LANDTAG RHEINLAND-PFALZ
16. Wahlperiode

Drucksache 16/882
14. Februar 2012

# Unterrichtung

**durch den Landesbeauftragten für den Datenschutz und die Informationsfreiheit**

## Dreiundzwanzigster Tätigkeitsbericht nach § 29 Abs. 2 Landesdatenschutzgesetz – LDSG – für die Zeit vom 1. Oktober 2009 bis 31. Dezember 2011

Dem Präsidenten des Landtags am 14. Februar 2012 überreicht.
Der Bericht wurde in der Datenschutzkommission nach § 26 Abs. 3 Satz 4 Landesdatenschutzgesetz vorberaten.

Druck: Landtag Rheinland-Pfalz, 16. Februar 2012

# Datenschutzbericht
## 2010/2011

# Inhalt

Die Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie die Beschlüsse der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) sind im Internetangebot des LfD unter folgender URL abrufbar: http://www.datenschutz.rlp.de/de/ds.php?submenu=grem

# Einführung

In unserer digitalisierten Welt, in der wir überall Datenspuren hinterlassen, im Internet und außerhalb des Netzes, nimmt die Bedeutung des Datenschutzes zwangsläufig zu und damit auch die öffentliche Aufmerksamkeit an ihm. Dies war auch in der Zeit von Oktober 2009 bis Ende 2011 der Fall, dem Berichtszeitraum für diesen – nunmehr 23. – Tätigkeitsbericht des LfD.

Naturgemäß richtet sich die öffentliche Aufmerksamkeit im Lande auch nach den Ereignissen, die bundesweit Schlagzeilen machen. Im Berichtszeitraum waren dies nicht mehr die großen Datenskandale wie noch 2008 und 2009, als die Deutsche Bahn, die Deutsche Telekom, Lidl und andere deutsche Unternehmen für Aufregung sorgten. An ihre Stelle traten vielmehr Google, Facebook und Co., also die US-amerikanischen Internetgiganten, über deren Aktivitäten alle Medien intensiv berichteten, die elektronischen ebenso wie die Printmedien und bei diesen die seriösen Tageszeitungen ebensowie die Massenblätter. Facebook sorgte sogar für den Aufmacher bei der „Bild"-Zeitung und für einen Boykott-Aufruf im „Stern" („Raus aus Facebook"). Auch über Google Street View berichteten sämtliche Medien monatelang auf ihren politischen Seiten, in ihren politischen Magazinen und im Feuilleton. Diese Berichterstattung beförderte eine gesellschaftliche Diskussion über den Datenschutz, die glücklicherweise immer noch im Gang ist.

Der „Datenhunger" des Staates trat demgegenüber in den Hintergrund, wenn man von der Vorratsdatenspeicherung absieht, die Anfang 2010 in einer spektakulären Entscheidung des Bundesverfassungsgerichts gestoppt wurde und seither auch nicht wieder eingeführt worden ist. Datenschutzdefizite beim Einsatz des sog. Staatstrojaners spielten zwar in der öffentlichen Diskussion ebenfalls noch eine gewisse Rolle. Im Übrigen herrschte aber eher Ruhe. Die neue Volkszählung wurde mit dem Segen des Bundesverfassungsgerichts und ohne nennenswerte Proteste in der Bevölkerung durchgeführt, der neue elektronische Personalausweis mit seinem RFID-Chip und besonderen Zusatzfunktionen mit kritischer Unterstützung der Datenschutzbeauftragten eingeführt und das ELENA-Verfahrensgesetz, das zu einer Vorratsdatenspeicherung zahlreicher Datensätze von 40 Millionen Beschäftigten geführt hätte, vom Bundestag still und leise aufgehoben.

Vor diesem Hintergrund spielte sich die datenschutzrelevante Entwicklung in Rheinland-Pfalz ab, jene im staatlichen Bereich und jene in der Wirtschaft. Weder in dem einen noch in dem anderen Bereich kam es zu großen Datenskandalen. Pannen und Datenschutzdefizite waren allerdings hier wie dort festzustellen. Immer mehr richtete sich die Aufmerksamkeit allerdings auf weitere Beteiligte: die Bürgerinnen und Bürger selbst, die zunehmend Daten von sich preisgeben, auch unbewusst Datenspuren hinterlassen und von der digitalen Entwicklung im Netz und außerhalb des Netzes nicht selten überfordert werden, was nicht zuletzt auch darin zum Ausdruck kommt, dass die Bürgerinnen und Bürger sich immer häufiger hilfesuchend an meine Dienststelle wenden. Dabei ging und geht es auch um Fragen der Informationstechnik, zumal diese immer nachhaltiger in alle Lebensbereiche eindringt.

Der nachfolgende Bericht stellt diese Entwicklung dar und gibt Rechenschaft darüber, wie der LfD seine ihm übertragenen Aufgaben wahrgenommen hat. Er gliedert sich in zwei große Abschnitte. Im ersten Abschnitt finden sich grundsätzliche Anmerkungen zum Stellenwert des Datenschutzes, zur Entwicklung des Datenschutzrechts und zu den thematischen Schwerpunkten des Datenschutzes sowie zum Datenschutz als Bildungs- und Erziehungsaufgabe. Im zweiten Abschnitt werden ausgewählte Prüfungsergebnisse zusammengefasst. Der Bericht endet mit einigen Bemerkungen zur Dienststelle des LfD und ihrer Entwicklung im Berichtszeitraum.

Wiederum wurde der LfD bei seiner Arbeit auf vielfältige Weise unterstützt: von den Abgeordneten aller im Landtag vertretenen Fraktionen, von der Landesregierung in ihrer jeweiligen Zusammensetzung, von der Datenschutzkommission unter ihrem Vorsitzenden, dem Abgeordneten Pörksen, und von vielen weiteren öffentlichen und privaten Stellen, die Interesse an der Arbeit des LfD gezeigt und seine Tätigkeit gefördert haben. Diese Unterstützung war hilfreich. Ich darf mich an dieser Stelle dafür bedanken.

Danken möchte ich auch meinen Mitarbeiterinnen und Mitarbeitern für ihren engagierten Einsatz, für ihre Anregungen und ihre Unterstützung. Ihre Belastung ist unverändert groß, so wie die von ihnen und mir wahrzunehmenden Aufgaben unverändert anspruchsvoll, abwechslungsreich und spannend sind.

Edgar Wagner

# I. Grundsatzfragen des Datenschutzes

## 1. Stellenwert des Datenschutzes

Der Datenschutz soll das „informationelle Selbstbestimmungsrecht“ sichern, das jeder Bürgerin und jedem Bürger einen Anspruch darauf gibt, „zu wissen, wer was wann bei welcher Gelegenheit über ihn weiß“ (BVerfGE 65,1). Da dieses Datenschutzgrundrecht in seinem Kern Bestandteil der Menschenwürde und zugleich Funktionsbedingung unserer demokratischen Ordnung ist, genießt es einen hohen Stellenwert und ist deshalb im Vergleich zu anderen Grundrechten und Verfassungspositionen alles andere als nachrangig. Doch wie steht es um den Stellenwert des Datenschutzes in der Verfassungspraxis und in der Alltagsrealität?

### 1.1 In Rheinland-Pfalz

In Rheinland-Pfalz genießt der Datenschutz einen seiner Bedeutung angemessenen Stellenwert. Das gilt insbesondere für den öffentlichen Bereich. Hier besteht ein in den vergangenen Jahrzehnten gewachsenes Bewusstsein für das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger, und zwar auf allen Ebenen und in allen Bereichen. Dabei geht der **Landtag** mit gutem Beispiel voran. Zum Ausdruck kommt dies insbesondere in seiner Gesetzgebungsarbeit, wobei von der Novellierung des Landesdatenschutzgesetzes (vgl. Tz. I-2.3.1) bis zu den Datenschutzvorschriften in der Neuregelung des Polizei- und Ordnungsbehördengesetzes (vgl. Tz. II-4.1) die parlamentarische Zustimmung fraktionsübergreifend war und auch die Opposition mit einschloss. Insoweit war und ist der Datenschutz in Rheinland-Pfalz – jedenfalls im Grundsatz – von einem breiten Konsens der politischen Kräfte getragen, was nicht nur bei der Gesetzgebung der Fall ist, sondern auch bei sonstigen grundlegenden Parlamentsbeschlüssen, etwa bei der Entschließung zum „Datenschutz als Bildungs- und Erziehungsaufgabe“ (vgl. Tz. I-4.1).

Selbst dort, wo die Fraktionen unterschiedliche Vorschläge vorgelegt haben, wie etwa im Abschlussbericht der Enquete-Kommission „Verantwortung in der digitalen Welt“, sind sie in datenschutzrechtlicher Hinsicht weiterführend. Dies gilt etwa für den im Mehrheitsvotum enthaltenen Vorschlag, in den rheinland-pfälzischen Schulen einen Medienkompass einzuführen, aber auch für die im Minderheitsvotum enthaltene Anregung, einen Runden Tisch „Medienkompetenz und digitale Kultur“ zu etablieren. Gerade dieser Vorschlag findet die entschiedene Zustimmung des LfD. Die rasante digitale Entwicklung in Staat und Gesellschaft sollte politisch wie fachlich begleitet werden. Die bundesweit anerkannte Bioethik-Kommission des Landes ist dafür ein gutes Vorbild.

Immer wieder hatte der LfD im Berichtszeitraum Gelegenheit, in den Fachausschüssen des Landtags zu aktuellen datenschutzrechtlichen und datenschutzpolitischen Fragen Stellung zu nehmen. Auch wenn dabei zuweilen zwischen der einen oder anderen Fraktion und dem LfD unterschiedliche Positionen vertreten wurden, ist die Diskussion doch fair und die parlamentarische Unterstützung für den LfD groß gewesen. Dies gilt auch für die Beratungen in der Datenschutzkommission.

Wie groß der Stellenwert des Datenschutzes im Parlament ist, wurde auch zu Beginn der neuen Legislaturperiode deutlich, als der Alterpräsident des Landtags, der Abgeordnete Carsten Pörksen, der zugleich Vorsitzender der Datenschutzkommission war und ist, einen Großteil seiner Rede in der konstituierenden Sitzung des Landtags dem Datenschutz widmete und ihn als eine der großen Zukunftsaufgaben unserer Zeit bezeichnete. Für den Datenschutz war diese Rede ein wichtiges parlamentarisches Signal und ein Zeichen dafür, dass der Landtag sich auch künftig für die datenschutzrechtlichen Belange seiner Bürgerinnen und Bürger einsetzen wird. Daran ändert auch der Umstand nichts, dass der letzte Tätigkeitsbericht des LfD zum Zeitpunkt der Drucklegung dieses Berichtes immer noch nicht im Landtag beraten worden ist.

Die parlamentarische Unterstützung kam und kommt nicht zuletzt auch in den Entscheidungen des Haushaltsgesetzgebers zum Ausdruck. Obgleich die finanzielle Lage angespannt war und ist, wurden dem LfD in den zurückliegenden Haushaltsjahren zusätzliche Haushaltsmittel zur Verfügung gestellt. Nach den vorliegenden Haushaltsentwürfen soll diese Unterstützung auch in den Haushaltsjahren 2012 und 2013 fortgesetzt werden.

Was für den Landtag gilt, gilt auch für die **Landesregierung**, die den LfD stets sehr frühzeitig in die Ausarbeitung ihrer datenschutzrelevanten Gesetzentwürfe einbindet und seinen Vorschlägen in der Regel auch weitgehend folgt. In der Zukunft wird es wichtig sein, welche Position die Landesregierung zu Facebook einnehmen wird. Insbesondere im Zusammenhang mit der Nutzung der sog. Fanpages sind eine Reihe von Datenschutzfragen zu klären, wobei der LfD darauf drängen wird, dass die Landesregierung ihre

Aufgeschlossenheit gegenüber diesem Netzwerk überdenkt und dies ggf. auch in einer entsprechenden Initiative im Bundesrat zum Ausdruck bringt. Dies hat die Landesregierung bei anderen datenschutzrelevanten Grundsatzfragen im Berichtszeitraum wiederholt getan, etwa mit dem Gesetzentwurf für digitale Panoramadienste (vgl. Tz. I-2.2) und der Entschließung über den datenschutzgerechten Einsatz von RFID (vgl. Tz. II-3.1.1). Mit anderen Worten: Die Landesregierung hat ihren Einfluss zugunsten des Datenschutzes nicht nur im Land, sondern auch im Bund geltend gemacht. Auch wenn sie im Berichtszeitraum datenschutzrechtliche Pannen nicht völlig vermeiden konnte und in der Regierungserklärung des Ministerpräsidenten zu Beginn der neuen Wahlperiode die datenschutzrechtlichen und datenschutzpolitischen Probleme unseres digitalen Zeitalters nicht eigens angesprochen wurden, zollt die Landesregierung dem Datenschutz doch die gebotene Aufmerksamkeit und Beachtung.

