geprägt. Der Bürger kann mit einer Behörde über das Internet online kommunizieren und behördliche Serviceleistungen über das Internet in Anspruch nehmen: Dienstleistungen der Verwaltung werden dabei on demand erbracht. Beispiele dafür sind: melderechtliche An- und Abmeldungen per E-Mail, die elektronische Steuererklärung (ELSTER) und die elektronische Antragstellung bei der Bundesversicherungsanstalt für Angestellte.

Seit Ende 1999 hat die Bundesregierung im Rahmen des Programms „Bund ONLINE 2005" die Bundesverwaltung sehr weit gehend virtualisiert. Alle internetfähigen Dienstleistungen der Bundesverwaltung stehen online bereit und können zu großen Teilen über das Netz abgewickelt werden. Unter dem Etikett „E-Government 2.0" arbeitet die Bundesverwaltung an einer weiteren Verbesserung ihres Online-Betriebs. Das Kernstück ist bisher das Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz - EGovG), das im August 2013 in Kraft getreten ist. Auch die Landesbehörden und die Kommunen sind zunehmend online für die Bürger erreichbar – allerdings in sehr unterschiedlichem Ausmaß und durchaus mit großen Qualitätsunterschieden

Inzwischen entwickelt sich eine spezielle Spielart des E-Government: das Mobile Government. Sie umfasst zwei Aspekte. Einmal geht es um den mobilen Zugang zur Verwaltung. Dabei soll Mobilkommunikation als zusätzlicher Zugangskanal der Bürger zur Verwaltung genutzt werden. In seinen Auswirkungen deutlich weiter reicht die zweite Dimension dieser Entwicklung: die Vision der mobilisierten Verwaltung. Sie kann die Leistungsfähigkeit der Verwaltung verbessern. Gleichzeitig wird sie aber die Strukturen der Verwaltungsorganisation verändern und rechtlichen Gestaltungsbedarf schaffen.

Nicht nur das Verhältnis der Verwaltung zum Bürger, sondern auch die Beziehungen zwischen Verwaltung und Wirtschaft werden virtualisiert. Ein strategisches Ziel des E-Government ist, gemeinsame elektronische Prozessketten zwi-

schen Unternehmen und Behörden aufzubauen. Die Schnittstelle zwischen Staat und Wirtschaft birgt ungenutzte Effizienzpotenziale. Sie könnten realisiert werden, wenn Behörden und Unternehmen integrierte Geschäftsabläufe etablieren und interoperable IT-Systeme benutzen. Anwendungsbeispiele wären etwa die Statistikmeldungen der Unternehmen und die Zoll- und Sicherheitskontrollen der Zoll-, Güterverkehrs- und Gesundheitsbehörden.

A2B-Electronic Commerce ist besonders weit fortgeschritten im Bereich der Vergabe öffentlicher Aufträge. Die elektronische Auftragsvergabe gilt als Schlüsselanwendung im Electronic Government. Das öffentliche Auftragsvergabeverfahren ist besonders gut für den Einsatz von IuK-Technologien geeignet. Sowohl im europäischen Recht als auch auf nationaler Ebene sind die rechtlichen Voraussetzungen für eine elektronische – im Idealfall medienbruchfreie – Auftragsvergabe der öffentlichen Hand geschaffen worden. Eine ganze Reihe von Bundesländern und Kommunen praktiziert die Vergabe öffentlicher Aufträge über das Internet. Der Bund betreibt eine zentrale elektronische Vergabeplattform, über die er seine Aufträge ausschreibt und Beschaffungen durchführt.

Mit der Vernetzung der Verwaltungen im In- und Ausland untereinander – dem A2A-Electronic Commerce – entwickelt sich ein – potenziell weltweites – Intranet der Verwaltungen. Eine Vorreiterrolle im nationalen Rahmen nehmen die Umweltbehörden der Bundesländer ein, die seit Anfang der neunziger Jahre eine Reihe von behörden- und länderübergreifenden Umweltinformationssystemen aufgebaut haben. Ein Beispiel für die beginnende Herausbildung eines Intranets, das die nationalen Staatsgrenzen überschreitet, ist die Vernetzung von Staats- und Regierungskanzleien in Deutschland, Österreich und der Schweiz. Auch auf kommunaler Ebene sind inzwischen unterschiedlichste Vernetzungen entstanden, die der interkommunalen Zusammenarbeit eine elektronische Dimension hinzufügen.

Schlüsselwörter:

Verwaltungsmodernisierung, Blended Government, interaktiver, service- und bürgerorientierter Dienstleistungsstaat, Grundbausteine der E-Government-Lösungen: Information, Kommunikation, Transaktion, (Re-) Organisation der zuständigen Verwaltungseinheiten

1.2 Grundbausteine des E-Government

Der Einsatz von IuK-Technik verändert die Verwaltung in vielerlei Beziehungen. Die organisatorischen, technischen, personellen, finanziellen und nicht zuletzt rechtlichen Veränderungen des Verwaltungsraums, die mit der Etablierung von E-Government-Projekten in Verbindung stehen, sind enorm. Anknüpfungspunkt der tiefgreifenden Reformbestrebungen sind die typischen Zielsetzungen und Grundbausteine von E-Government-Lösungen: **Information** (als einseitige Leistung der Verwaltung), **Kommunikation** (als Möglichkeit des Informationsaustausches), **Transaktion** (als Form der Abwicklung rechtlich bindender Vorgänge über das Internet) und **(Re-)Organisation** der zuständigen Verwaltungseinheiten.

1.2.1. Information

Bisher bedeutsamstes Potential des Einsatzes moderner Medien in der Verwaltung ist die Verbesserung der **Bürgerinformationen über Internet Portale**, sei es durch Angaben über Aufgaben, Zuständigkeiten, einzelne Verwaltungsverfahren oder das zur Verfügungstellen von Rechtsvorschriften. Derartige Angebote bestehen mittlerweile flächendeckend bei nahezu allen Verwaltungseinheiten auf Bundes-, Landes- und Kommunalebene. Insoweit ist die **Transparenz** der Verwaltung wesentlich verbessert worden, wobei allerdings in der Benutzerfreundlichkeit und der sinnvollen Ausgestaltung der unterschiedlichen Portale erhebliche Qualitätsunterschiede bestehen.

Schlüsselwörter:

Bürgerinformation über Internet Portale, Transparenz

1.2.2 Kommunikation

Die Kommunikationsmöglichkeiten des Internet (E-Mail, Chats, Foren u.a.) werden zunehmend von der Verwaltung ausgeschöpft, wobei zunehmend auch web 2.0-Technologien zum Einsatz kommen. Verwaltungsintern unterfällt der Gebrauch neuer Medien dabei im Wesentlichen den allgemeinen Regelungen. D.h. hinsichtlich der Fragen der privaten und dienstlichen Internetnutzung der Angestellten und Beamten, den Kontroll- und Überwachungsmöglichkeiten des Dienstherren, aber auch der notwendigen Maßnahmen zur IT-Sicherheit und zum Datenschutz bestehen keine tiefgreifenden Unterschiede zu deren Behandlung beim Tätigwerden privater Organisationen. Verwaltungsextern wird die Kommunikation zwischen Bürger und Behörde insbesondere durch die Regelungen zur elektronischen Kommunikation in den Verwaltungsverfahrensgesetzen des Bundes und der Länder (§ 3a VwVfG) gesteuert. Als Kommunikationsmedium wird bisher nahezu ausschließlich E-Mail genutzt. Eine Kommunikation über Behördenportale ist dagegen nur teilweise etabliert (so aber z.B. das Hamburg-Gateway). In naher Zukunft werden indes neue innovative Strukturen mit den sog. Bürgerportaldiensten geschaffen, deren rechtlicher Rahmen sich gerade im Gesetzgebungsprozess befindet.

Schlüsselwörter:

private und dienstliche Internetnutzung, Verwaltungsverfahrensgesetze, Behördenportal

1.2.3 Transaktion

Die Abwicklung rechtlich bindender Vorgänge über das Internet erfolgt bisher nur in geringem Umfang. Die Verwaltung ist zwar online, aber sie ist noch nicht wirklich vernetzt. So gibt es bislang nur wenig funktionierende, komfortable Portallösungen. Zum anderen fehlt es vielfach auch an der Verknüpfung der Internetdienstleistungen mit den realen Verwaltungsabläufen. So kann es durchaus Sinn machen, einzelne Stationen eines Genehmigungsverfahrens zu digitalisieren, auch wenn das gesamte Verfahren noch nicht online abgewickelt werden kann. Freilich stehen dem teils auch bindende Zuständigkeitsregelungen und eine ge-

wisse organisatorische Zersplitterung der Verwaltungseinheiten entgegen, die durch eine behutsame Reorganisation von Teilen der öffentlichen Verwaltung erst behoben werden muss.

Freilich stehen dem teils auch bindende Zuständigkeitsregelungen und eine gewisse **organisatorische Zersplitterung der Verwaltungseinheiten** entgegen, die nicht nur durch eine behutsame Reorganisation von Teilen der öffentlichen Verwaltung behoben werden können. Wesentliche Wachstums- und Servicepotentiale lassen sich im nationalen E-Government (unter Einbindung aller Verwaltungsebenen) durch eine Abstimmung von **Standards** und **Interoperabilität** erreichen. Aufgrund der „Kleinteiligkeit" der bisherigen E-Government-Aktivitäten (Entwicklung von „Insellösungen") von Ländern und Kommunen fehlt es in vielen Verwaltungsbereichen an der Möglichkeit, medienbruchfrei und effektiv mit anderen Behörden zu interagieren, sodass die (freiwillige und kooperative) **Einigung** auf Standards zur Sicherung der Interoperabilität (und zur erforderlichen IT-Sicherheit) die vordringlichste Aufgabe der nächsten Jahre sein wird.

Die Reform des **elektronischen Verwaltungsverfahrens** hat neue Transaktionsfelder eröffnet. Mit der rechtlichen Ausgestaltung der elektronischen Kommunikation kann etwa der Erlass elektronischer Verwaltungsakte rechtssicher bewerkstelligt werden. Praktisches Hemmnis ist dabei allerdings nach wie vor das Erfordernis einer qualifizierten elektronischen Signatur bei Verwaltungsakten, für die die Schriftform angeordnet ist (vgl. § 3a Abs. 2 VwVfG). Denn es ist nicht absehbar, dass sich der Einsatz der Signaturtechnik in der Praxis auch auf längere Sicht etablieren könnte. Für die Zukunft sind – auch in (teilweiser) Ersetzung qualifizierter elektronischer Signaturen – neue rechtssichere Authentifizierungsmodi in virtuellen Umgebungen auszuloten. Dabei stellt insbesondere die sichere Identifizierung des Bürgers beim Erstkontakt mit der Verwaltung ein erhebliches Problem dar. Dem technikgestützten Identitätsmanagement könnte dabei mit der Verbreitung des **elektronischen Personalausweises** (als „Massenanwendung") zum Durchbruch verholfen werden. Dieser stellt demnach auch einen wesentlichen Baustein in den Überlegungen zur sicheren Online-Kommunikation auf Bürgerportalen mittels **De-Mail** dar und könnte auch im Rahmen eines föderal strukturierten Identitätsmanagements (z.B. Deutschland-Online-Projekt S.A.F.E.) zur Authentifizierung in E-Government und E-Justice-Anwendungen genutzt werden. Sein Einsatz kommt nahezu in allen Identifizierungsstrukturen in Betracht, etwa im Zusammenhang mit der elektronischen Gesundheitskarte, dem elektronischen Einkommensnachweis (ELENA) oder im anvisierten Bundesmelderegister. In diesem Kontext ist der sogenannte elektronische Identitätsausweis (§ 10 PAuswG) eine maßgebliche Funktion des elektronischen Personalausweises. Die Verwendung dieser Nutzer-ID ist freiwillig und wird im Falle der Ablehnung des Bürgers ausgeschaltet. Zusätzlich wird der elektronische Personalausweis als sichere Signaturerstellung ausgestaltet (§ 22 PAuswG) und bietet damit (was allerdings für den Bürger mit zusätzlichen Kosten verbunden ist) die Möglichkeit, qualifizierte elektronische Signaturen zu erzeugen.

Eine nicht zu unterschätzende Schubwirkung hat das nationale E-Government aufgrund gemeinschaftsrechtlichen Anpassungsdrucks erhalten. Die **EU-Dienstleistungsrichtlinie (DLRL)**, die eigentlich bis Ende 2009 in nationales Recht hätte umgesetzt werden müssen, greift in bislang kaum bekanntem Ausmaß in das Verfahrensrecht der Mitgliedsstaaten ein. Gem. Art. 6 Abs. 1 DLRL müssen Dienstleister bei einem sogenannten einheitlichen Ansprechpartner (EA) alle Verfahren und Formalitäten erledigen können, die für die Erbringung ihrer Dienstleistung im Bestimmungsland erforderlich sind, und das „auf Wunsch" **vollständig in elektronischer Form**, Art. 8 DLRL. Insoweit haben sich die Verwaltungen der Herausforderung zu stellen, im nationalen föderal zersplitterten Verwaltungsraum Verwaltungsverfahren mit medienbruchfreier elektronischer Transaktion zu implementieren. Vor dem Hintergrund der bestehenden Kompetenzordnung werden mit Umsetzung der Richtlinie die einheitlichen Ansprechpartner zum Knotenpunkt einer umfassenden, Ebenen übergreifenden elektronischen Vernetzung der beteiligten Behörden. Insoweit müssen Maßnahmen der Verwaltungsmodernisierung erfolgen, die bislang eher stockend realisiert wurden. Schlagworte und Konzepte, wie „One-Shop-Government", Dienstleistungscenter, „Front-Office/Back-Office-Strukturen", Orientierung an Lebenslagen der Verwaltungskunden usw. sind erfolgreich in die nationale Verwaltungskultur zu integrieren. Ob dies zeitnah gelingt, kann kaum prognostiziert werden. Zwar wurden die allgemeinen verwaltungsverfahrens-rechtlichen Anforderungen der DLRL mit dem 4. VwVfÄndG, die teils noch in die entsprechenden Landesgesetze zu transferieren sind, umgesetzt, sodass insoweit eine beachtliche Restrukturierungsmaßnahme im deutschen Verfahrensrecht greift: Mit dem einheitlichen Ansprechpartner fungiert künftig eine Stelle, die dem One-Stop-Shop-Gedanken gerecht werden muss. Die Vermittlungsfunktion der Ansprechpartner ist aber nur realisierbar, wenn eine interoperable und leistungsfähige Vernetzung zu den zuständigen Stellen geschaffen wird, was bisher in noch nicht ausreichendem Umfang bewerkstelligt wurde.

Die verwaltungsorganisationsrechtliche Verortung der als **einheitliche Ansprechpartner (EA)** zuständigen Stellen obliegt den Ländern, wobei deren Lösungen recht unterschiedlich sind. Diese reichen von der Ansiedelung des EA auf kommunaler Ebene (Kommunalmodell), über verschiedene Varianten des so genannten Wirtschaftskammermodells (Industrie- und Handelskammern sowie Handwerkskammern als EA), die Allkammerlösung (Industrie- und Handelskammern, Handwerkskammern und Kammern der freien Berufe als EA), das Mittelbehördenmodell (Landesmittelbehörden als EA) bis hin zu Kooperationsmodellen zwischen Kommunen und Kammern. Ebenfalls mögliche rein privatwirtschaftliche Modelle wurden indes – aus wenig nachvollziehbaren Gründen – bislang nicht aufgegriffen. Die erforderlichen technisch-organisatorischen Rahmenbedingungen werden von dem Projektauftrag „Deutschland Online Dienstleistungsrichtlinie" erarbeitet, wobei hinsichtlich Standardisierungsfragen die Grundgesetzänderung in Art. 91c GG Erleichterung in der praktischen Umsetzung bringen kann. Die Chance, im Rahmen der Umsetzung der DLRL eine an der Etablierung effektiver E-Governmentstrukturen ausgerichtete grundlegende Verwaltungsreform voranzutreiben (was nahe gelegen hätte), scheint indes vertan. Zum einen wur-

den bislang Genehmigungsverfahren nicht nennenswert vereinfacht. Zum anderen wird weiter an der qualifizierten digitalen Signatur zur Ersetzung der Schriftform festgehalten.

Schlüsselwörter:

Portallösungen, Standards, Interoperabilität, elektronisches Verwaltungsverfahren, elektronischer Personalausweis, De-Mail, EU-Dienstleistungsrichtlinie, Einheitlicher Ansprechpartner

1.2.4 (Re-)Organisation

Gute E-Government-Anwendungen beschränken sich nicht auf den Einsatz moderner Kommunikationstechniken, mit denen bestehende Verwaltungsabläufe abgebildet werden. Vielmehr erfordert die Integration benutzerfreundlicher Anwendungen oftmals eine Neudefinition der Organisation, der Struktur, der Abläufe und der Prozesse der Verwaltung selbst (E-Government als Triebkraft der Verwaltungsmodernisierung). Medienbruchfreie Portallösungen, die dem Gedanken des **One-Stop-Government** bzw. dem sog. „**Lebenslagenkonzept**“ verhaftet sind, sind in ihrer konsequenten Umsetzung oftmals mit der überkommenen Zuständigkeitsordnung der einzelnen Verwaltungsträger nicht vereinbar. Hier gilt es weiter nach neuen innovativen Modellen zu suchen, die mit der bestehenden Rechtsordnung in Einklang gebracht werden können.