Besonders hervorzuheben ist das von gegenseitigem Vertrauen geprägte Verhältnis des LfD zu den für die Sicherheit im Lande zuständigen Behörden und Stellen. Hier sind häufig unterschiedliche, sogar gegensätzliche Grundpositionen in einen angemessenen Ausgleich zueinander zu bringen. Kompromisse müssen gesucht und gefunden werden. Das zuständige **Innenministerium** und die nachgeordneten Dienststellen waren dazu in aller Regel bereit. Die Zusammenarbeit bei der Novellierung des Polizei- und Ordnungsbehördengesetzes (vgl. Tz. II-4.1), der datenschutzrechtlichen Gestaltung von POLIS (vgl. Tz. II-4.2) und der Überprüfung des datenschutzgerechten Einsatzes von sog. Online-Trojanern (vgl. Tz. I-3.5) macht dies deutlich. Das bedeutet nicht, dass es immer einvernehmliche Lösungen und einheitliche Auffassungen gibt. Bei der Vorratsdatenspeicherung (vgl. Tz. II-8.2.4) etwa gehen die Auffassungen offenkundig auseinander. Trotzdem muss es auch im Sicherheitsbereich darum gehen, den Datenschutz selbst dann zu verankern, wenn damit sicherheitspolitische Risiken verbunden sein können. Den Datenschutz gibt es nicht zum Nulltarif. Die Verantwortung dafür muss letztlich der Innenminister tragen. Deshalb ist der LfD für jeden tragfähigen Kompromiss dankbar. Dass das gegenseitige Verständnis groß ist, belegt im Übrigen auch die in diesem Jahr fortgesetzte Praxis, eine Beamtin bzw. einen Beamten aus dem Polizeibereich zum LfD abzuordnen. Diese Praxis hat sich – wie die Zusammenarbeit im Übrigen – bewährt.

Entsprechende personelle Verbindungen gibt es auch zum **Justizministerium** und zur rheinland-pfälzischen Justiz, denn seit einiger Zeit ist auch ein Vertreter der Richterschaft zum LfD abgeordnet. Damit einher gehen seit zwei Jahren Treffen mit den behördlichen Datenschutzbeauftragten aus dem Bereich der Justiz, an denen neben dem Justizminister auch die Spitzen der rheinland-pfälzischen Justiz teilnehmen, was deren Aufgeschlossenheit für den Datenschutz unterstreicht. Aus diesen Treffen sind Fortbildungsveranstaltungen für Richterinnen und Richter sowie Staatsanwältinnen und Staatsanwälte hervorgegangen, die unter Einbeziehung der Deutschen Richterakademie im kommenden Jahr noch verstärkt und ausgebaut werden sollen. Dabei geht es nicht nur um den Datenschutz in der Justizverwaltung, sondern auch um den Datenschutz als prozessualer Rahmen und Maßstab für justizielle Entscheidungen. Dies ist ein weites Feld, das nur gemeinsam aufgearbeitet werden kann. Je früher damit begonnen wird, desto besser. Aus diesem Grund werden seit einiger Zeit auch Rechtsreferendarinnen und -referendare in der Dienststelle des LfD ausgebildet und in Arbeitsgemeinschaften von Mitarbeiterinnen und Mitarbeitern des LfD unterrichtet. Zuweilen können besonders qualifizierte Studierende, v.a. der Rechtswissenschaften, auch mehrwöchige Praktika beim LfD absolvieren. Über 30 angehende Juristinnen und Juristen wurden auf diesem Weg im Berichtszeitraum in der Dienststelle des LfD mit den aktuellen Fragen des Datenschutzes vertraut gemacht. Dass der Datenschutz gerade im Justizministerium besonders gefördert wird, wurde im Übrigen 2010/2011 deutlich, als der seinerzeitige Minister zu den sich im Zusammenhang mit Google Street View ergebenden Rechtsfragen ein Rechtsgutachten in Auftrag gab, dessen Ergebnisse zu einer Bundesratsinitiative der Landesregierung führten.

Besonders wichtig waren im Berichtszeitraum die datenschutzpolitischen Maßnahmen, die vom **Bildungsministerium** initiiert oder unterstützt wurden. Dass der Datenschutz im Lande – mehr als anderswo – auch als Bildungs- und Erziehungsaufgabe gesehen und v.a. auch in den Schulen des Landes praktiziert wird, ist ihm zu verdanken. Wegen der Einzelheiten dieses Engagements wird auf die Tz. I-4 verwiesen.

Schließlich waren auch die gemeinsamen Aktivitäten mit dem **Verbraucherschutzministerium** hilfreich. Denn der Verbraucherdatenschutz gewinnt in Zeiten des Internets immer mehr an Bedeutung. Unter Einbeziehung der Verbraucherzentrale wurden eine Vielzahl von einschlägigen Informationsschriften für die Bürgerinnen und Bürger erstellt, Veranstaltungen durchgeführt, etwa zu RFID-Problematik, und entsprechende politische Initiativen vorbereitet. Die neue Zuordnung dieses Bereichs zum Justizministerium wird an der guten Zusammenarbeit nichts ändern. Zu

den vielen Aufgaben, die gemeinsam angegangen werden müssen, wird v.a. ein besserer Schutz von Kindern und Jugendlichen im Internet gehören.

Regelmäßig kam und kommt es darüber hinaus zu Treffen des LfD mit den Datenschutzbeauftragten der **Ressorts und der Staatskanzlei**. Sie dienen dem Informationsaustausch, sollen sicherstellen, dass die Internetpräsenz der Landesregierung datenschutzkonform realisiert wird und dafür sorgen, dass die Anregung des LfD auch im nachgeordneten Bereich berücksichtigt werden, wobei die Aufgeschlossenheit der Behörden des Landes, insbesondere der Kommunen, für den Datenschutz ohnehin groß ist. Fehler und Nachlässigkeiten in dem einen oder anderen Bereich, auf die im Folgenden noch näher eingegangen wird, ändern daran nichts, zumal ihre Folgen regelmäßig im Sinne des Datenschutzes behoben wurden.

Gerade im **kommunalen Bereich** sind die Anliegen des Datenschutzes gut aufgehoben. Der gemeinsam erzielte Kompromiss beim Einsatz von Solarkatastern (vgl. Tz. II-7.1.1) macht dies deutlich, wobei die kommunalen Spitzenverbände in diesem und in weiteren Fällen dem Datenschutz zur Seite standen und stehen. Sie unterstützen auch die jährlichen Treffen des LfD mit den Datenschutzbeauftragten der Kommunen, an denen regelmäßig 70 bis 80 kommunale Datenschutzbeauftragte teilnehmen. Dieses Netzwerk war beispielgebend für vergleichbare Treffen mit den Datenschutzbeauftragten der Justiz, der Polizei und der Hochschulen, die dazu geführt haben, dass auch zwischen den jährlichen Treffen ein reger kollegialer Austausch stattfindet – auch in speziellen Foren, die im Internetangebot des LfD für die behördlichen Datenschutzbeauftragten eingerichtet worden sind.

Bei den Entscheidungen der rheinland-pfälzischen **Gerichte** spielte das informationelle Selbstbestimmungsrecht bzw. der Datenschutz – jedenfalls quantitativ – offenbar nur eine geringe Rolle. Jedenfalls wurden gerade einmal zwei Dutzend Entscheidungen mit einem bemerkenswerten Datenschutzbezug veröffentlicht, wobei die meisten dieser Entscheidungen von den Arbeitsgerichten stammten. Nennenswerte Impulse für den Datenschutz gingen aber auch von diesen Entscheidungen nicht aus.

Auch in den **Hochschulen** des Landes gewinnt der Datenschutz an Bedeutung und zwar nicht nur in der Hochschulverwaltung, wo etwa ein Konsens beim Einsatz der Videoüberwachung gefunden wurde. Auch im Bereich der Lehre findet der Datenschutz mehr und mehr seinen Platz. Deutlich wurde dies auch bei diversen Veranstaltungen, die der LfD etwa mit der Universität Koblenz-Landau, der Universität Trier sowie der Deutschen Hochschule für Verwaltungswissenschaften in Speyer durchgeführt hat. In Speyer haben der LfD und seine Mitarbeiterinnen und Mitarbeiter auch regelmäßig Lehrveranstaltungen übernommen, was auch für andere Universitäten und Fachhochschulen im Land gilt, von denen der LfD immer wieder zu Vorträgen eingeladen wurde und wird. Um das Interesse des wissenschaftlichen Nachwuchses am Datenschutz weiter zu fördern, hat der LfD mit Unterstützung des Bildungsministeriums und der Hochschulen im Lande außerdem einen Datenschutzpreis (vgl. Tz. II-6.2.3) für wissenschaftliche Arbeiten zum Datenschutz ausgelobt. Die Ergebnisse sind beeindruckend.

**ZDF** und **SWR** unterstehen mit Blick auf die Rundfunkfreiheit zwar nicht der Kontrolle des LfD, sie sind in ihrem Bereich selbst für den Datenschutz zuständig und verantwortlich. Trotzdem finden regelmäßige Treffen mit den dortigen Datenschutzbeauftragten und auch gemeinsame Veranstaltungen zu aktuellen Datenschutzfragen statt. In der Endphase des Ratifizierungsverfahrens zum 15. Rundfunkänderungsstaatsvertrag haben die guten Kontakte zum Justiziar des SWR zu einem Kompromiss in wichtigen Datenschutzfragen geführt, der auch vom Landtag anerkannt wurde und in der von den Rundfunkanstalten noch zu erlassenden Satzung seinen Ausdruck finden soll.

Der Stellenwert, den der Datenschutz bei den in Rheinland-Pfalz ansässigen **Medien** genießt, misst sich am Umfang und Inhalt der Berichterstattung. Diese war und ist – bei den Printmedien sowie bei Rundfunk und Fernsehen – breit gefächert, informativ und stets korrekt. Insoweit erfüllen die Medien eine wichtige gesellschafts- und bildungspolitische Aufgabe, die gar nicht hoch genug geschätzt werden kann. Denn ohne diese Berichterstattung hätte der Datenschutz in der Bevölkerung nicht die Resonanz, auf die er angewiesen ist.

Diese Resonanz zeigte sich u.a. bei der großen Zahl der **Rheinland-Pfälzerinnen und Rheinland-Pfälzer**, die zu Beginn des Jahres 2011 gegen die Aufnahme ihrer Häuserfassaden durch Google und deren Wiedergabe im Online-Dienst „Street View“ Widerspruch eingelegt haben. Nach den vorliegenden Schätzungen waren es über 50.000 Bürgerinnen und Bürger alleine in unserem Land. Das Interesse am Datenschutz kommt aber auch in der ständig wachsenden Zahl von Petitionen zum Ausdruck, die den LfD mittlerweile aus der Bevölkerung erreicht. Pro Jahr sind es weit über 2.000 Anfragen und Eingaben,

wobei drei Viertel von ihnen, also rund 1.500, den privaten Sektor betreffen. Im Vergleich zum Jahre 2008, als dem LfD die Zuständigkeit für den Datenschutz im nicht-staatlichen Bereich übertragen wurde, ist dies ein Zuwachs um mehr als das Zehnfache. Dies zeigt aber auch, wo die Trägerinnen und Träger des Datenschutzgrundrechts, also die Bürgerinnen und Bürger, die eigentlichen Probleme für den Schutz und die Sicherheit ihrer Daten sehen: im privatwirtschaftlichen Bereich (vgl. Tz. II-2.1). Das belegen auch alle wissenschaftlichen Untersuchungen und Umfragen, denen zu Folge die Bürgerinnen und Bürger dem Staat bei der Verarbeitung ihrer Daten eher vertrauen als der Wirtschaft (vgl. Forsa-Umfrage im Auftrag der BITKOM).