Ohne eine von allen Behörden beachtete und gegenseitig anerkannte Zuständigkeitsordnung wären widerspruchsfreie und verbindliche Verwaltungsentscheidungen (gleichsam das gesellschaftlich relevante Produkt der Verwaltungstätigkeit) nicht möglich. Dennoch bietet sich eine behutsame Anpassung an die geänderten technischen Rahmenbedingungen an. In Zeiten webbasierter E-Government-Lösungen erscheint das nahe gelegene Rathaus nicht mehr als zwingender Zuständigkeitsfaktor. Wenn man Verwaltungsvorgänge vom heimischen PC aus betreiben kann, mag es wichtiger sein, überhaupt eine schnelle, maßgerechte Entscheidung zu erhalten, als dass diese vor Ort getroffen werden müsste. Im virtuellen Verwaltungsraum sind Regelungen zur Zuständigkeit eher hinderlich. In letzter Konsequenz müsste eine virtuelle Verwaltung gar die vollständige Loslösung von ortsabhängigen Organisationen bedeuten, die nach außen mit einer zentralen Organisationseinheit auftritt. Eine Art **Verwaltungscallcenter** könnte dann eine einheitliche Anlaufstelle des Bürgers für alle Verwaltungsangelegenheiten bilden.

Teils mag dabei auch die Änderung überkommener Zuständigkeitsvorschriften notwendig sein sowie eine Anpassung an neue Abläufe und Organisationen, die nicht unter dem geltenden Recht entwickelt wurden, sondern aus ökonomischen Erwägungen unter Berücksichtigung technologischer Machbarkeit ins Spiel gebracht werden. Freilich müssen sich diese innerhalb der Zuständigkeits- und Kompetenzordnung des föderativen Systems der Bundesrepublik Deutschland bewegen. Einer völligen Neuordnung der Zuständigkeiten ohne Gebietsbezug – wie teils gefordert – ist nicht notwendig. Es lassen sich auch **neue Kooperationsinstrumente** entwickeln, die bei gleichzeitig klarer gesetzlicher Grenzziehung für Kooperationen, die Verantwortlichkeiten sowie Geheimhaltung und Datenschutz gewährleisten.

Die Trennung der Verwaltungsräume von Bund und Ländern, aber auch die Gewährleistung der Selbstverwaltungsrechte gegenüber der mittelbaren Staatsverwaltung zeigen den (potentiellen) Bemühungen um eine „universelle“ Vereinheitlichung bestimmte Grenzen, jedenfalls aber bedenkenswerte Herausforderungen, auf. Werden auch mittels innovativer E-Government-Applikationen (örtliche) Zuständigkeitsregelungen nicht vollends aufgehoben werden können, so sind zielführende **E-Government-Kooperationen** zwischen einzelnen Verwaltungsträgern unumgänglich. Hierfür müssen vor allem **einheitliche technische und organisatorische** (z.B. Nutzung gemeinsamer Datenpools usw.) **Standards** geschaffen werden, wozu nun in Art. 91c GG die verfassungsrechtlichen Grundlagen geschaffen wurden.

Schlüsselwörter:

Integration benutzerfreundlicher Anwendungen, Motor der Verwaltungsmodernisierung, One-Stop-Government, Lebenslagenkonzept, Zuständigkeitsordnung, virtueller Verwaltungsraum

1.2.5 Exkurs: Die Einbindung Privater in die öffentliche Aufgabenerfüllung – IT-Outsourcing

Eine virtuelle Verwaltungswelt lässt sich ohne das Instrument des IT-Outsourcing kaum verwirklichen. Die Beteiligung privater Dienstleister, insbesondere an der technischen Vorbereitung und Abwicklung von Verwaltungsvorgängen, ist angesichts deren **spezifischen Know-hows** und auch der mit der Einschaltung Privater verbundenen **Entlastungsmöglichkeiten der öffentlichen Haushalte** vielfach notwendig. Outsourcing bedeutet dabei die vollständige oder teilweise Auslagerung einer definierten Ressource wie der Informationsverarbeitung an ein externes Unternehmen.

Outsourcingfähige Tätigkeiten im Rahmen der Informationsverarbeitung der öffentlichen Verwaltung reichen von der Planung der Informationstechnikleistung (IT-Leistung), der Ressourcenbeschaffung (Hard- und Software, Personal und Know-how) über den Betrieb von Rechenzentren, Netzen, Recovery-Services, Wartung, Facilities und Systemmanagement bis zur Haustechnik. Insbesondere Netz-Dienstleistungen, wie die Betriebssystempflege, das Operating, Bereitstellung von Datenbanksystemen und Tools, der Übernahme, Pflege und Entwicklung von Anwendungssoftware bis zur Datensicherung, Wiederanlaufplanung, Systemdokumentation und nicht zuletzt auch ganze Datenverarbeitungsvorgänge werden mittlerweile von privaten Dienstleistern für die Verwaltung wahrgenommen.

Dabei sind die Grenzen der Einsatzmöglichkeiten privater Dienstleister bisher kaum trennscharf ausgelotet. Obwohl diese Rechtsfragen zunehmend Bedeutung bekommen, nachdem private Organisationen zunehmend in die **Vorbereitung hoheitlicher Verwaltungsentscheidungen** einbezogen werden; häufig in Daten verarbeitende Funktion und im Zusammenhang mit der Umsetzung von E-Government-Projekten.

Den maßgeblichen **verfassungsrechtlichen Rahmen** bildet diesbezüglich **Art. 33 Abs. 4 GG**. Die Vorschrift enthält nicht nur eine institutionelle Garantie des Be-

rufsbeamtentums, sondern ist auch freiheitssichernde Strukturvorgabe gegen einen zu weitgehenden Rückzug des Staates aus seiner Verantwortung zu eigener Aufgabenwahrnehmung. Ein nach Art. 33 Abs. 4 GG den Beamten vorbehaltener Aufgabenbereich darf nicht aus dem staatlichen Organisationszusammenhang ausgelagert werden. Handelt es sich um die *„Ausübung hoheitsrechtlicher Befugnisse"* besteht aufgrund der organisationsrechtlichen Sperrwirkung des Art. 33 Abs. 4 GG keine Möglichkeit einer privatberuflichen oder gewerblichen Betätigung. Zunehmend wird Art. 33 Abs. 4 GG extensiv interpretiert. Von der Ausübung hoheitsrechtlicher Befugnisse sei danach die Wahrnehmung *bloßer technischer Hilfsfunktionen* bei der staatlichen Aufgabenerfüllung ausgenommen. Diese ist von einer hoheitsrechtlichen eigenverantwortlichen Aufgabenwahrnehmung abzugrenzen. Während technisch geprägte Hilfstätigkeiten, die eine eigene Entscheidung nicht oder lediglich in unerheblichem Umfang erfordern, in ihrer Ausübung nicht Beamten vorbehalten bleiben müssen, ist dies zwingend erforderlich, wenn die betreffende Tätigkeit dergestalt in den administrativen Entscheidungsprozess eingebunden ist, dass sie inhaltlich auf den außenwirksamen Akt Einfluss nimmt. Maßgeblich für die Grenzziehung, welche Funktionen Privaten als Hilfstätigkeit übertragen werden können und welche Aufgaben zwingend durch den Staat selbst wahrgenommen werden müssen, ist demnach der Umfang der Entscheidungsbefugnis über hoheitliche Aufgaben. Diese Abgrenzung läuft parallel zur Differenzierung zwischen einer **Auftragsdatenverarbeitung** und einer sog. **Funktionsübertragung** nach den Datenschutzgesetzen des Bundes und der Länder.

Nach überwiegender Ansicht liegt eine **Auftragsdatenverarbeitung** vor, wenn dem Auftragnehmer die Entscheidungsbefugnis über die Daten fehlt und er bei der Verarbeitung unselbstständig tätig und den Weisungen des Auftraggebers unterworfen ist; der Auftragnehmer in vollständiger Abhängigkeit hinsichtlich der Art und des Umgangs und nach den Vorgaben des Auftraggebers die Daten erhebt und/oder verwendet, gleichsam als „verlängerter Arm" für den Auftraggeber mit den Daten umgeht, nur Hilfs- bzw. Unterstützungsfunktionen ausübt; sich der Auftragsschwerpunkt in erster Linie auf die technische Durchführung der Datenverarbeitung richtet.

Eine **Funktionsübertragung** ist dagegen anzunehmen, wenn dem Auftragnehmer eigene Entscheidungsbefugnisse hinsichtlich des „wie" und der Auswahl der Daten zustehen. Er erledigt bei der Funktionsübertragung die ihm übertragene Aufgabe selbstständig und der Auftraggeber kann auf die Verarbeitung nicht mehr ohne weiteres durch Weisungen Einfluss nehmen; eine Übertragung der zu Grunde liegenden Aufgabe auf den Dienstleister erfolgt; eine Dienstleistung erbracht wird, die über die weisungsabhängige technische Datenverarbeitung hinausgeht; dem Dienstleister Rechte zur Nutzung an den Daten für eigene Zwecke überlassen sind und er ein eigenes Interesse an der Datenverwendung hat.

Rechtliche Unsicherheiten bei der Vertragsgestaltung bestehen kaum mehr. **Outsourcingverträge** sind in der staatlichen Verwaltung kein Novum; eine umfassende rechtliche Beleuchtung ist bereits erfolgt. Dabei können auch die staatlichen Aufsichtsbehörden bei der Vertragsgestaltung und Kontrolle ihren Pflichten problemlos

nachkommen und ihren Beitrag etwa in der Erarbeitung von Musterverträgen leisten, wie dies in anderen Verwaltungsbereichen auch häufig der Fall ist.

Schlüsselwörter:

IT-Outsourcing, Vorbereitung hoheitlicher Verwaltungsentscheidungen, Ausübung hoheitsrechtlicher Befugnisse, Funktionsübertragung, technische Hilfsfunktionen, Auftragsdatenverarbeitung, Entscheidungsbefugnis, Outsourcing-Vertrag

Aufgaben zur Lernkontrolle:

1. *Warum reicht es nicht aus, E-Government allein unter rein technischen Gesichtspunkten zu beurteilen?*
2. *Was sind die Grundbausteine von E-Government-Lösungen? Was ist darunter zu verstehen?*
3. *Was ist unter IT-Outsourcing zu verstehen und welche rechtlichen Probleme stellen sich hierbei?*

2. Verfassungsrechtliche Rahmenbedingungen des E-Governments

2.1 IT-Zusammenarbeit von Bund und Ländern (Art. 91c GG)

Die Harmonisierung und die Schaffung von Interoperabilität im IT-Bereich sind im föderalen Gefüge der Bundesrepublik wesentliche Erfolgsfaktoren einer modernen elektronischen Verwaltung. Allerdings sind die bisherigen Versuche föderaler IT-Steuerung gescheitert, wie der bestehende „IT-Flickenteppich“ verdeutlicht. Insoweit ist eine neue, Ebenen übergreifende IT-Steuerung erforderlich, die die Handlungsfähigkeit des Gesamtstaates stärkt, einheitliche Lebensverhältnisse ermöglicht und die Wettbewerbsfähigkeit Deutschlands im europäischen Vergleich steigert. Dem kam der Gesetzgeber im Rahmen der sog. **Föderalismusreform II** nach, indem er die IT-Zusammenarbeit von Bund und Ländern in Art. 91c GG einer verfassungsrechtlichen Regelung zugeführt hat. Danach können „Bund und Länder […] bei der Planung, der Errichtung und dem Betrieb informationstechnischer Systeme zusammenwirken“. Als konkretisierende Rechtsgrundlage dienen **staatsvertragliche Vereinbarungen** über die für die Kommunikation zwischen ihren IT-Systemen notwendigen Standards und Sicherheitsanforderungen (Art. 91c Abs. 2 GG). Diese Legitimation der IT-Zusammenarbeit zwischen Bund und Ländern war sinnvoll und verfassungsrechtlich notwendig. Sie erfüllt die Anforderungen an eine zulässige Mischverwaltung, die das BVerfG präzisiert hat (BVerfGE 119, 331 – ARGE – Hartz IV). Dahinter steckt ein zustimmungswürdiges IT-Steuerungskonzept für den virtuellen Verwaltungsraum Deutschland, das einen Ausweg aus dem Dilemma von technisch notwendiger Einheit und rechtlich notwendiger Vielfalt zeigen kann.

In Art. 91c Abs. 1 GG ist eine allgemeine Zusammenarbeit von Bund und Ländern bei der Planung, Einrichtung und dem Betrieb der für die Aufgabenerfüllung benötigten informationstechnischen Systeme vorgesehen (quasi als Grundlage eines **kooperativen IT-Staates**). Die Norm ist äußerst weit gefasst. Mit der Bezugnahme auf die Planung, Errichtung und den Betrieb informationstechnischer Systeme umfasst Art. 91c Abs. 1 GG seinem Wortlaut nach jegliche Hard- und Software im Verwaltungsgebrauch. Auf die Spitze getrieben würde im Ergebnis jede Anschaffung eines neuen Rechners oder die Implementierung eines Fachverfahrens in einer Kreisverwaltungsbehörde der Zusammenarbeit des Art. 91c Abs. 1 GG unterfallen. Dass dadurch die von Art. 79 Abs. 3 GG garantierte Eigenstaatlichkeit der Länder unzulässig beeinträchtigt werden könnte, liegt auf der Hand. Insoweit ist eine erkennbar einschränkende Auslegung von Art. 91c Abs. 1 GG geboten. Rückschlüsse dafür lassen sich aus Art. 91c Abs. 2 GG folgern. Denn die Zusammenarbeit von Bund und Ländern gemäß Art. 91c Abs. 2 GG ist inhaltlich eng begrenzt. Die Norm kann nur so verstanden werden, dass Bund und Länder die für die Ebenen übergreifende Kommunikation **zwingend erforderlichen Interoperabilitäts- und Sicherheitsstandards** mittels Staatsvertrag festlegen können. Das ergibt sich bereits aus dem Wortlaut des Art. 91c Abs. 2 GG in Formulierungen wie „zwischen“ ihren Systemen und „notwendige“ Standards und Sicherheitsanforderungen. Nach den ursprünglichen Beratungen und auch dem ausfüllenden Staatsvertrag (§ 3 Abs. 1) soll der Fokus auf einheitlichen verbindlichen Schnittstellenstandards auf der Basis von Marktstandards liegen. Es ist also nur eine sehr beschränkte IT-(Mindest-)Abstimmung in Art. 91c Abs. 2 GG vorgesehen, nämlich die Festlegung bestimmter, zur Interoperabilität zwingend erforderlicher (keineswegs aller) Kommunikationsstandards. Erfasst werden nur solche IT-Standards, die der Kommunikation „zwischen“ den IT-Systemen dienen, also nicht darüber hinaus gehende Technologievorgaben, selbst wenn sie im Sinne einer Harmonisierung und zentralen IT-Steuerung des IT-Betriebs „notwendig“ erscheinen mögen. Auch sind mit „Sicherheitsanforderungen“ nur solche Vorkehrungen gemeint, die die Ebenen über-greifende Kommunikation gegen Angriffe und systemimmanente Schwachstellen stärken. Eine Kompetenz zur umfassenden Schaffung von IT-Sicherheit beinhaltet die Vorschrift dagegen aufgrund der eindeutigen Begrenzung auf die Kommunikationsschnittstellen („Interoperabilität“) nicht. Damit gibt die Regelung des Art. 91c Abs. 2 GG als „Konkretisierung des Zusammenwirkens“ von Bund und Ländern nach Art. 91c Abs. 1 GG zu erkennen, dass ausschließlich eine partielle IT-Abstimmung ermöglicht werden soll, die auf „technische Notwendigkeiten“ begrenzt sein muss und inhaltliche Regelungsmaterien der Länder möglichst nicht erfassen soll.

Zur weiteren Umsetzung des neuen Art. 91c GG haben der Bund und die Länder einen Staatsvertrags geschlossen. Er regelt im Wesentlichen die Einrichtung, Arbeitsweise und Entscheidungsmodalitäten eines **gemeinsamen IT-Planungsrates**, beschreibt die Regelungen zur Festlegung von IT-Interoperabilitätsstandards und IT-Sicherheitsstandards durch den IT-Planungsrat und seine Aufgaben im Bereich des Verbindungsnetzes.