Soweit es um **Unternehmen** geht, die ihren Sitz in Rheinland-Pfalz haben, ist der Datenschutz durchaus ein Thema, wobei die Aufmerksamkeit offenbar mit der Größe der Unternehmen wächst. Deshalb sind die Kontakte des LfD etwa zur BASF oder zu Boehringer Ingelheim besonders eng, und deshalb haben jedenfalls die großen Unternehmen im Lande entsprechend den gesetzlichen Bestimmungen auch betriebliche Datenschutzbeauftragte. Eine Umfrage des LfD bestätigte dies (vgl. Tz. I-3.7). Von den 1.500 größten Unternehmen im Lande haben über 92 Prozent solche Datenschutzbeauftragte. Die Erfahrungen zeigen aber, dass ein ausreichendes Datenschutzniveau in den Unternehmen nur sichergestellt werden kann, wenn die interne Datenschutzkontrolle der betrieblichen Datenschutzbeauftragten durch die externe Kontrolle seitens des LfD ergänzt wird. Angesichts der begrenzten personellen Mittel des LfD lässt sich diese externe Kontrolle aber ohnehin nur stichprobenweise durchführen. Umso wichtiger ist die Rolle, die den Kammern und Berufsverbänden in diesem Zusammenhang zukommt. Der LfD ist sich bewusst, dass der Datenschutz nicht gerade im Mittelpunkt der Kammer- und Verbandsaktivitäten steht und auch nicht stehen kann. Er hat dafür auch Verständnis. Trotzdem muss insgesamt mehr für den Datenschutz in den Betrieben unternommen werden. Dafür müssen beide Seiten mehr investieren. Der LfD wird die Kammern und Verbände frühzeitiger in seine Aktivitäten einbinden und Vorschläge für gemeinsame Initiativen und Aktivitäten entwickeln, wobei es dem LfD ohnehin mehr um Beratung als um Kontrolle geht. Das eine wie das andere wird aber nur mit der Unterstützung der Kammern und Verbände zum Ziel führen. Die notwendige Zusammenarbeit wird im Ansatz auch schon praktiziert. Sie ist aber auszubauen und zu intensivieren.

Alles in allem könnte man also mit dem Stellenwert, den der Datenschutz in Rheinland-Pfalz – in der Theorie und in der Praxis – genießt, zufrieden sein, zumal der von den die neue Landesregierung tragenden politischen Parteien vereinbarte Koalitionsvertrag eine Vielzahl von neuen Datenschutzinitiativen enthält. Trotzdem kann von Zufriedenheit keine Rede sein. Allerdings hängt dies mit Entwicklungen zusammen, die von Rheinland-Pfalz aus nicht oder nur mittelbar beeinflusst werden können. Gemeint sind v.a. das Internet und die wachsende Zahl von datenschutzrelevanten Online-Angeboten, gemeint sind die internationalen Online-Anbieterinnen und -Anbieter und die nationalen Online-Nutzerinnen und -Nutzer, die gigantischen Datensammlerinnen und -sammler und die sorglosen Datenlieferantinnen und -lieferanten, gemeint sind v.a. Google, Facebook, Apple und Microsoft.

## 1.2 Im Internet

Diese Internetgiganten stammen aus den USA und haben dort auch ihren Hauptfirmensitz. Die US-amerikanische Datenschutzkultur ist aber mit der unsrigen nicht zu vergleichen. Deshalb sind die Geschäftsmodelle von Google, Facebook und Co. nur schwer mit dem hiesigen Verständnis von Datenschutz in Einklang zu bringen. V.a. Google und Facebook sind darauf ausgerichtet, so viele persönliche Daten und Informationen wie möglich von ihren Nutzerinnen bzw. Nutzern und Mitgliedern zu erhalten bzw. in Erfahrung zu bringen. Sie betreiben deshalb eine aggressive Kommerzialisierung der Privatsphäre und zwar im industriellen Maßstab. So wie infolge der industriellen Revolution die Arbeitskraft der Menschen ausgebeutet wurde, so wird heute – im Zuge der digitalen Revolution – ihre Privatsphäre ausgebeutet. Private Informationen und persönliche Daten sind folglich auch die Währung, in der für die Nutzung der meisten Online-Angebote gezahlt werden muss. Diese Daten und Informationen sind die Grundlage der sog. personalisierten bzw. personalisierbaren Werbung, aus deren Erlös Facebook und Co. ihre Online-Dienste finanzieren. Je mehr Daten und Informationen akquiriert werden, desto zielgenauer ist diese Werbeform und desto höher sind Umsatz und Gewinn, mit dem dann wieder neue Online-Angebote entwickelt werden können, die keinem anderen Zweck dienen, als neue Daten zu akquirieren. Daten und Informationen sind also der Motor, der den digitalen Kreislauf insbesondere im Internet am Laufen und in Bewegung hält.

Dass Geschäftsmodelle, die auf diesem Prinzip aufbauen, zwangsläufig in einem Spannungsverhältnis zum Datenschutz stehen, liegt auf der Hand. Sie unterlaufen den Grundsatz der Datensparsamkeit, da sie

jede Nutzerin bzw. jeden Nutzer und jedes Mitglied anhalten, so viele Daten und Informationen wie möglich von sich preiszugeben. Außerdem ignorieren sie das Prinzip der Datentransparenz, da es für einzelne Nutzerinnen und Nutzer nicht mehr nachvollziehbar ist, welche Daten von ihnen gespeichert werden und wie mit diesen im Einzelnen verfahren wird. So verlieren die Nutzerinnen und Nutzer in den sozialen Netzwerken die Kontrolle über ihre Daten, zumal sie kaum in der Lage sind, Daten, die sie einmal zur Verfügung gestellt haben, auch wieder zu löschen bzw. in ein anderes Netzwerk mitzunehmen, wenn sie einen Wechsel beabsichtigen.

Soll der Datenschutz diesen Geschäftsmodellen nicht zum Opfer fallen, müssen ihnen Grenzen gezogen werden. Dafür bedarf es konkreter Regelungen. Da das Interesse der Anbieter auf die lückenlose Digitalisierung des menschlichen Lebens und darauf gerichtet ist, die dabei gewonnnen Daten und Informationen komplett zu verwerten, kann diese Regulierung nicht Google, Facebook und Co. überlassen bleiben. Selbstregulierung und Selbstverpflichtung können nur subsidiär zum Zuge kommen. Verantwortlich ist in erster Linie der Staat und, da es um den Schutz von Grundrechten geht, der Gesetzgeber. Er muss die Rahmenbedingungen für entsprechende Geschäftsmodelle festlegen und notfalls auch über Kommerzialisierungsverbote nachdenken, etwa zugunsten von Kindern, die sich millionenfach in sozialen Netzwerken, insbesondere in Facebook, tummeln. Das Land, v.a. die Landesregierung tragen dafür nur eine mittelbare Verantwortung. Sie führt über den Bundesrat, da in erster Linie der Bund die für die geschilderten digitalen Zusammenhänge erforderlichen Regelungen schaffen kann. Die sich daraus ergebenden Möglichkeiten wurden von der Landesregierung bisher trotz diverser Initiativen noch nicht ausreichend genutzt. Dies gilt aber nicht nur für Rheinland-Pfalz. Vielmehr hat sich der Bundesrat insgesamt noch nicht mit dem gebotenen Nachdruck für eine ausreichende und abgewogene Regulierung eingesetzt.

Sorgen bereiten aber nicht nur Facebook und Co., Sorgen bereiten auch die Nutzerinnen und Nutzer bzw. Mitglieder dieser Online-Plattformen. In der Bundesrepublik sind mittlerweile 52,7 Millionen Personen über 14 Jahre online. Das sind 74,7 Prozent. Rheinland-Pfalz liegt genau im Durchschnitt und mit ebenfalls 74,7 Prozent im Vergleich zu den übrigen Bundesländern an siebter Stelle (vgl. (N)onliner Atlas 2011, S. 10; http://www.nonliner-atlas.de/ ). Was die Nutzung der Social Media Welt anbelangt, liegen die Rheinland-Pfälzerinnen und Rheinland-Pfälzer aber bundesweit mit 73 Prozent sogar an der Spitze. Das ist das Ergebnis des Social Media Atlas 2011 (vgl. http://www.faktenkontor.de/ ). Einerseits ist dies ein Zeichen für technische Aufgeschlossenheit, andererseits aber auch Anlass hinter diese Zahlen zu blicken.

Denn die Onliner – auch die rheinland-pfälzischen – geben in einem bisher nicht bekannten Umfang Daten und Informationen von sich preis, wobei immer deutlicher wird, dass die Online-Kommunikation dazu verführt, mehr von sich preiszugeben, als man dies bei einer Face-to-Face-Kommunikation tun würde. Nur zum Teil hängt dies damit zusammen, dass Kommunikationsvorgänge, die im Netz stattfinden, ihre eigenen Spielregeln haben, die den Nutzerinnen und Nutzern offenbar nicht immer bekannt sind, so wie ihnen auch die Funktionsbedingungen des Internets nicht ausreichend bewusst sind. Dazu gehört auch das sog. ewige Online-Gedächtnis. So lange es keinen digitalen Radiergummi und keine digitalen Verfallsdaten gibt, müssen sich die Online-Nutzerinnen und -Nutzer darauf einstellen, dass sie im Netz nicht mit der Gnade des Vergessens rechnen können.

Das richtige Verhalten im Netz, d.h. der verantwortungsvolle Umgang mit den eigenen Daten und der respektvolle Umgang mit den Daten anderer, kann allerdings nicht vom Staat, auch nicht von der Landesregierung, verordnet werden. Er muss von den Menschen erlernt werden. Dazu kann der Staat und kann auch unser Land Hilfestellungen anbieten und leisten. Rheinland-Pfalz tut dies in einem vergleichsweise großen Umfange. Im Mittelpunkt seiner Aktivitäten steht das Regierungsprogramm „Medienkompetenz macht Schule“. Teil dieses Programms sind die Schülerworkshops (vgl. Tz. I-4.3), die der LfD den weiterführenden Schulen im Lande zu aktuellen Datenschutzfragen anbietet. Zum großen Teil werden sie vom Bildungsministerium finanziert, mit dem zusammen auch das den Workshops zugrunde liegende fachliche und pädagogische Konzept ausgearbeitet wurde. Die Nachfrage nach diesen Workshops ist ernorm. Mehr als 6.000 Schülerinnen und Schüler wurden auf diese Weise binnen eines Jahres erreicht. Dies zeigt, dass der Datenschutz nicht mehr nur als Aufgabe von Gesetz und Kontrolle verstanden werden darf, sondern immer mehr zu einem Bildungs- und Erziehungsauftrag wird.

Die Vermittlung einer ausreichenden Medien- und Datenschutzkompetenz wird entscheidend dafür sein, ob die Bürgerinnen und Bürger sich und ihre Privatsphäre auch im Internetzeitalter behaupten können und ob sich unsere Demokratie auch als Lebensform

bewahren lässt. Datenschutzbewusstes Verhalten der Bürgerinnen und Bürger wird aber umgekehrt auch Vorraussetzung dafür sein, dass der Staat seine Überwachungs- und Kontrollmaßnahmen nicht unter Berufung auf datenschutzrechtliches Desinteresse der Bürgerinnen und Bürger immer weiter ausbaut.

Dass der Stellenwert des Datenschutzes im Internet fragil ist und auch mit besseren Gesetzen und mehr Datenschutzkompetenz fragil bleibt, ist im Übrigen systembedingt und damit in gewisser Weise unvermeidbar. Anonyme Angriffe auf Websites und die Veröffentlichung der digitalen Raubzüge und ihrer Beute bei Wikileaks und vergleichbaren Plattformen machen das immer wieder deutlich. Das Netz bietet keine völlige Sicherheit und der Staat keinen völligen Schutz vor digitalen Straßenräubern und virtueller Selbstjustiz. So gesehen bringt uns das Internet nicht nur „Frieden, Freiheit und Wohlstand“, wie Bundeswirtschaftsminister Rösler im September 2011 bei der Eröffnung der Internationalen Funkausstellung in Berlin ankündigte, sondern auch Selbstjustiz, digitale Opfer und staatliche Ohnmacht. Deshalb ist das Internet eben doch ein Stück „Wilder Westen“ im 21. Jahrhundert.

## 1.3 In der Cloud

Die technologische Entwicklung macht beim Internet nicht Halt und die datenschutzrechtlichen Probleme enden nicht bei den sozialen Netzwerken. Eine Ahnung von den Herausforderungen, die in der Zukunft auf den Datenschutz zukommen, vermittelt heute bereits das sog. Cloud Computing. Was ist darunter zu verstehen? Die Datenverarbeitung auf einer bei Anwenderinnen und Anwendern vorhandenen IT wird zunehmend als Auslaufmodell gesehen und Cloud Computing, d.h. die Datenverarbeitung in einer mehr oder weniger abstrakten „IT-Wolke“ als Revolution in der Computerbranche gesehen. So wie Strom aus der Steckdose kommt und beliebige Geräte versorgt, werden beim Cloud Computing IT-Leistungen bedarfsgerecht via Netzwerk bereitgestellt; Software, Infrastruktur für den Betrieb von Anwendungen, Speicherplatz oder Bandbreite können flexibel aus dem Netz bezogen werden, benötigt wird lediglich ein Endgerät mit Browser. Wer den Mailserver seines Internetproviders nutzt, dort ein Internetangebot auf einem virtuellen Webserver betreibt, seinen Kalender online führt oder Dokumente online bearbeitet, nutzt Cloud Computing.

Schätzungen zufolge sollen sieben Prozent der deutschen Unternehmen mit mehr als 100 Mitarbeiterinnen und Mitarbeitern Cloud Computing bereits nutzen, für 2011 wird für Deutschland ein Marktvolumen von ca. 56 Millionen Euro erwartet. Bis 2015 werden durchschnittliche Wachstumsraten von jährlich über 40 Prozent prognostiziert. Grundlage für diesen Wachstumstrend sei v.a. die Vielfalt der Anwendungsmöglichkeiten für kleine und mittlere Unternehmen, die nur Hardware und Personal einsparen möchten. Großunternehmen hingegen werden eher in die Lage versetzt, Lastspitzen abzufedern und flexibler zu agieren. Langfristig werde Cloud Computing einen beträchtlichen Teil traditioneller IT-Strukturen ersetzen. Heruntergebrochen auf die rheinland-pfälzische Wirtschaft mit ihrer größtenteils mittelständischen Struktur bedeutet dies einen wachsenden Markt für entsprechende Angebote. Ähnlich ist die Situation in der Verwaltung, insbesondere bei den Kommunen. Auch hier gibt es Überlegungen, Datenbestände auszulagern oder IT-Strukturen in der Cloud zu virtualisieren, um sich damit des Betriebs eigener Informationstechnik zu entledigen.

Nicht in die Wolke verlagert werden kann allerdings die datenschutzrechtliche Verantwortung der Cloud-Nutzerinnen und -Nutzer. Wo private Anwenderinnen und Anwender frei entscheiden können, ob sie ihre Daten unter nur wenig fassbaren Bedingungen in die Wolke legen, haben Wirtschaft und Verwaltung eine weitreichende Verantwortung für die Daten ihrer Kundinnen und Kunden, Klientinnen und Klienten oder Leistungsempfängerinnen und -empfänger. Diese Verantwortung kann aber nur noch eingeschränkt wahrgenommen werden. Ob Daten in Koblenz oder Kalkutta vorgehalten werden, welchem Recht sie dabei unterliegen, welche Stellen darauf zugreifen können oder welchen Sicherheits- und Datenschutzstand der Cloud-Anbieter gewährleistet, entzieht sich meist der Kenntnis und häufiger noch den Einwirkungsmöglichkeiten der Cloud-Nutzerin und -Nutzer. Vielfach besteht nicht mehr die Möglichkeit, die eingesetzte IT zu kontrollieren bzw. sie in der Gestaltung und beim Betrieb wirksam zu beeinflussen. Prüf- und Kontrollpflichten können dann faktisch nicht mehr wahrgenommen werden, entsprechende Vereinbarungen stehen nur auf dem Papier.

Möglich erscheint dies noch am ehesten dort, wo lediglich Datenhaltung, Bandbreiten oder Rechenleistung aus der Wolke bezogen werden. Beim konsequenten Einsatz kryptografischer Mechanismen bei der Datenspeicherung und der im Rahmen der Auftragsdatenverarbeitung entwickelten Mechanismen können bestimmte Szenarien datenschutzgerecht gestaltet werden. Wo jedoch personenbezogene Daten außerhalb einer wirksamen Kontrolle der Cloud-Nutzerinnen und -Nutzer verarbeitet werden, können die Risiken

unter den gegenwärtigen Bedingungen in der Regel nicht kompensiert werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich am 28./29. September 2011 mit der „Datenschutzkonformen Gestaltung und Nutzung von Cloud-Computing“ befasst (http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=dsb&ber=082_cloud). Außerdem hat der Arbeitskreis „Technik“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Anforderungen an datenschutzkonforme Cloud Computing-Lösungen in einer Orientierungshilfe zusammengefasst (http://www.datenschutz.rlp.de/downloads/oh/ak_oh_cloudcomputing.pdf).

Kernpunkte:

- Transparenz über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der angebotenen Dienstleistungen,
- ein verlässliches IT-Sicherheits- und Datenschutzkonzept,
- Vereinbarungen zum Ort der Datenverarbeitung und zur Benachrichtigung bei geplanten Veränderungen,
- Kontroll- und Einwirkungsmöglichkeiten der Cloud-Nutzerinnen und -Nutzer und
- Regelungen zur Umsetzung von Auskunftsansprüchen Betroffener und zur Datenlöschung.

Datenschutzrechtlich problematisch ist auch der **Zugriff US-amerikanischer Sicherheitsbehörden** (vgl. Tz. I-2.1.3) auf die Daten, die in der Cloud durch Rechnersysteme US-amerikanischer Unternehmen verarbeitet werden. Die Datenschutzbeauftragten des Bundes und der Länder haben sich deshalb darum bemüht, ein einheitliches europäisches Votum dazu zu erreichen. In ihrem Schreiben an die Art. 29-Gruppe, das sie auch an die Europäische Kommission und an die Bundesregierung geleitet haben, führen sie aus:

„Die von den Zugriffen der ausländischen Behörden betroffenen personenbezogenen Daten unterliegen in den jeweiligen Staaten oft keinen datenschutzrechtlichen Restriktionen, die europäischen Standards auch nur ansatzweise genügen könnten. Die Zweckbindung, die Beachtung des Erforderlichkeitsgrundsatzes, die Datenlöschung nach Zweckerfüllung, die Gewährleistungen der Betroffenenrechte und des Rechtsschutzes in Datenschutzfragen sind unseres Wissens z.B. in den USA nicht gewährleistet.“

Deshalb verlangen die Datenschutzbeauftragten, dass mit den zuständigen Stellen in den USA geklärt wird, wie das im deutschen Grundgesetz, in der Charta der Grundrechte der Europäischen Union und im Vertrag von Lissabon garantierte Grundrecht auf Datenschutz im Hinblick auf diese Herausforderung gewährleistet werden kann.

Der LfD hält diese Problematik angesichts der sich stetig ausbreitenden Verlagerung von Datenverarbeitungsprozessen in die Cloud für bedeutsam und unterstützt alle Bestrebungen, die europäischen Datenschutzstandards auch in diesem Bereich wirksam werden zu lassen.

## 1.4 In der Zukunft

Wenn in Zeiten des Internets und der Cloud ein hinreichender Datenschutz nur noch mühsam zu gewährleisten ist, was wird dann erst in der Zukunft sein? Wird es so sein, wie die Wortführer der digitalen Szene es seit einiger Zeit bereits prognostizieren? „You have no privacy anymore, so get over it“. So beschied der damalige CEO von Sun Microsystems, Scott McNealy schon 1997 die Onliner. Ganz auf seiner Linie ist auch Eric Schmidt, der frühere Chef von Google, für den die Privatsphäre nur ein Rückzugsgebiet für jene ist, die etwas zu verbergen haben. „Wenn es etwas gibt, von dem Sie nicht wollen, dass es irgendjemand erfährt, sollten Sie es vielleicht ohnehin nicht mehr tun“, sagte er während eines Interviews mit dem Fernsehsender CNBC im Dezember 2009, und auf der Internationalen Funkausstellung in Berlin rief er 2010 die Menschen auf, noch mehr Daten von sich preiszugeben: „Letztlich geht es buchstäblich um all Ihre Informationen. E-Mails, Sachen, die Ihnen am Herzen liegen. Mit Ihrer Erlaubnis natürlich.“ Auch von Mark Zuckerberg kennt man ähnliche Äußerungen. Im Januar 2010 war davon zu lesen, dass er die Privatsphäre für eine „alte Konvention“ halte, die überholt und nicht mehr zeitgemäß sei. Angesichts solcher Stellungnahmen ist es kein Wunder, dass der frühere Präsident Prof. Hans-Jürgen Papier des Bundesverfassungsgerichts, das die Privatsphäre so konsequent wie sonst niemand im Lande verteidigt, mit dramatischen Worten vor einem „Supergau für den Datenschutz“ warnte. Wohin geht also die digitale Reise, und wird der Datenschutz noch ein aufmerksamer Reisebegleiter sein?

IBM als einer der weltgrößten Hersteller von Informationstechnik bezeichnet die kommenden zehn Jahre als „Decade of Smart“, in der Verkehr, Energienutzung, Gesundheitswesen oder Wohnen und Leben von smarten, sprich mit Informationstechnik versehenen kommunikationsfähigen Lösungen, gekennzeichnet sein werden. Für das „Internet der Dinge“, das über

kurz oder lang Sensoren, Energiezähler, RFID-bestückte Objekte und Alltagsgeräte bis hin zu Kühlschränken, Kaffeemaschinen, Rolladensteuerungen oder Rasensprengern umfassen soll, werden bis 2020 fünzig Milliarden teilnehmende Geräte prognostiziert. Viele davon werden Daten produzieren, die personenbeziehbar Nutzungsgewohnheiten erkennen lassen. Ergänzend liefern die für 2013 geschätzten 900 Millionen GPS-fähigen Geräte wie Smartphones, Digitalkameras oder Navigationslösungen Standortdaten und ermöglichen Bewegungsprofile ihrer Nutzerinnen und Nutzer oder, in Verbindung mit sog. Location-based-Services, auch Konsum- und Verhaltensprofile.

Der Umfang der daraus resultierenden Datenbestände wird immens sein. Gegenwärtig werden laut Eric Schmidt, dem ehemaligen Google-Chef, in zwei Tagen so viele Daten erzeugt wie zuvor vom Beginn der menschlichen Zivilisation bis zum Jahr 2003. Im Telekommunikationsbereich lag z.B. das Datenaufkommen allein in den Netzen der Deutschen Telekom im Jahr 2011 bei 400.000 Terabyte im Monat. Ausgedruckt entspräche dies einem Papierstapel, der mehrfach von der Erde bis zum Mond reicht.

Um diese als „Big Data“ bezeichneten Datenbeständen überhaupt handhaben zu können, entstehen zur Zeit neue Ordnungs- und Sortiermöglichkeiten. Seit kurzem ist es etwa möglich, ein Petabyte (= 1.000 Terabyte) an Daten innerhalb einer halben Stunde zu sortieren; für diesen Rekord wurde die Aufgabe auf ein System von 8.000 Servern verteilt. Diese technische Leistung ist die Grundlage für spezielle Vorhersagemodelle. Nutzungs- und Standortdaten werden zu Kommunikations-, Konsum-, Verhaltens- und Bewegungsprofilen verdichtet, Aggregation und Kontextinformationen erlauben bereits heute Voraussagen, wo sich eine Person zu einem bestimmten Zeitpunkt aufhalten und was sie dann tun wird.

Wie hoch der Preis für solche Erkenntnisse sein wird, wissen wir heute noch nicht. Aber die Erfahrung lehrt, dass wir dafür zahlen werden müssen, mit individuellen Opfern und gesellschaftlichen Risiken. Zu den harmlosen Prognosen gehört es, dass sich künftig aufgrund von Sicherheitsmängeln Stalkerinnen und Stalker in einschlägigen Systemen Zugang zu den Daten verschaffen, die sie für die Ortsermittlung ihrer Opfer verwenden können.

Wirtschaft und Wissenschaft, Politik und Online-Pioniere machen es sich zu leicht, wenn sie zugestehen, dass solche Entwicklungen aufmerksam beobachtet und bewertet werden müssten und dass „man dann auch bei der Gesetzgebung flexibel zu sein habe“. Wir erleben es ja bereits derzeit, dass die Flexibilität der Gesetzgeber oft genug nur darin besteht, es bei den alten Regelungen zu belassen und ihre Anpassung an die neue Zeit zu versäumen.

### 1.5 In der Gesamtbeurteilung

Den Stellenwert des Datenschutzes im Lande bestimmen also nicht nur der Landtag, die Landesregierung und die übrigen Landesbehörden, sondern auch die Unternehmen, die ihren Sitz in Rheinland-Pfalz oder außerhalb des Landes haben, ihre Leistungen aber – wie Facebook und Co. – auch den Rheinland-Pfälzerinnen und Rheinland-Pfälzern anbieten. Hinzu kommen die Medien und v.a. die Menschen selbst, die mit ihrem öffentlichen und privaten Verhalten das Datenschutzniveau wesentlich mit beeinflussen. Versucht man, diese Faktoren zu bewerten, dann ergibt sich ein diffuses Gesamtbild.