Der IT-Planungsrat von Bund und Ländern übernimmt die Koordinierung in Fragen der Informationstechnik, wie etwa die Festlegung von IT-Interoperabilitätsstandards und IT-Sicherheitsstandards. Im Übrigen ist der Staatsvertrag angesichts der erheblichen Rechtsfolgen und seiner intendierten Verbindlichkeit erstaunlich vage formuliert. Z.B. hätte konkreter geregelt werden sollen, welche Rolle dem IT-Planungsrat bei der Steuerung von E-Government-Projekten auf Landesebene zukommt. Offensichtlich sollen dem IT-Planungsrat relativ weitreichende Zuständigkeiten eingeräumt werden können. Dies folgt etwa aus § 1 Abs. 1, 3. Spiegelstrich des Staatsvertrages, wonach der IT-Planungsrat „E-Government-Projekte“ steuern kann, soweit sie ihm „zugewiesen werden“. Ausweislich der Begründung soll der Begriff des „E-Government“ weit zu verstehen sein. Es soll keine Beschränkung auf technische Fragestellungen erfolgen, sondern eine umfassende Steuerung ermöglicht werden. Dies widerspricht der gebotenen restriktiven Auslegung von Art. 91c Abs. 1 GG. Aufgrund der Einschränkung „auf Zuweisung“ sind zwar keine verfassungsrechtlichen Bedenken (Eigenstaatlichkeit der Länder) zu erheben. Allerdings hätte dann im Staatsvertrag geregelt werden müssen, wer in welchem Verfahren dem IT-Planungsrat derartige Projekte zuweisen kann, ob der IT-Planungsrat verpflichtet ist, die Projektsteuerung (ggf. unter welchen Voraussetzungen) zu übernehmen (dafür spräche der Wortlaut „zuweisen“), welche Kompetenzen er dabei im „Außenverhältnis“ (etwa gegenüber betroffenen Dritten wie IT-Unternehmen) hätte, in welchem Umfang die delegierte „Steuerung“ von E-Government-Projekten erfolgen kann usw. Begrenzungen erscheinen geboten. Es widerspräche dem Grundsatz der Eigenstaatlichkeit der Länder, wenn es diesen ermöglicht würde, ohne inhaltliche Einschränkung sämtliche E-Government-Projekte an eine demokratisch nicht unmittelbar legitimierte Stelle zur (selbständigen) Erledigung zu übertragen.

Von erheblicher Bedeutung ist in den vom IT-Planungsrat zu bewältigenden Aufgaben die Gewährleistung der IT-Sicherheit, auch vor dem Hintergrund des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Auch hierzu trifft der Vertrag keine Aussagen. Zudem hätte angesichts der Novellierung des BSI-Gesetzes auch das Verhältnis zwischen dem BSI und dem IT-Planungsrat (IT-Sicherheitskompetenz versus IT-Steuerungskompetenz) geklärt werden müssen. Sinnvoll wäre schließlich auch ein integriertes Datenschutzkonzept gewesen.

2.2 Grundrechtsschutz der Vertraulichkeit und Integrität Informationstechnischer Systeme

Von besonderer Bedeutung für das E-Government ist ein neues Grundrecht, das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (BVerfG v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGe 120, 274)

Das Bundesverfassungsgericht stützt sich in dem neuen Grundrecht mit den **„informationstechnischen Systemen“** auf eine Begrifflichkeit, die schon vielfach umschrieben wurde, als Rechtsbegriff jedoch noch nicht etabliert ist. Der Begriff

des „informationstechnischen Systems“ ist wohl weit zu fassen. Darunter kann man ein System verstehen, welches aus Hard- und Software sowie aus Daten besteht und der Erfassung, Speicherung, Verarbeitung, Übertragung und Anzeige von Informationen und Daten dient. Erfasst wird aber nicht jedes informationstechnische System, das personenbezogene Daten erzeugen, verarbeiten oder speichern kann: Das Grundrecht ist vielmehr anzuwenden, „wenn die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten“.

Beispiele: PC (installiert und mobil; geschäftliche und private Nutzung); Mobiltelefone oder elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können; darüber hinausgehend private und Firmennetzwerke sowie das Internet mit seinen angeschlossenen Servern und Clientrechnern.

Das Gericht führt zwei Schlüsselbegriffe ein – die Vertraulichkeit und die Integrität eines IT-Systems. **Vertraulichkeit** ist die Eigenschaft eines IT-Systems, berechtigten Subjekten (also jenen Personen, denen der Informationsherr „vertraut“) den Zugriff auf bestimmte Objekte zu gestatten und gleichzeitig unberechtigten Subjekten den Zugriff auf diese Objekte zu verwehren. Geschützt ist danach das Verfügungsinteresse des berechtigten Nutzers.

Integrität bedeutet die Eigenschaft eines IT-Systems, Informationen in solcher Weise zu speichern und bereitzuhalten, dass sie vor Verlust oder unberechtigter Veränderung sicher sind. Die damit gemeinte Systemintegrität umfasst also jene Schutzkomponenten, die eine Kompromittierung des IT-Systems im Rahmen seiner Funktionsfähigkeit verhindern sollen. Geschützt ist danach das Funktionserhaltungsinteresse des berechtigten Nutzers.

Das neue Grundrecht wurde geschaffen, um zwei unterschiedliche **Lücken** zu schließen: Zum einen die Lücke des Systemschutzes, um bereits die Kompromittierung von IT-Systemen zu unterbinden. Zum anderen die Lücke der informationellen Selbstbestimmung: Deren Schutzwirkung wurde als zu gering empfunden, wenn es um mehr geht als die Information als solches, nämlich um die Verknüpfung der Informationen, die u. A. belastende Nutzerprofile ermöglichen. An dieser Stelle sollten strenge Verfahrensvorkehrungen geschaffen werden, was über ein neues Grundrecht leichter zu bewerkstelligen war als über die extensive Auslegung des Rechts auf informationelle Selbstbestimmung.

Das IT-Sicherheitsgrundrecht schützt insbesondere vor **heimlichen Eingriffen in die Vertraulichkeit und Integrität informationstechnischer Systeme.** Geschützt sind sowohl die im Arbeitsspeicher gehaltenen als auch die temporär oder dauerhaft auf den Speichermedien des Systems abgelegten Daten. Das Grundrecht schützt auch vor Datenerhebungen mit Mitteln, die zwar technisch von den Datenverarbeitungsvorgängen des betroffenen informationstechnischen Systems unabhängig sind, aber diese Datenverarbeitungsvorgänge zum Gegenstand haben. So

liegt es etwa bei einem Einsatz von sogenannten Hardware-Keyloggern oder bei einer Messung der elektromagnetischen Abstrahlung von Bildschirm oder Tastatur. Unerheblich ist, ob ein Zugriff leicht oder nur mit erheblichem Aufwand möglich ist. Ein Schutz besteht nur, soweit der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt. Soweit die Nutzung des eigenen informations-technischen Systems über informationstechnische Systeme stattfindet, die sich in der Verfügungsgewalt anderer befinden, erstreckt sich der Schutz des Nutzers auch hierauf.

Ein Eingriff kann zu **präventiven** oder **repressiven** Zwecken erfolgen.

Für die Annahme eines Eingriffes ist **keine Datenerfassung erforderlich**; es reicht aus, wenn das geschützte technische System angetastet wird (dann ist die entscheidende technische Hürde für eine Ausspähung genommen).

Exkurs: Online-Durchsuchung als Eingriff in das Grundrecht auf Gewährleistung von Vertrauen und Integrität informationstechnischer Systeme.

Die Online-Durchsuchung stellt einen schwerwiegenden Eingriff dar. Sie ermöglicht den Zugriff auf den gesamten Datenbestand des Betroffenen, der vor allem auch detaillierte Informationen über die persönlichen Verhältnisse und die Lebensführung des Betroffenen umfasst. Die erhobenen Daten ermöglichen damit weitreichende Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zu einer Bildung von Verhaltens- und Kommunikationsprofilen. Die Eingriffsintensität wird weiter durch die Heimlichkeit des Zugriffs erhöht. Schließlich kann weder ausgeschlossen werden, dass die Infiltration Schäden auf dem Zielrechner verursacht und zu Datenverlusten führt, noch dass dies bei Dritten geschieht, wenn etwa die Zielperson eine Infiltrationssoftware unbewusst an Dritte weiterleitet.

Ein derart schwerwiegender Eingriff ist nur angemessen, wenn die Ermächtigungsgrundlage ihn davon abhängig macht, dass bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Zudem muss das Gesetz den Grundrechtsschutz des Betroffenen auch durch geeignete Verfahrensvorkehrungen sichern.

Überragend wichtig sind zunächst **Leib**, **Leben** und **Freiheit der Person;** ferner solche Güter der Allgemeinheit**,** deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

Das Erfordernis tatsächlicher Anhaltspunkte führt dazu, dass Vermutungen oder allgemeine Erfahrungssätze allein nicht ausreichen, um den Zugriff zu rechtfertigen. Vielmehr müssen **bestimmte Tatsachen** festgestellt sein, die eine Gefahrenprognose tragen.

Die Prognose muss auf die Entstehung einer konkreten Gefahr bezogen sein. Die konkrete Gefahr wird durch drei Kriterien bestimmt: den **Einzelfall,** die **zeitliche Nähe des Umschlagens einer Gefahr in einen Schaden** und den **Bezug auf individuelle Personen als Verursacher.**

Der Zugriff auf das informationstechnische System kann allerdings schon gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Die Tatsachen müssen zum einen den Schluss auf ein wenigstens seiner Art nach **konkretisiertes und zeitlich absehbares Geschehen** zulassen, zum anderen darauf, dass **bestimmte Personen beteiligt** sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann.

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist in erster Linie ein **Abwehrrecht** des Bürgers gegen den Staat. Noch nicht geklärt, im Ergebnis aber zu bejahen (hierzu *Heckmann*, Staatliche Schutz- und Förderpflichten zur Gewährleistung der IT Sicherheit, in: FS für Gerhard Käfer, 2009, S. 129 ff.) ist die Frage, ob das sog. „IT-Grundrecht" über diese Funktion zur Abwehr staatlicher Online-Zugriffe hinaus weitergehende Pflichten oder Garantien begründet, die sich dem gleichen Schutzziel (Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und damit offenbar der IT-Sicherheit dienend) widmen, jedoch solche Gefährdungen einbeziehen, die außerhalb staatlicher Eingriffsmaßnahmen entstehen. Dazu gehört insbesondere das stetig wachsende Feld der Internetkriminalität, mithin die Bedrohung der IT-Sicherheit durch nichtstaatliche (quasi private) Gefahrenlagen.

Der inhaltliche Umfang und die Reichweite der grundrechtlichen **Schutzpflicht** zur Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme entsprechen inhaltlich dem komplementären Schutzbereich des korrespondierenden Freiheitsrechtes, d.h. der Reichweite und dem Regelungsgehalt der abwehrrechtlichen Dimension, wie sie das Bundesverfassungsgericht in seiner Entscheidung vom 27.02.2008 näher umschrieben hat. Es begründet in diesem Sinne unter den Schlagworten „Vertraulichkeit" und „Integrität" einen Schutz- und Gewährleistungsauftrag des Staates mit dem Ziel der Vermeidung und Bekämpfung nichtstaatlicher Eingriffe, die darauf abzielen, durch Infiltration, Manipulation und Ausforschung informationstechnischer Systeme einen (unbefugten) Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erlangen. In seiner ersten Schutzrichtung richtet sich die Schutzpflicht dabei auf die Gewährleistung der Vertraulichkeit der in einem informationstechnischen System gespeicherten Daten. Gleichzeitig wird – in seiner zweiten Schutzrichtung – die Integrität der informationstechnischen Systeme geschützt, um Systemzugriffe zu vermeiden, über die Leistungen, Funktionen und Speicherinhalte durch unbefugte Dritte genutzt werden könnten. Die grundrechtliche Schutzpflicht richtet sich an alle staatlichen Handlungsträger und ist diesen gegenüber nach Maßgabe des Art. 1 Abs. 3 GG normativ verbindlich, begründet allerdings **keinen umfassenden IT-Sicherheitsgewährleistungsanspruch des Bürgers** in dem Sinne, dass der Staat jegliche Maßnahme wahrzunehmen hätte, die tatsächlich oder aus Sicht des Bürgers vermeintlich zur Erhöhung des (abstrakten oder konkreten) IT-Sicherheitsniveaus (und damit der Vertraulichkeit und Integrität informations-technischer Systeme) führt.

In einem gewissen Umfang sind aber **staatliche Leistungs- und Förderpflichten** aus dem neuen „IT-Grundrecht“ ableitbar. Ausgangspunkt ist dabei die Gewährleistung eines unbedingten und insoweit unabdingbaren Minimalstandards. Erfasst sind in diesem Sinne zunächst die Grundentscheidung und die Grundverantwortung des Staates für eine aktive und effektive Gewährleistung der IT-Sicherheit in der Bundesrepublik Deutschland („ob“), aber auch die Verpflichtung zur Vornahme grundlegender und elementarer Maßnahmen und Strukturentscheidungen („Wie“), deren Fehlen einer evidenten Verletzung der grundrechtlich geschützten Rechts- und Schutzgüter gleichkäme. Jenseits dieses unabdingbaren Minimalschutzes können dann – in Abhängigkeit von der Gewichtung der betroffenen Rechtsgüter – unterschiedlich weit reichende Handlungspflichten entstehen. Insgesamt gilt, dass sich das Entschließungs- und Auswahlermessen der staatlichen Handlungsträger umso weiter konkretisieren und insoweit zu Handlungs- und Unterlassungspflichten verdichten lässt, je stärker sich die Beeinträchtigung der durch das Grundrecht geschützten Rechtsgüter darstellen und je geringer sich im Vergleich dazu die Kollision mit anderen verfassungsrechtlich geschützten Zielvorgaben oder (rechtsstaatlichen) Rahmenbedingungen auswirkt. Eine Verdichtung zu einer Handlungspflicht im Sinne einer konkreten Einzelmaßnahme (gleich einer „Ermessenreduzierung auf Null“) kann es demnach nur dort geben, wo eine bestimmte Maßnahme zum elementaren Schutz der Rechtsgüter des „IT-Grundrechts“ unbedingt erforderlich ist und die damit verfolgten Schutzinteressen andere durch diese Maßnahme betroffene und insoweit beeinträchtigte oder vernachlässigte Interessen wesentlich überwiegen.

Allerdings bedürfen die grundrechtlichen Schutzpflichten in der Regel vielfach einer **Konkretisierung durch einfache Gesetze**. Diese Konkretisierung des Schutzauftrages findet gerade im Bereich der Informationstechnologie etwa durch die Vorgaben des Telemediengesetzes oder des Datenschutzrechtes statt. Dies schließt jedoch die Möglichkeit nicht aus, dass Schutzpflichten – unabhängig von einer gesetzesförmigen Ausgestaltung – unmittelbare Pflichten des Gesetzgebers begründen.

Insgesamt lässt sich sagen, dass das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme keinen allgemeinen Leistungsanspruch auf eine **adäquate IT-Ausstattung des Bürgers** begründet. Eine Leistungspflicht besteht allenfalls im Sinne der Unterstützung des Bürgers bei der Absicherung und Gewährleistung der Vertraulichkeit und Integrität seiner informationstechnischen Systeme gegenüber unbefugten Zugriffen von dritter Seite.

2.3 Grundrecht auf IT-Abwehr

Mit der umfassenden Etablierung von E-Government-Angeboten wird die Frage diskutiert, ob gegen diese Art staatlicher Verwaltungstätigkeit auch Abwehransprüche bestehen (*Heckmann*, MMR 2006, 3). Haben diejenigen, die von solchen Modernisierungsmaßnahmen betroffen sind, dies bedingungslos hinzunehmen oder können sie auf konventioneller Information und Kommunikation beharren: die Verwaltungsbediensteten am „elektronischen Arbeitsplatz“, die Hochschullehrer in der E-University, Richter und Anwälte unter Geltung des Justizkommu-

nikationsgesetzes und vor allem die Bürger und Unternehmer mit zunehmend angebotenen und mitunter verlangten elektronischen Behördenkontakten?

Angesichts der je nach Personengruppe völlig unterschiedlich betroffenen grundrechtlichen Positionen kann dies nicht einheitlich beantwortet werden. Jedenfalls im „**verwaltungsinternen Bereich**" können sich Verwaltungsbedienstete grundsätzlich nicht (nach Art. 33 Abs. 2 bzw. Abs. 5 GG) gegen den Einsatz neuer Medien in ihrem Tätigkeitsbereich erwehren. Anders ist dies nur zu beurteilen, wenn mit dem Einsatz von E-Government die Wissenschaftsfreiheit (Art. 5 Abs. 3 GG) oder die richterliche Unabhängigkeit (Art. 97 GG) berührt ist. Die mit besonderen verfassungsrechtlichen Freiheiten versehenen Hochschullehrer und Richter können sich zumindest dort einer Hochschul- bzw. Justizmodernisierung mittels neuer Medien entgegenstellen, wo es um die inhaltliche Beeinflussung geht, die aus der IT-Nutzung droht.

Im „**verwaltungsexternen Bereich**" bestehen dagegen bisher kaum greifbare Grenzen. Eine generelle Verpflichtung der Bürger, ein bestimmtes E-Government-Angebot der Verwaltung zu nutzen, besteht bisher nicht. Das korrespondierende Recht auf „IT-Abstinenz" ergibt sich bereits einfachgesetzlich aus § 3a VwVfG (bzw. den gleichlautenden Vorschriften auf Landesebene). Danach ist die elektronische Kommunikation mit der Verwaltung nur zulässig, wenn (insb.) der Bürger hierfür den Zugang eröffnet hat. Es gilt demzufolge das „Freiwilligkeitsprinzip"; aufgedrängtes E-Government findet gegenüber dem Bürger nicht statt.