Einerseits ist das Datenschutzbewusstsein innerhalb der Landesverwaltung respektabel und die Bereitschaft von Landtag und Landesregierung, den Datenschutz auszubauen, durchaus vorhanden. Andererseits betreiben Facebook und Co. – auch in Rheinland-Pfalz – ein Geschäftsmodell, das in einem kaum auflösbaren Spannungsverhältnis zum Datenschutz steht. Noch wichtiger ist aber, dass wir in der Bundesrepublik Deutschland und damit auch in Rheinland-Pfalz trotz der großen Zahl einschlägiger Entscheidungen des Bundesverfassungsgerichts keinen gesellschaftlichen Konsens zur Wertigkeit und Bedeutung des Datenschutzes gefunden haben.

Bei den Bürgerinnen und Bürgern ist der Datenschutz als allgemeine Zielsetzung zwar anerkannt, als Maßstab für das eigene Verhalten aber eher nachrangig. Während die einen vorgeben, sie hätten nichts zu verbergen, protestieren die anderen gegen den „Überwachungsstaat“. Während die für den Verbraucherdatenschutz zuständige Bundesministerin ihren Account aus Protest gegen die zahlreichen Datenschutzverstöße von Facebook kündigt, beantragen Millionen Verbraucherinnen und Verbraucher zur selben Zeit die Mitgliedschaft. Sie tun dies, obwohl 70 Prozent der Mitglieder in Datenschutzfragen kein Vertrauen zu Facebook haben. Obwohl mittlerweile auch viele Medien sehr kritisch über Facebook berichten, betreiben sie doch auf dieser Plattform eine Fanpage.

Wie widersprüchlich das Verhalten vieler Beteiligter ist, zeigt auch die Diskussion über den Beschäftigtendaten-

schutz (vgl. Tz. I-3.1). Obwohl das Massenscreening bei der Deutschen Bahn und der Deutschen Telekom vor wenigen Jahren allgemein als Datenschutzskandal bewertet wurde und den Bundesinnenminister sogar veranlasste, einen Datenschutzgipfel einzuberufen, sollen diese Screening-Verfahren jetzt gesetzlich legitimiert werden – wenn es denn zu einem Beschäftigtendatenschutzgesetz kommt. Denn obwohl die Präsidentin des Bundesarbeitsgerichts ein solches Gesetz dringend gefordert hat, stehen sich Arbeitgeberverbände und Gewerkschaften in dieser Sache so konträr und kompromisslos gegenüber, dass sie die ihnen jeweils nahe stehenden politischen Parteien und Parlamentsfraktionen in einen Konflikt treiben, der für den Datenschutz keinen Vorteil, sondern nur Nachteile bringen wird.

Diese Beispiele lassen sich beliebig fortsetzen. Sie zeigen, dass viele Akteurinnen und Akteure den Datenschutz zwar oft im Munde führen, aber trotzdem auf ihn verzichten, wenn er eigenen – persönlichen, wirtschaftlichen oder politischen – Vorteilen im Wege steht. Dies ist am Ende wohl auch ein Indiz dafür, dass es bisher offenbar nicht gelungen ist, den Bürgerinnen und Bürgern sowie Verbraucherinnen und Verbrauchern, den Arbeitnehmerinnen und Arbeitnehmern und digitalen Netzwerkerinnen und Netzwerkern den persönlichen Wert des informationellen Selbstbestimmungsrechts plausibel zu machen. So gesehen ist die Situation des Datenschutzes – auch in Rheinland-Pfalz – durchaus prekär. Er genießt zwar öffentliche Aufmerksamkeit wie selten zuvor, auch die wohlwollende Unterstützung staatlicher Organe im Lande, allerdings fehlt es ihm wohl auch an Überzeugungskraft und an nachvollziehbaren Konzepten, und selbst wo diese vorliegen, zögert man, sie umzusetzen. Wenn man bedenkt, welche Entwicklungen auf uns zukommen und wie sehr die Cloud, RFID, die sonstigen „smarten“ Techniken und „Big Data“ die Welt verändern und unsere Privatsphäre bedrohen werden, dann spricht manches dafür, dass der Datenschutz, so wie er vom Bundesverfassungsgericht für den staatlichen Bereich konzipiert worden ist, für den nicht-staatlichen bald nur noch ein romantisches Ideal darstellen wird.

Wie kann von Rheinland-Pfalz aus diese Entwicklung beeinflusst werden? Auch in den 1970er Jahren kamen von Rheinland-Pfalz mit dem Landesdatenschutzgesetz richtungsweisende Impulse für den Datenschutz in der Bundesrepublik. Warum sollte es nicht gelingen, an diese Tradition anzuknüpfen? Auch wenn es keine Patentrezepte dafür gibt, gibt es doch genügend Möglichkeiten, die problematische Entwicklung zu beeinflussen: Der Landtag sollte die skizzierte Entwicklung öfter als dies bisher der Fall war in seinen Plenarsitzungen thematisieren und die Landesregierung sie zum Gegenstand von Bundesratsinitiativen machen. Die Themen liegen auf der Hand: Sie reichen von den sozialen Netzwerken bis zu dem in der Diskussion befindlichen europäischen Rechtsrahmen. Beide – der Landtag und die Landesregierung – müssten in Datenschutzfragen mit gutem Beispiel vorangehen. Das betrifft auch die Fanpages bei Facebook. Davon sollte Abstand genommen werden, weil sie in datenschutzrechtlicher Hinsicht sehr problematisch sind (vgl. Tz. I-3.2.2). Weil nicht nur die Fanpages dem Datenschutz zuwiderlaufen, sondern Facebook insgesamt, sollten Landtag und Landesregierung ihr Augenmerk auch stärker auf alternative Netzwerke ohne zentrale Datenspeicher lenken. Solche Netzwerke gibt es; sie sollten aber stärker als bisher unterstützt werden. Landtag bzw. Landesregierung sollten außerdem einen runden Tisch „Digitale Kultur und Medienkompetenz“ einsetzen. Mit Hilfe der Zukunftsinitiative Rheinland-Pfalz ließen sich v.a. Fragen der Entwicklung der Informationstechnologie aufarbeiten, und auch die im Koalitionsvertrag vereinbarte Landesdatenschutzkonferenz könnte für diese Zwecke genutzt werden. Aufklärungskampagnen, die in anderen Bereichen durchaus erfolgreich waren, könnten auch die digitale Aufklärung befördern, wie überhaupt der Datenschutz noch stärker als bisher als Bildungs- und Erziehungsaufgabe begriffen werden muss, wobei insbesondere auch die Eltern von jungen Onlinern einzubeziehen sind. Im hessischen Landtag wurde der Entwurf für ein Gesetz zur Förderung der Medienkompetenz in Hessen eingebracht (vgl. Hessischer Landtag Drs. 18/4218) – ein kreativer Vorschlag, wie man die Problematik anpacken könnte.

Natürlich könnten auch die Aktivitäten des LfD verstärkt werden. Er könnte insbesondere digitale Dienstleistungen oder digitale Produkte auditieren. Man muss ihn dazu personell nur in die Lage versetzen. Es gibt also genügend Möglichkeiten, auch von Rheinland-Pfalz aus tätig zu werden. Nach Lage der Dinge wird es aber zu einer entscheidenden Richtungsänderung nur dann kommen, wenn das Bundesverfassungsgericht die Gelegenheit zu einer zweiten Volkszählungsentscheidung erhält, dieses Mal für den privaten und privatwirtschaftlichen Bereich. Es macht optimistisch, dass der gegenwärtige Präsident des Bundesverfassungsgerichts, Andreas Voßkuhle, im Dezember 2011 in einem „Spiegel“-Interview deutlich gemacht hat, dass mit einer solchen Entscheidung über kurz oder lang durchaus gerechnet werden kann, wobei sich dann allerdings der Europäische Gerichtshof ebenfalls entsprechend positionieren müsste.

# 2. Entwicklung des Datenschutzrechts

Das Datenschutzniveau in Staat und Gesellschaft hängt von mehreren Faktoren ab, v.a. von den Datenschutzgesetzen. Sie bilden die Grundlage des Datenschutzes. Für ihren Erlass sind die Europäische Union, der Bundestag und die Bundesregierung und – auf Landesebene – der Landtag und die Landesregierung verantwortlich, wobei sich die Kompetenz des Landes im Wesentlichen auf den Datenschutz innerhalb der Regierung und der Verwaltung beschränkt.

Zu den Aufgaben des LfD gehört es, die Entwicklung des Datenschutzrechts auf diesen Ebenen zu beobachten und bei Bedarf auch darauf Einfluss zu nehmen. Dies geschieht, was das europäische und nationale Datenschutzrecht anbelangt, v.a. in Stellungnahmen gegenüber der Landesregierung, die – wie der Landtag auch – vom LfD zu beraten ist. Angesichts der Fülle der einschlägigen Regelungen bzw. Regelungsabsichten und wegen der begrenzten personellen Kapazitäten des LfD ist dies allerdings nur punktuell möglich. V.a. die datenschutzrechtlichen Entwicklungen, die sich auf der europäischen Ebene vollzogen haben und noch vollziehen werden, standen nicht immer im Mittelpunkt der Aufmerksamkeit des LfD. Es gab andere Prioritäten. Dies wird und muss sich allerdings ändern, nicht zuletzt deshalb, weil das Datenschutzrecht künftig stärker als bisher von der europäischen Ebene bestimmt werden wird.

## 2.1 Internationales Recht und Europarecht

### 2.1.1 Novellierung des europäischen Rechtsrahmens

Die maßgeblichen datenschutzrechtlichen Regelungen auf europäischer Ebene sind veraltet. Sie stammen aus dem Jahre 1995 und damit aus einer Zeit, als das Internet den Bürgerinnen und Bürgern noch nicht zur Verfügung stand. Eine Überarbeitung dieser Regelung – der Europäischen Datenschutzrichtlinie 95/94 EG – ist somit überfällig, zumal die Europäische Union mit dem Vertrag von Lissabon im Dezember 2009 eine Grundrechtscharta erhalten hat, in deren Art. 8 jeder Person das Grundrecht auf Schutz der sie betreffenden Daten garantiert wird. Deshalb ist es auch zu begrüßen, dass sich die Europäische Kommission seit Mitte 2009 mit der Novellierung des europäischen Rechtsrahmens befasst. Zu dem im November 2010 vorgestellten „Gesamtkonzept für den Datenschutz in der Europäischen Union“ haben auch die Datenschutzbeauftragten Stellung genommen, wobei sie deutlich gemacht haben, dass sie, eine von den Mitgliedstaaten auszufüllende Richtlinie einer unmittelbar geltenden Verordnung vorziehen würden. Im Übrigen hat die Kommission folgende Kernziele formuliert:

- Stärkung der Rechte des Einzelnen, damit die Sammlung und Nutzung personenbezogener Daten auf das erforderliche Mindestmaß beschränkt wird.
- Jede Person sollte klar und in transparenter Weise darüber informiert werden, wie, warum, von wem und wie lange ihre Daten gesammelt und verwendet werden.
- Jede Person sollte die Möglichkeit haben, der Verarbeitung ihrer personenbezogenen Daten nach vorheriger Aufklärung freiwillig zuzustimmen, z.B. beim Online-Surfen, und jede Person sollte das „Recht vergessen zu werden“ haben, wenn ihre Daten nicht länger gebraucht werden oder sie will, dass ihre Daten gelöscht werden.
- Stärkung der Binnenmarktdimension durch Verringerung des Verwaltungsaufwands für Unternehmen und die Gewährleistung gleicher Rahmenbedingungen. Gegenwärtig herrschen nach Auffassung der Kommission Unterschiede bei der Umsetzung der Datenschutzbestimmungen der Europäischen Union, und nicht immer sei klar, wessen Vorschriften gelten. Dies beeinträchtige den freien Verkehr personenbezogener Daten in der Europäischen Union und bewirke höhere Kosten.
- Überarbeitung der Datenschutzbestimmungen im Bereich der Zusammenarbeit der Polizei- und Strafjustizbehörden, damit personenbezogene Daten Einzelner auch hier geschützt werden. Die Kommission überprüft zur Zeit auch die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, wonach die Unternehmen Kommunikationsdaten über einen Zeitraum zwischen sechs Monaten und zwei Jahren speichern müssen.
- Gewährleistung eines hohen Schutzniveaus bei außerhalb der Europäischen Union übermittelten Daten durch die Verbesserung und Erleichterung von Verfahren für den internationalen Datentransfer. Die Europäische Union strebt bei der Zusammenarbeit mit Drittstaaten dasselbe Schutzniveau an und will sich weltweit für hohe Datenschutzstandards einsetzen.
- Wirksamere Durchsetzung der Vorschriften durch die Stärkung und weitere Harmonisierung der Aufgaben und Befugnisse der Datenschutzbehörden. Nach Auffassung der Kommission bedarf es einer besseren Zusammenarbeit und Abstimmung, um eine konsequentere Anwendung der Datenschutzbestimmungen im gesamten Binnenmarkt zu gewährleisten.

Um sich über den Stand der Novellierung und den zu erwartenden Inhalt genauer zu informieren, hat der LfD Ende November 2011 in Brüssel Gespräche mit

Vertreterinnen und Vertretern der Kommission und des Europäischen Parlaments geführt. Dabei wurde deutlich, dass die für Anfang 2012 angekündigten Regelungsvorschläge mindestens aus dem Entwurf einer Verordnung und dem Entwurf einer Richtlinie bestehen werden, wobei die Richtlinie offenbar für den Bereich von Justiz und Polizei vorgesehen ist. Diese Erwartung scheint sich zu bestätigen, wie die beiden vorzeitig bekannt gewordenen und im Internet abrufbaren Entwürfe deutlich machen. Auch wenn davon auszugehen ist, dass diese Entwürfe im Abstimmungsverfahren innerhalb der Kommission noch verändert werden, bevor sie dem Europäischen Parlament vorgelegt werden, kann jetzt bereits vermutet werden, dass das angestrebte europäische Datenschutzrecht zwar zu mehr Rechtssicherheit für alle Beteiligten führen wird, dass dies aber womöglich in der Bundesrepublik Deutschland mit einer Nivellierung des Datenschutzniveaus einhergeht. Der LfD hat bereits bei seinem Brüsseler Besuch Verständnis dafür geäußert, wenn das europäische Datenschutzrecht künftig im Interesse der Wirtschaft den Datenverkehr erleichtern wird, zugleich aber auch davor gewarnt, dies durch einen Abbau individueller Datenschutzrechte zu erkaufen. Dies würde sich letztlich auch für die Wirtschaft nicht bezahlt machen.

Im Übrigen bleibt abzuwarten, ob sich die Absicht, eine EU-Datenschutzverordnung zu erlassen, überhaupt durchsetzen lässt. Für die Bundesrepublik Deutschland selbst würde sie keine Vorteile bringen. Im Gegenteil: Sie würde die gewachsene Datenschutzkultur einschließlich unserer Datenschutzgesetze und der ihnen zugrunde liegenden Entscheidungen des Bundesverfassungsgerichts zur Makulatur machen. Umso wichtiger wird es sein, dass auch vom rheinland-pfälzischen Landtag und der Landesregierung alles unternommen wird, um das Europäische Parlament und den Europäischen Rat, die beide dem Projekt zustimmen müssen, noch zum Umdenken zu bewegen.

### 2.1.2 Europäischer Gerichtshof

Was in der Bundesrepublik Deutschland schon längst Realität ist, könnte sich auch auf europäischer Ebene wiederholen. Der Europäische Gerichtshof könnte sich zu einem maßgeblichen Hüter des Datenschutzgrundrechtes entwickeln. Mindestens drei Entscheidungen könnten dies nahe legen.

Am 9. März 2010 hat der Europäische Gerichtshof festgestellt, dass die für die Kontrolle der Datenverarbeitung im nicht-öffentlichen Bereich zuständigen Stellen der Länder entgegen Art. 28 der Europäischen Datenschutzrichtlinie nicht völlig unabhängig sind (Urteil des Europäischen Gerichtshof vom 9. März 2010, Az. C-518/07). Völlige Unabhängigkeit bedeute nicht allein, dass eine Einflussnahme von den zu kontrollierenden datenverarbeitenden Stellen auszuschließen sei (funktionelle Unabhängigkeit). Vielmehr sei der Begriff der völligen Unabhängigkeit in einem umfassenden Sinne zu verstehen. Es müsse gewährleistet sein, dass keinerlei politische oder institutionelle Einflussnahme, etwa im Sinne einer Aufsicht über die Datenschutzaufsichtsbehörde stattfinde. Schon der Anschein einer solchen möglichen Einflussnahme müsse ausgeschlossen werden. Auch wenn diese Entscheidung in den Mitgliedsstaaten der Europäischen Union zum Teil heftig kritisiert wurde, übrigens auch in der Bundesrepublik Deutschland und hier nicht nur von der Exekutive, sondern zum Teil auch von der Rechtslehre, ist sie konsequent und im Sinne der Datenschutzbeauftragten. In den Bundesländern hat sie auch zu den notwendigen gesetzgeberischen Korrekturen geführt. Darauf wird an anderer Stelle noch näher eingegangen (vgl. Tz. I-2.3.1).

Am 9. November 2010 hatt der Europäische Gerichtshof auf Vorlage des Verwaltungsgerichts Wiesbaden des Weiteren entschieden, dass die europarechtlichen Regelungen zur ausnahmslosen und umfassenden Veröffentlichung von Name, Gemeinde und Subventionshöhe der Empfängerinnen und Empfänger europäischer Agrarsubventionen ungültig sei. Das informationelle Selbstbestimmungsrecht der betroffenen Landwirtinnen und Landwirte sei durch die angegriffene Regelung nicht ausreichend beachtet worden (Urteil des Europäischen Gerichtshofs vom 9. November 2010, Az. C-92/09, C-93/09; vgl. Tz. II-2.3).

Im November 2011 nahm der Europäische Gerichtshof auch zu der in der Rechtslehre und der Rechtsprechung bis dahin umstrittenen Frage Stellung, ob die sog. IP-Adressen personenbezogene Daten seien (Urteil des Europäischen Gerichtshofs vom 24. November 2011, Az. C-70/10; vgl. Tz. II-1.5). Die Antwort des Gerichts fiel ebenso knapp wie spektakulär aus: „Ja“.

Allerdings: Ende November 2011 hat der Europäische Gerichtshof auch zu einer Grundsatzfrage Stellung genommen, die bei der im Jahre 2012 anstehenden Novellierung der EU-Datenschutzrichtlinie ebenfalls eine entscheidende Rolle spielen wird: Darf ein Mitgliedsstaat das vorgegebene europäische Datenschutzniveau erheblich überschreiten, wenn dadurch der freie Datenverkehr in Europa eingeschränkt wird? Die Antwort des Europäischen Gerichtshofs ist eindeutig: Nein, ein Mitgliedstaat hat nicht die Freiheit, einen weitergehenden Datenschutz auf Kosten des freien Datenverkehrs anzustreben. Das wird bei der kommenden Neuregelung des europäischen

Datenschutzes besonders Deutschland treffen, das mit erheblichem Aufwand ein besonders hohes Datenschutzniveau angestrebt und verwirklicht hat (Urteil des Europäischen Gerichtshofs vom 24. November 2011, Az. C-468/10, C-469/10).

Es ist zu hoffen, dass der Europäische Gerichtshof – trotz dieser aus bundesrepublikanischer Datenschutzsicht problematischen Entscheidung – für das Datenschutzgrundrecht seiner Bürgerinnen und Bürger Sorge tragen wird. Die Erfahrungen in der Bundesrepublik haben gezeigt, dass der Datenschutz auf entsprechende höchstrichterliche Entscheidungen angewiesen ist. So wie z.B. die sog. Vorratsdatenspeicherung (vgl. Tz. II-8.2.4) im März 2010 vom Bundesverfassungsgericht für verfassungswidrig erklärt wurde, sollte dem Europäischen Gerichtshof Gelegenheit gegeben werden, auch die der Vorratsdatenspeicherung zugrunde liegende EU-Richtlinie zu beanstanden. Denn zu den EU-Vorschriften, deren Vereinbarkeit mit Art. 8 der EU-Grundrechtscharta fragwürdig ist, gehört auch diese Richtlinie. Darauf hat u.a. die Bundesjustizministerin hingewiesen. Der LfD teilt ihre Bedenken.

### 2.1.3 Abkommen mit den USA

Die rechtlichen und faktischen Möglichkeiten von US-amerikanischen Sicherheitsbehörden, auf Daten europäischer Bürgerinnen und Bürger zuzugreifen, sind ebenso vielfältig wie datenschutzrechtlich problematisch.

Dies betrifft zunächst die Speicherung und Auswertung von sog. Finanztransaktionsdaten nach dem **„SWIFT"-Abkommen**. Zweck des Abrufs dieser Daten ist es, den internationalen Kampf gegen den Terrorismus zu unterstützen. Einzelheiten können in den beiden letzten Tätigkeitsberichten nachgelesen werden (vgl. 21. Tb., Tz. 2.7, 22.3 und 22. Tb., Tz. 2.1.1). Zwar räumt dieses Abkommen vom August 2010 den betroffenen Bürgerinnen und Bürgern ein Recht auf Auskunft, Berichtigung, Löschung oder Sperrung ein. Doch ist vollkommen unklar, wie dieses Recht durchgesetzt werden kann, wenn die Daten erst einmal in den USA sind. Der Umfang der zu übermittelnden Daten ist immer noch sehr groß, ebenso ist die Speicherungsdauer von fünf Jahren unverhältnismäßig lang. Dies alles ist vor dem Hintergrund zu betrachten, dass es sich um sehr sensible Zahlungsverkehrsdaten handelt und meistens solche Personen betroffen sind, die gar nicht in terroristische Machenschaften involviert sind.

Auch die notwendige Kontrolle lässt zu wünschen übrig: Als Kontrollinstanz wurde nämlich Europol bestimmt. Hier soll überprüft werden, ob die an „SWIFT" gerichteten Auskunftsbitten durch die USA auch den im Abkommen festgelegten Anforderungen entsprechen. Allerdings befindet sich Europol dabei in einem Interessenkonflikt. Denn Europol profitiert als Polizeibehörde selbst von den Auswertungen durch die US-Behörden (vgl. Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17. März 2011 „Gravierende Defizite bei der Umsetzung des ‚SWIFT'-Abkommens – dringender Handlungsbedarf auf nationaler und europäischer Ebene"). Die europäischen Datenschutzbeauftragten haben sich zuletzt im Sommer 2011 gegenüber der US-Regierung für einen besseren Datenschutz beim sog. „SWIFT"-Abkommen eingesetzt. Man kann also sicher sagen: Fortsetzung folgt.

Datenschutzrechtlich problematisch ist im Übrigen auch der Zugriff US-amerikanischer Sicherheitsbehörden bei der **Fluggastdatenspeicherung** (vgl. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17. März 2011 „Keine Vorratsspeicherung und Rasterung von Flugpassagierdaten!"). Zentraler Gegenstand des Entwurfs ist die systematische Erfassung der Daten aller Fluggäste, die EU-Außengrenzen überqueren. Diese Daten aus den Buchungssystemen der Fluggesellschaften sollen anlass- und verdachtsunabhängig an eine nationale Zentralstelle der Sicherheitsbehörden übermittelt und regelmäßig für fünf Jahre gespeichert werden. Ziel soll es sein, damit Personen ausfindig zu machen, die in Terrorismus oder schwere Kriminalität verwickelt sein könnten. Diese Form von Vorratsdatenspeicherung und Rasterung von Passagierdaten ist nach Auffassung der Konferenz der Datenschutzbeauftragten mit dem grundgesetzlich garantierten Recht auf informationelle Selbstbestimmung unvereinbar.

### 2.1.4 Datenübermittlungen an US-amerikanische Unternehmen und das „Safe Harbor"-Abkommen

Im Berichtszeitraum entstanden erhebliche Zweifel, ob sich US-amerikanische Unternehmen wirklich an die Anforderungen halten, die von den „Safe Harbor-Principles" gefordert werden.