Etwas anderes gilt für **Unternehmen**, denen gegenüber sich Staat und Verwaltung weniger zurückhaltend zeigen. Anders als beim „normalen" Bürger kann dem Unternehmer elektronische Kommunikation durchaus aufgezwungen werden. Ein Paradebeispiel für „aufgedrängtes" E-Government stellt die Pflicht zur elektronischen Umsatzsteuervoranmeldung bzw. Lohnsteuer-Anmeldung durch Arbeitgeber dar.

Zumindest für nicht technikaffine oder sozial schwache Bürger ist eine Art Bürgerrecht auf IT-Abwehr (oder IT-Abstinenz) in Betracht zu ziehen, wenn man die leistungs- und teilhaberechtliche Dimension der Grundrechte fokussiert, wie es die globale Diskussion um das Thema **Digital Divide** auch nahe legt. Ein gewichtiges Argument gegen E-Government lautet, dass gerade die hauptsächlichen Zielgruppen der Leistungsverwaltung – ältere Menschen, Arme und schlecht Ausgebildete – oft nicht über den Zugang zum Medium Internet, bzw. die Fähigkeit das Internet zu nutzen, verfügen. Ungleichbehandlungen könnten die Folge sein, Art. 3 Abs. 1 GG scheint berührt. Dies hieße, auf absehbare Zeit E-Government und traditionelle Verwaltungsverfahren parallel (gleichsam doppelt) zu führen. Dies jedenfalls solange, bis die notwendige umfassende Akzeptanz und Verbreitung von IT-Technologie in allen gesellschaftlichen Schichten gesichert ist. Dazu gehört aber nicht nur ein gesicherter – und inzwischen auch hinreichend schneller – Zugang ins Internet sowie ausreichende Grundkenntnisse zur IT-Nutzung. Grundsätzlich müssen alle digitalen Dienstleistungen der Verwaltung auch Behinderten vollumfänglich zugänglich sein (Art. 3 Abs. 3 Satz 2 GG).

2.4 Grundrecht auf IT-Einsatz - Die Pflicht zur barrierefreien Ausgestaltung staatlicher Internetangebote

Der Frage nach einem Recht auf IT-Abwehr steht umgekehrt die (grundrechtliche) Forderung nach einem Recht auf IT-Einsatz gegenüber. Etwa als Teilhaberecht an technologischen Errungenschaften zur Beseitigung spezifischer Nachteile von Behinderten. Ob sich ein derartiges Recht unmittelbar aus Art. 3 Abs. 3 Satz 2 GG herleiten lässt, kann indes weitgehend dahingestellt bleiben, nachdem der einfache Gesetzgeber (v.a. in Reaktion auf supranationale Entwicklungen) mit dem Behindertengleichstellungsgesetz (BGG) und der flankierenden Barrierefreien Informationstechnik-Verordnung (BITV) seinem Schutzauftrag mittlerweile in weitem Umfang nachgekommen ist.

Auf Grund der Vorschriften des **Behindertengleichstellungsgesetzes** (BGG) müssen die IT-gestützten G2C-Angebote der öffentlichen Gewalt auch hierzulande barrierefrei gestaltet werden. Das bedeutet, dass alle E-Government-Plattformen, Internetauftritte, etc. für behinderte Menschen in der allgemein üblichen Weise, ohne besondere Erschwernis und grundsätzlich ohne fremde Hilfe zugänglich und nutzbar sein müssen. Barrierefreiheit ist nicht bereits dann gegeben, wenn behinderten Menschen ein „Sonderzugang“ eingerichtet wird. Um das Prädikat „barrierefrei“ zu erhalten, muss das Webangebot die insgesamt vierzehn in der Barrierefreie Informationstechnik-Verordnung (BITV-Bund) festgelegten Anforderungen an Programmierung und Gestaltung erfüllen. Diese regeln unter anderem audio-visuelle Inhalte, die Sprache, die Verwendung neuer Technologien sowie die universelle Nutzbarkeit. Rechtlich verpflichtend ist die BITV nur auf Bundesebene. Auf Landes- und kommunaler Ebene ist die Rechtslage noch uneinheitlich. Während beispielsweise in Hamburg, wie in den meisten Bundesländern, sowohl ein Landesgleichstellungsgesetz sowie die landesrechtliche Barrierefreie Informationstechnik-Verordnung – HmbBITVO – existiert, ist in Sachsen eine entsprechende Verordnung nicht vorgesehen. Am Beispiel von Bayern zeigt sich, dass in den Bundesländern die konkreten Verpflichtungen im Vergleich zur Bundesregelung verwässert werden. Nach der BayBITV haben die Vorgaben zur Schaffung barrierefreier Informationstechnik öffentlicher Stellen lediglich Soll-Charakter. Es steht jedoch fest, dass alle Bundesländer früher oder später der BITV Bund entsprechende Anforderungen an die Webauftritte der öffentlichen Gewalt stellen werden. Vor allem auf Gemeindeebene wird in Bezug auf die Notwendigkeit eines barrierefreien Webdesigns teilweise mit Unverständlichkeit reagiert, vor allem in Bezug auf die Belastung kleinerer Gemeinden mit wenigen behinderten Einwohnern mit vermeintlich hohen Kosten.

2.5 E-Democracy

Die neuen Medien werden zunehmend auch für demokratische Prozesse genutzt. Unter dem Schlagwort **E-Democracy** werden insbesondere Petitionen, Abstimmungen und Wahlen in elektronischer Form diskutiert. Allerdings hat das BVerfG zuletzt den Einsatz von Wahlcomputern bei der Bundestagswahl für unzulässig erklärt (BVerfG v. 03.03.2009 – 2 BvC 4/07 – *Heckmann*, jurisPR-ITR 2009 Anm. 2). Der **Grundsatz der Öffentlichkeit der Wahl** gebiete es, dass alle

wesentlichen Schritte der Wahl öffentlich überprüfbar sind, was bei Einsatz der streitgegenständlichen Wahlcomputer nicht gewährleistet sei: Der Einsatz von Wahlgeräten, die die Stimmen der Wähler elektronisch erfassen und das Wahlergebnis elektronisch ermitteln, genügt nur dann den verfassungsrechtlichen Anforderungen, wenn die wesentlichen Schritte von Wahlhandlung und Ergebnisermittlung zuverlässig und ohne besondere Sachkenntnis überprüft werden können. Während bei der herkömmlichen Wahl mit Stimmzetteln Manipulationen oder Wahlfälschungen unter den Rahmenbedingungen der geltenden Vorschriften jedenfalls nur mit erheblichem Einsatz und einem präventiv wirkenden sehr hohen Entdeckungsrisiko möglich sind, sind Programmierfehler in der Software oder zielgerichtete Wahlfälschungen durch Manipulation der Software bei elektronischen Wahlgeräten nur schwer erkennbar. Die große Breitenwirkung möglicher Fehler an den Wahlgeräten oder gezielter Wahlfälschungen fordert besondere Vorkehrungen zur Wahrung des Grundsatzes der Öffentlichkeit der Wahl.

Der **Wähler selbst** muss ohne nähere computertechnische Kenntnisse nachvollziehen können, ob seine abgegebene Stimme als Grundlage für die Auszählung oder jedenfalls als Grundlage einer späteren Nachzählung unverfälscht erfasst wird. Wird das Wahlergebnis durch rechnergesteuerte Verarbeitung der ausschließlich in einem elektronischen Speicher abgelegten Stimmen ermittelt, genügt es nicht, wenn anhand eines zusammenfassenden Papierausdrucks oder einer elektronischen Anzeige lediglich das Ergebnis des im Wahlgerät durchgeführten Rechenprozesses zur Kenntnis genommen werden kann.

Bemerkenswert ist die Aussage des Gerichts, dass Einschränkungen der bürgerschaftlichen Kontrollierbarkeit des Wahlvorgangs **nicht durch technische und organisatorische Sicherungsmaßnahmen** (wie etwa einer Zertifizierung) kompensiert werden könnten. Diesbezüglich löst das Gericht das dem Technikeinsatz innewohne Komplexitätsdilemma, welches das Erstarken von „Expertokratien" tendenziell fördert und möglicherweise einen schwindenden Einfluss auf demokratische Legitimationsakte zur Folge hat, zu Gunsten eines jedermann transparenten Wahlverfahrens auf, das den Willen des Volkes genau, nachvollziehbar und für jedermann überprüfbar – (vorerst) auf Papier – festhält.