Safe Harbor (englisch für „Sicherer Hafen") ist eine besondere Datenschutzvereinbarung zwischen der Europäischen Union und den USA, die es europäischen Unternehmen ermöglicht, personenbezogene Daten legal in die USA zu übermitteln. Die EG-Datenschutzrichtlinie verbietet es grundsätzlich, personenbezogene Daten aus EU-Mitgliedsstaaten in Staaten zu übertragen, die über kein dem EG-Recht vergleichbares Datenschutzniveau verfügen. Dies trifft auf die USA zu, da diese keine umfassenden gesetzlichen Regelungen kennen, die den Standards der Europäischen Gemeinschaften

entsprechen. Damit der Datenverkehr zwischen den USA und der Europäischen Union nicht zum Erliegen kommt, wurde zwischen 1998 und 2000 ein besonderes Verfahren entwickelt. US-Unternehmen können dem Safe Harbor Abkommen beitreten und sich auf der entsprechenden Liste des US-Handelsministeriums eintragen lassen, wenn sie sich verpflichten, die „Safe Harbor-Principles" (englisch für „Grundsätze des sicheren Hafens") und die dazugehörenden – verbindlichen – Frequently Asked Questions (FAQ) zu beachten. Im Jahr 2000 hat die Europäische Union anerkannt, dass bei den Unternehmen, die dem Safe Harbor-System beigetreten sind, ein ausreichender Schutz besteht. Bislang sind mehr als 1.000 Unternehmen dem Safe Harbor-Abkommen beigetreten, darunter Microsoft, General Motors, Amazon.com, Google, Hewlett-Packard und Facebook. (Quelle: Wikipedia 2011)

Diese Zweifel gründeten auf der australischen Studie „The US Safe Harbor – Fact or Fiction?" vom Dezember 2008. Im Mittelpunkt der Kritik europäischer Datenschutzbehörden steht die mangelnde Kontrolle der Unternehmen. Bislang kann ein US-Unternehmen die Mitgliedschaft durch Selbsterklärung erlangen, die sog. Selbstzertifizierung, und dies dem Department of Commerce mitteilen, um sich auf einer zentralen Liste eintragen zu lassen. Eine Überprüfung erfolgt nicht. Zuständig für die Verfolgung von Verstößen gegen Safe Harbor ist die Federal Trade Commission (FTC). Als für den Verbraucherschutz zuständige Behörde kann sie gegen unfaire und irreführende Praktiken vorgehen. Erstmalig wurden 2009 von der FTC Maßnahmen gegen Unternehmen ergriffen, die fälschlicherweise behauptet hatten, sich nach Safe Harbor selbst zertifiziert zu haben. Eine Überprüfung der Einhaltung der Safe Harbor-Grundsätze – Informationspflicht, Wahlmöglichkeiten, Weitergabe, Sicherheit, Datenintegrität, Auskunftsrecht und Durchsetzung – ist nicht erfolgt. Es bestehen Bedenken, ob dieses Konzept aufrecht erhalten werden kann, wenn das Department of Commerce nicht die Einhaltung der Selbstverpflichtungen der an Safe Harbor teilnehmenden Unternehmen in einem höheren Maße kontrolliert. Der „Düsseldorfer Kreis" hat mit Beschluss vom 29. April 2010 unter der Überschrift „Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen" folgende Position formuliert:

„Solange eine flächendeckende Kontrolle der Selbstzertifizierungen US-amerikanischer Unternehmen durch die Kontrollbehörden in Europa und den USA nicht gewährleistet ist, trifft auch die Unternehmen in Deutschland eine Verpflichtung, gewisse Mindestkriterien zu prüfen, bevor sie personenbezogene Daten an ein auf der Safe Harbor-Liste geführtes US-Unternehmen übermitteln.

Die obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich weisen in diesem Zusammenhang darauf hin, dass sich Daten exportierende Unternehmen bei Übermittlungen an Stellen in die USA nicht allein auf die Behauptung einer Safe Harbor-Zertifizierung des Datenimporteurs verlassen können. Vielmehr muss sich das Daten exportierende Unternehmen nachweisen lassen, dass die Safe Harbor-Selbstzertifzierungungen vorliegen und deren Grundsätze auch eingehalten werden. Mindestens muss das exportierende Unternehmen klären, wann die Safe Harbor-Zertifizierung des Importeurs erfolgte. Eine mehr als sieben Jahre zurückliegende Safe Harbor-Zertifizierung ist nicht mehr gültig. Außerdem muss sich das Daten exportierende Unternehmen nachweisen lassen, wie das importierende Unternehmen seinen Informationspflichten nach Safe Harbor gegenüber den von der Datenverarbeitung Betroffenen nachkommt. Dies ist auch nicht zuletzt deshalb wichtig, damit das importierende Unternehmen diese Information an die von der Übermittlung Betroffenen weitergeben kann.
Diese Mindestprüfung müssen die exportierenden Unternehmen dokumentieren und auf Nachfrage der Aufsichtsbehörden nachweisen können. Sollten nach der Prüfung Zweifel an der Einhaltung der Safe Harbor-Kriterien durch das US-Unternehmen bestehen, empfehlen die Aufsichtsbehörden, der Verwendung von Standardvertragsklauseln oder bindenden Unternehmensrichtlinien zur Gewährleistung eines angemessenen Datenschutzniveaus beim Datenimporteur den Vorzug zu geben. […]"

## 2.2 Bundesrecht

Auf der Bundesebene wurde in den beiden zurückliegenden Jahren zwar viel über den Datenschutz geredet, aber kaum etwas entschieden. Die Bundesregierung veranstaltete sog. Datenschutzgipfel, verkündete sog. Datenschutzthesen und kündigte auch neue Datenschutzgesetze an. Geschehen ist aber nichts, jedenfalls in den Bereichen, in denen die datenschutzrechtlichen Defizite immer größer werden: im privatwirtschaftlichen Bereich, insbesondere im Internet.

Die Vorstellungen des ehemaligen Bundesinnenministers de Maizière, man könne Datenschutzregeln, die für analoge Technologien entwickelt worden sind, in entsprechender Weise auf die digitale Entwicklung in Staat und Gesellschaft anwenden, ist abwegig. Das zeigt die Praxis, und das bestätigen auch die Entscheidungen der Gerichte, die sich immer öfter nur noch mit verfassungskonformer Auslegung der alten, aus der Vorinternetzeit stammenden Regelungen zu helfen wissen. Diese Entscheidungen sind Ausdruck einer wachsenden Rechtsunsicherheit, die ausschließlich zu Lasten der Nutzerinnen und Nutzer bzw. Verbraucherinnen und

Verbraucher geht. Denn vorhandene Regelungslücken und normative Defizite werden von der Wirtschaft im Allgemeinen und von der Internetwirtschaft im Besonderen stets zu Gunsten der eigenen Interessen genutzt. Die Interessen und Rechte der Verbraucherinnen und Verbraucher bleiben dabei oft auf der Strecke. Insoweit verfehlt der Staat seine aus den Grundrechten folgende Aufgabe, sich schützend vor die Bürgerinnen und Bürger zu stellen, die durch die digitale Entwicklung ohnehin zunehmend überfordert werden.

Überfällig ist deshalb v.a. die Modernisierung des **Bundesdatenschutzgesetzes**. Sie ist unterblieben, obwohl sie von den Koalitionspartnern auf Bundesebene verabredet worden war und obwohl die Datenschutzbeauftragten des Bundes und der Länder in einem **Eckpunktepapier** die notwendigen Änderungen im Einzelnen beschrieben haben.

- Die Datenverarbeitung muss transparenter werden. Die Betroffenen müssen in der Lage sein, ihre Rechte auf Auskunft, Berichtigung oder Löschung auf einfache Weise und auf elektronischem Wege wahrnehmen zu können. Entwicklerinnen und Entwickler sowie Verwenderinnen und Verwender informationstechnischer Systeme sollten gesetzlich verpflichtet sein, datenschutzfreundliche Technik bereitzustellen und einzusetzen („Privacy by Design“). Den Betroffenen, die zunehmend selbst aktive Teilnehmerinnen und Teilnehmer an IT-Verfahren sind und dabei persönliche Daten von sich und von Dritten verwenden, sollten IT-Produkte und Dienste mit den jeweils datenschutzfreundlichsten Einstellungen zur Verfügung gestellt werden („Privacy by Default“).
- Das Datenschutzrecht muss internetfähig werden. Dabei kommt der grundsätzlich unbeobachteten Nutzung elektronischer Dienste besondere Bedeutung zu. Es sind die Voraussetzungen zu schaffen, dass die Betroffenen auch im Netz ihre Rechte adäquat wahrnehmen können. Ebenso wie das Internet global ist, müssen auch datenschutzrechtliche Mindeststandards global gelten und durchgesetzt werden können. Gesetzliche Regelungen für ein hohes und verbindliches Datenschutzniveau sind weiterhin wichtig. Zusätzlich müssen aber auch die Anreize gestärkt werden, dass die verantwortlichen Stellen Datenschutz als im eigenen Interesse liegendes Anliegen begreifen. Dies kann z.B. durch ein Datenschutzaudit geschehen, also die Zertifizierung der Datenschutzeigenschaften von Produkten und Diensten auf Basis unabhängiger Begutachtung. Ein solches Datenschutzaudit könnte die Erfolgsaussichten datenschutzfreundlicher Angebote im Wettbewerb verbessern.
- Für die Gewährleistung des technischen und organisatorischen Datenschutzes und der Datensicherheit sollten statt konkreter, auf eine bestimmte technische Umgebung fixierter Maßnahmen allgemeinverbindliche Schutzziele gesetzlich festgeschrieben werden. Damit würde ein technikneutraler und flexibler Ansatz geschaffen, der den grundrechtlichen Vorgaben des Rechts auf informationelle Selbstbestimmung und des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme auch bei sich verändernden technologischen oder organisatorischen Rahmenbedingungen Rechnung trägt.
- Die bei Verstößen gegen das Datenschutzrecht vorgesehenen Sanktionen haben sich zum Teil als nicht ausreichend erwiesen. Deshalb muss die Durchsetzung von Schadensersatzansprüchen sowie die Verfolgung von Ordnungswidrigkeiten erleichtert werden.
- Schließlich muss das Datenschutzrecht insgesamt leichter lesbar und damit einfacher anwendbar werden. Durch die seit 1990 vorgenommenen zahlreichen Gesetzesänderungen haben einige Vorschriften des Bundesdatenschutzgesetzes einen solchen Umfang angenommen, dass sie von den Rechtsanwenderinnen und -anwendern – auch von solchen mit juristischer Vorbildung – bisweilen kaum noch verstanden werden. Es sind zudem teilweise unklare Normen entstanden, die zu Unsicherheiten und vermeidbarem Streit über die Auslegung führen.

Wie gesagt: Diese Eckpunkte wurden von Bundesregierung bisher nicht aufgegriffen.

Der Bund war auch nicht in der Lage, ein sog. **Datenschutzauditgesetz** zu verabschieden, das in § 9a BDSG ausdrücklich für notwendig gehalten wird. Eine entsprechende Gesetzesnovellierung war zwar 2008 eingebracht, dann aber 2009 nicht weiter verfolgt worden. Keinen wesentlichen Fortschritt brachte auch die Novellierung der Datenschutzregelungen zum **Adressdatenhandel** (vgl. 22. Tb., Tz. 2.2.2) Gesetzesvorschläge, die als Reaktion auf diverse Datenskandale das informationelle Selbstbestimmungsrecht gestärkt hätten, waren auf Druck der allgegenwärtigen Lobbyvertreterinnen und -vertreter wieder zurückgenommen bzw. entschärft worden.

Auch die vom Bundesrat einstimmig beschlossenen **Gesetzentwürfe zur Regelung digitaler Panoramadienste und sonstiger Online-Angebote** (vgl. Tz. I-1.1) wurden von der Bundesregierung abgelehnt. Die Begründungen überzeugen nicht. Mit Blick auf Google Street View und vergleichbare Dienste hieß es, dass Einzelfallgesetze nicht weiterhelfen würden. Hinsichtlich

der vorgeschlagenen Regelung für soziale Netzwerke wurde auf das europäische Recht und auf die Notwendigkeit von Selbstverpflichtungen der Anbieter verwiesen. Wären noch andere Gesetzentwürfe im Bundesrat verabschiedet worden, wären diese sicherlich auch auf den Widerstand der Bundesregierung getroffen.

Dass sie offenbar nicht gewillt ist, dem Datenschutz auch im Internet zum Zuge zu verhelfen, zeigt auch das Schicksal des vom früheren Bundesinnenminister de Maizière Ende 2010 vorgelegten Entwurfs für ein sog. **Rote-Linien-Gesetz**, mit dem eine von Online-Anbieterinnen und -Anbietern nicht überschreitbare Grenze für Internetveröffentlichungen markiert werden sollte. Dazu sollte z.B. das Verbot der Erstellung von Persönlichkeitsprofilen durch die Auswertung der Aktivitäten von Netznutzerinnen und -nutzern gehören, aber auch das Verbot des Einsatzes von Bilderkennungssoftware zur Identifizierung Einzelner im Netz. Der Entwurf ist allerdings in der Versenkung verschwunden, offenbar soll das Projekt nicht weiter verfolgt werden.

Auch beim **Beschäftigtendatenschutzgesetz** (vgl. Tz. I-3.1) ist der Bund nicht weitergekommen. Zwar liegt insoweit ein Gesetzentwurf vor, der vom Bundestag auch schon in erster Lesung beraten und an die Ausschüsse überwiesen worden ist. Nach einer Anhörung blockieren sich dort aber die Koalitionsfraktionen offenbar gegenseitig. Es steht zu befürchten, dass auch dieses Datenschutzprojekt scheitern wird, obwohl nicht zuletzt die Präsidentin des Bundesarbeitsgerichts mit Nachdruck ein Arbeitnehmerdatenschutzgesetz gefordert hat.