Fraglich ist unterdessen, wie sinnvoll elektronische Wahlen allerdings sein werden, die den Anforderungen des BVerfG Rechnung tragen Das Gericht nennt als verfassungskonforme Alternative computergestützter Wahlen den Einsatz solcher „Wahlgeräte, in denen die Stimmen neben der elektronischen Speicherung anderweitig erfasst werden. Dies ist beispielsweise bei elektronischen Wahlgeräten möglich, die zusätzlich zur elektronischen Erfassung der Stimme ein für den jeweiligen Wähler sichtbares Papierprotokoll der abgegebenen Stimme ausdrucken [„voter verified paper audit trail printers"], das vor der endgültigen Stimmabgabe kontrolliert werden kann und anschließend zur Ermöglichung der Nachprüfung gesammelt wird." Der Vorteil dieser Vorgehensweise erschließt sich erst auf den zweiten Blick, bedeutet der **kalkulierte Medienbruch** (elektronische Stimmzählung plus Papier) doch einen Mehraufwand, der die Investition in elektronische Wahlsysteme in Frage stellt. Das Argument, der Papierausdruck erzeuge Nachvollziehbarkeit der Stimmabgabe, verfängt nicht, weil die Manipulation so gestaltet werden kann, dass

Bildschirm- und Druckerausgabe noch synchron sind, Änderungen nämlich erst bei der Übermittlung der Daten – und dann eben unmerklich – erfolgen. Natürlich würde das bei einem Vergleich des elektronischen Zählergebnisses mit einer händischen Auszählung auffallen. Das betrifft das Argument der Nachprüfbarkeit der Stimmabgabe. Jedoch: Hat man einmal Vertrauen in die (geprüfte) Sicherheit elektronischer Wahlsysteme, bedarf es der aufwändigen Erzeugung und Sammlung von über 30 Millionen Papierausdrucken (bei einer Bundestagswahl) nicht. Vertraut man der Technik nicht, dann wird es faktisch bei jeder elektronischen Wahl eine erzwungene „Vergleichszählung" der „Papierstimmen" geben, weil sich zumindest die Bewerber und Unterstützer der unterlegenen Parteien diese Chance nicht entgehen lassen. Das würde sich auch nicht auf einzelne Wahlkreise beschränken („Domino-Effekt"). Diese Nachzählung könnte auch kaum verwehrt werden, wäre sie doch Ausdruck des Grundsatzes der Öffentlichkeit der Wahl, den das BVerfG als verfassungsrechtliches K.-o.-Kriterium gegen jegliche Wahlsysteme anführt, die von Personen ohne informationstechnische Spezialkenntnisse nicht überprüfbar sind (was bei Wahlcomputern oder ähnlichen Technologien in der Natur der Sache liegt). Vor diesem Hintergrund erscheint der Einsatz elektronischer Wahlgeräte nur deshalb sinnvoll, weil damit die (bewusste oder unbewusste) Abgabe ungültiger Stimmen vermieden werden kann (was sich in der Menüführung des Wahlvorgangs technisch leicht umsetzen lässt). Ob das alleine den finanziellen Aufwand elektronischer Wahlen rechtfertigt, bliebe zu untersuchen.

Bemerkenswert ist, dass das BVerfG den Grundsatz der Öffentlichkeit der Wahl nicht einfach auf die öffentliche Wahrnehmung der Wahlhandlung (Stimmabgabe) herunterbricht und damit einem substituierenden Einsatz von Wahlcomputern eine (endgültige) Absage erteilt. Vielmehr werden die **wesentlichen Instrumente der IT-Sicherheitsgewährleistung** (Einbeziehung vertrauenswürdiger Instanzen und Experten, Schaffung von Transparenz durch Publizität, Prävention durch Zulassungsverfahren bis hin zu der „Gesamtheit sonstiger technischer und organisatorischer Sicherungsmaßnahmen") explizit aufgeführt und als zur „Kompensation ungeeignet" ausgeschieden. **Sicherheit und Vertrauen** stehen hier beziehungslos nebeneinander. Gefordert wird eine bürgerschaftliche Kontrollierbarkeit durch Optik und Haptik: „Rechtsstaatlich begründete Öffentlichkeit dient der Transparenz und Kontrollierbarkeit staatlicher Machtausübung. Sie setzt voraus, dass die Handlungen der staatlichen Organe von den Bürgern [selbst, gegenwärtig und unmittelbar] zur Kenntnis genommen werden können." Dabei könnte es – im Extremfall – sogar sein, dass Wahlhandlungen von Menschen für Menschen durch Menschen kontrolliert eine höhere Fehlerrate aufweisen als jene im elektronischen Wahlverfahren: Die durch persönliches, offenes Handeln gewährleistete Öffentlichkeit der Wahl legitimiert dieses Ergebnis.

Man mag dies als Besonderheit des Wahlrechts, seiner Wahlgrundsätze und dem besonderen Legitimationsfaktor in einer repräsentativen Demokratie zurechnen. Dennoch wird es Überlegungen geben, ob sich vergleichbare Forderungen nach einer Nachvollziehbarkeit von elektronischen Handlungen für den Bürger als technischen Laien auch auf **andere Bereiche** (E-Government, E-Justice etc.) übertragen lassen. Auch dort gibt es Ausprägungen eines Öffentlichkeitsgrund-

satzes, die zumindest in abgeschwächter Form eine bürgerschaftliche Kontrolle verlangen. In der Tat verliert das Recht mit seinen persönlichen Handlungen in einem durchgehend vernetzten, medienbruchfrei gestalteten virtuellen Verwaltungsraum mit informationstechnologischen Workflows an Steuerungskraft. In automatisierten Geschäftsprozessen liegt die Hauptverantwortung beim Programmierer. Rechtliche Standards werden durch technische Standards abgelöst. Das Recht dient bestenfalls der Qualitätssicherung. Es wird Aufgabe des momentan entstehenden IT-Sicherheitsrechts sein, **Handlungs- und Haftungsmaßstäbe für den IT-Einsatz zu bilden** und der Phantasie technologischer Innovationen jene Grenzen zu setzen, die sich aus dem Leitbild einer freiheitlich-bürgerlichen Verfassung mit menschlichem Antlitz ergeben.

3. Einfachgesetzliche Vorgaben

3.1 Allgemeiner rechtlicher Rahmen

Die Abwicklung von Verwaltungsvorgängen über das Internet unterscheidet sich aus rechtlicher Sicht erheblich von der Abwicklung per Post oder im persönlichen Kontakt vor Ort in einer Behörde. Dabei ist inzwischen ein umfassender und anwendbarer rechtlicher Rahmen entstanden, den es bei der Einführung von E-Government zu beachten gilt. Grundlegende Regelungen zur elektronischen Kommunikation finden sich in den § 3a, 33, 37 Abs. 2 – 4, 39 Abs. 1, 41 Abs. 2 und 44 Abs. 2 VwVfG. Ergänzend dazu sind die Vorschriften aus dem **Signaturgesetz** (SigG) und der Verordnung zur elektronischen Signatur (SigV) heranzuziehen. Namentlich sind dies Normen zur Erläuterung der unterschiedlichen Niveaus von Signaturen (§ 2 SigG), zum Inhalt von qualifizierten Zertifikaten (§ 7 SigG; § 14 SigV), zur Sperrung von qualifizierten Zertifikaten (§ 8 SigG), über Produkte für qualifizierte elektronische Signaturen (§ 17 SigG; § 15 SigV), über ausländische elektronische Signaturen (§ 23 SigG) sowie zum Verfahren langfristiger Datensicherung (§ 17 SigV). Weiterhin finden sich gesetzliche Grundlagen im **Telemediengesetz** (TMG). Zu beachten sind dabei insbesondere Vorschriften über die Zulassungs- und Anmeldefreiheit von Telemediendiensten (§ 4 TMG), die Impressumspflicht (§ 5 TMG) als auch zur Haftung (§§ 7 ff. TMG).

Auch das Gesetz zur Gleichstellung behinderter Menschen (BGG) und die Verordnung zur **Schaffung barrierefreier Informationstechnik** nach dem Behindertengleichstellungsgesetz (BITV, BGBl I 2002, 2645) beinhalten essentielle Regelungen, insbesondere was den Webauftritt von Behörden angeht. Zu nennen sind dabei § 11 BGG, welcher der Bundesverwaltung die Pflicht oktroyiert, die Belange von Personen mit Behinderung bei der Gestaltung von Online-Angeboten gesondert zur berücksichtigen, sowie die Regelungen der BITV, welche die in diesem Zusammenhang begünstige Gruppe behinderter Menschen definieren, die betroffenen Arten und Bereiche der Online-Angebote der Verwaltung festlegen und letztlich die in Anwendung zu bringenden technischen Standards umschreiben. In diesem Zusammenhang sind auch Anspruchsgrundlagen des Arbeitnehmers auf barrierefreien Zugriff von Online-Angeboten zuzugreifen, welche sich im SGB IX finden, zu erwähnen.