Offenbar hat die Bundesregierung stattdessen auf eine andere Karte gesetzt: Die Errichtung einer **Stiftung Datenschutz**, die sich verstärkt um die digitale Bildung der Bevölkerung und um die vergleichende Prüfung von Online-Angeboten und Online-Dienstleistungen kümmern soll. Abgesehen davon, dass die Bundesregierung aber offenbar auch mit diesem Vorhaben nicht weiterkommt – trotz wiederholter Ankündigungen ist die Stiftung auch 2011 nicht realisiert worden –, ist eine solche Stiftung datenschutzrechtlich und datenschutzpolitisch fragwürdig. Mit ihr würden den unabhängigen Landesdatenschutzbeauftragten Aufgaben entzogen und auf eine der Bundesaufsicht unterstehende und von der Wirtschaft finanziell abhängige Stiftung des Bundes übertragen. Ein solches Unterfangen ist bereits verfassungsrechtlich zweifelhaft. Wenn man für digitale Produkte oder digitale Dienstleistungen Vergleichstests organisieren und veröffentlichen will, kann dies auch von der Stiftung Warentest übernommen werden. Und wenn man dafür doch unbedingt eine neue Stiftung gründen will, genügt eine Stiftung „Datentest“. Für den Datenschutz im Übrigen aber sind die Datenschutzbeauftragten berufen.

Von Bedeutung ist immerhin das sog. **De-Mail-Gesetz**, das vom Bundestag im Mai 2011 mit dem Ziel verabschiedet worden ist, eine Infrastruktur für eine rechtssichere elektronische Kommunikation aufzubauen, die den Beteiligten Sicherheit gibt über die Identität der Kommunikationspartnerinnen und -partner und die Authentizität und Integrität der übermittelten Nachrichten. Dazu gehört neben einem Postfach- und Versanddienst auch eine geschützte Dokumentenablage. Die Übertragung von Nachrichten erfolgt generell verschlüsselt. Nachrichten werden unterwegs auf Schadsoftware geprüft, und es werden Versandbestätigungen sowie – bei Bedarf – Empfangsbestätigungen verschickt. Behörden können sich zum Nachweis der Zustellung Abholbestätigungen ausstellen lassen. Nachbesserungsbedarf besteht aber bei den noch nicht zureichenden Vorkehrungen zur Datensicherheit (vgl. 23. Tb. des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Tz. 3.3). Grundsätzlich befürwortet der LfD das Ziel einer sicheren und verlässlichen elektronischen Kommunikation. Im Zeitalter des elektronischen Versands von Rechnungen, Kontoauszügen oder Zugangsdaten für Internetportale wird es zwingend erforderlich, zusätzliche Sicherheitsmaßnahmen für die elektronische Kommunikation bereitzustellen. Entscheidend wird es jedoch sein, welche Akzeptanz De-Mail bei den Bürgerinnen und Bürgern finden wird. Und diese hängt nicht zuletzt von der Sicherheit, dem Datenschutz und der Transparenz des Verfahrens ab.

So bestehen die „großen“ datenschutzrechtlichen Leistungen des Bundes letztlich darin, dass bestimmte Regelungen gestoppt bzw. dem Bundestag erst gar nicht vorgelegt wurden. Gemeint ist das **ELENA-Verfahrensgesetz**, das zu einem gigantischen Datenmoloch geführt hätte, wenn es nicht vom Bundestag wieder aufgehoben worden wäre. Gemeint ist aber auch die **Vorratsdatenspeicherung** (vgl. Tz. II-8.2.4), auf die sich die Koalitionsregierung bisher nicht verständigen konnte. Aus Datenschutzsicht ist dies zu begrüßen. Bedauerlich ist nur, dass eine so fundamentale Frage zum Koalitionsgezänk verkommt. Denn bei der Vorratsdatenspeicherung geht es um die Frage, wie viel Sicherheitsstaat eine freiheitliche Gesellschaft verträgt. Es geht um die Grenzen, die auch bei der Bekämpfung des Terrorismus und der organisierten Kriminalität nicht überschritten werden sollten. Die Erfahrung lehrt uns, dass es bei einer Vorratsdatenspeicherung, die – völlig unabhängig vom Vorliegen einer Gefahr – feststellen soll, wer wann mit wem und wie lange telefoniert hat und wo er sich dabei aufgehalten hat, nicht bleiben wird. Der nächste Schritt wird darin bestehen,

auch festzuhalten, wer was im Internet gelesen, gesucht und geschrieben hat. Die digitale Technologie würde dies und noch mehr ermöglichen. Nur wäre ein Staat, der von solchen Möglichkeiten Gebrauch machen würde, kein freiheitlicher Staat mehr. Der freiheitliche Staat muss sich auf die Suche nach Alternativen und nach Kompromissen begeben. Die Datenschutzbeauftragten haben dafür Vorschläge unterbreitet. Der Bundesdatenschutzbeauftragte hat sich jüngst noch einmal für ein sog. „Quick Freeze Plus"–Verfahren ausgesprochen, demzufolge Internetverbindungsdaten für ein oder zwei Wochen gepuffert werden, so dass die Strafverfolgungsbehörden die Möglichkeit hätten, diese Daten einzufrieren und zur Verfolgung schwerer Straftaten auch zu verwenden. In jedem Falle ist dies eine Frage, mit der sich das Parlament befassen muss. Denn die Diskussion um die datenschutzrechtlichen Grenzen eines Sicherheits- bzw. Präventivstaates ist so wesentlich, dass sie in dem Forum geführt werden muss, das von der Verfassung dafür vorgesehen ist: im Parlament. Koalitionsausschüsse reichen dafür nicht aus.

Sie reichen v.a. auch deshalb nicht aus, weil das Parlament sich in den digitalen Fragen unserer Zeit ohnehin in der Defensive befindet. Die Communty will ein freies Internet und wehrt sich nach Kräften gegen gesetzliche Regelungen. Die Wirtschaft will aus anderen Gründen ebenfalls ein freies Internet und setzt sich nicht minder gegen parlamentarische Regeln zur Wehr. Die Bundesregierung verweist auf den globalen Charakter des Internets und spricht sich ebenfalls gegen nationale Gesetze und für europäische Regelungen aus. All das schwächt das Parlament.

Deshalb ist es sinnvoll, dass der Bundestag eine Enquete-Kommission eingesetzt hat, die sich mit allen Fragen des Internets befasst. Angesichts der dargestellten Probleme sollte sich diese Enquete-Kommission aber auch mit dem Vorschlag des Doyens des deutschen Datenschutzes, Professor Simitis befassen, digitale Entwicklungen, die zu Lasten der Persönlichkeitsrechte der Bürgerinnen und Bürger gehen, zumindest in zeitlich befristeten Gesetzen zu regeln. Solche Zeitgesetze würden das Parlament stärker als bisher in die digitale Entwicklung von Staat und Gesellschaft einbeziehen, parlamentarische Selbstblockaden aufheben und dafür sorgen, dass staatliche Regulierungen in der Regel auf der Höhe der technischen Entwicklung wären.

Im Vergleich dazu bringt die von der Bundesregierung immer wieder ins Gespräch gebrachte Selbstregulierung durch die Wirtschaft nur Nachteile. Entweder es beteiligen sich nicht alle relevanten Unternehmen an solchen Selbstverpflichtungen oder diese werden nicht beachtet. Und selbst wenn sie beachtet würden, wären sie nicht ausreichend, da sie in der Regel Vereinbarungen zu Lasten der Verbraucherinnen und Verbraucher darstellen. Dies hat man mittlerweile sogar in den USA erkannt, wo man in der Vergangenheit den Datenschutz überwiegend dem Markt überlassen hat. Mittlerweile spricht man aber auch im Kongress davon, dass es im Internet einen „Krieg um die Privatsphäre der Bürger" gäbe, dass man deshalb eine Art „Bill of Rights" für den Datenschutz benötige und dass Selbstverpflichtungen der Wirtschaft allenfalls ergänzend zum Zuge kommen könnten. Parlamentarische Leitentscheidungen können sie nicht ersetzen.

Der Berliner Historiker Michael Stürmer hat in einem Leitartikel in der „Welt" jüngst von den „entfesselten Kräften des Internets" gesprochen (vgl. „Welt" vom 29. Juli 2011) und daraus die Sorge abgeleitet, wir erlebten gegenwärtig womöglich den Anfang vom Ende unserer Demokratie. In einer solchen Zeit darf das nationale Parlament nicht nur zusehen. Es muss auch entscheiden.

## 2.3 Landesrecht

### 2.3.1 Novellierung des Landesdatenschutzgesetzes

Das Urteil des Europäischen Gerichtshofs vom 9. März 2010 (Az. C-92/09; vgl. Tz. I-2.1.2), mit dem es die völlige Unabhängigkeit der Datenschutzbeauftragten anmahnte, führte zu einer Novellierung des Landesdatenschutzgesetzes. Um die völlige Unabhängigkeit des LfD als Datenschutzaufsichtsbehörde zu sichern, wurde die bisher bestehende Rechtsaufsicht des Kabinetts gestrichen und die Dienstaufsicht des Landtagspräsidenten modifiziert. Die Novellierung des Landesdatenschutzgesetzes verfolgte aber noch weitere Ziele. V.a. sollten Regelungen aus der Novellierung des Bundesdatenschutzgesetzes vom 1. September 2009 in das Landesdatenschutzgesetz übernommen werden. Die Vorschriften des Landesdatenschutzgesetzes zur Auftragsdatenverarbeitung sowie zur Stellung der behördlichen Datenschutzbeauftragten und zur Informationspflicht öffentlicher Stellen bei Datenpannen wurden deshalb nach dem Vorbild der Novelle II des Bundesdatenschutzgesetzes modifiziert. Gleichzeitig wurden die Aufgaben des LfD präziser gefasst und seine Berichtspflicht gegenüber dem Landtag dem Jahreszyklus angepasst. Bei dieser Gelegenheit wurde auch die Vorschrift zur Videoüberwachung öffentlich zugänglicher Räume differenzierter gefasst (vgl. Tz. II-7.1.3).

Zudem wurden die Aufgaben des LfD in zwei Punkten konkretisiert: Es wurde klargestellt, dass seine Aufgabe, mit anderen Stellen, die den Datenschutz als Aufgabe haben, Verbindung zu halten und auf eine einheitliche

Datenschutzpraxis hinzuwirken, sich auch auf die behördlichen und betrieblichen Datenschutzbeauftragten bezieht (§ 24 Abs. 7 Satz 2 LDSG; vgl. Tz. I-3.8). Außerdem wurden die Bürgerinnen und Bürger in die Beratungspflicht des LfD einbezogen. In § 24 Abs. 8 des LDSG heißt es jetzt:

„Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit berät und informiert die Bürgerinnen und Bürger in Fragen des Datenschutzes und der Datensicherheit, insbesondere über die ihnen bei der Bearbeitung ihrer Daten zustehenden Rechte und über geeignete Maßnahmen des Selbstdatenschutzes."

### 2.3.2 Datenschutz in sonstigen Landesgesetzen

Die Entwicklung des Datenschutzes zur Querschnittsmaterie, die nahezu alle übrigen Regelungsgebiete durchdringt, setzte sich auch im Berichtszeitraum fort. Von den 71 seit Oktober 2009 verabschiedeten Landesgesetzen weisen 13 datenschutzrechtliche Bezüge von eigenem Gewicht auf, besonders hervorzuheben sind hier etwa das Archivgesetz, das Gesetz zur Ausführung des Zensusgesetzes (vgl. Tz. II-7.2.2) und die Rundfunkänderungsstaatsverträge (vgl. Tz. II-1.1), aber auch das Landesbeamtengesetz (vgl. Tz. II-3.2.2) und das Geodateninfrastrukturgesetz.

Durch die höhere Aufmerksamkeit, die der Datenschutz in den gesellschaftlichen Debatten der vergangenen Jahre hinzugewonnen hat, werden auch die datenschutzrechtlichen Bezüge vieler Regelungsmaterien „entdeckt", die bislang nicht jedem bewusst waren. Der LfD unterstützt das Parlament, die Landesregierung und die Kommunen auch bei der Fortentwicklung dieses Rechtsbestandes durch umfangreiche Beratungstätigkeit und durch das Einbringen eigener Regelungsvorschläge.

# 3. Schwerpunkte des Datenschutzes

## 3.1 Das Beschäftigtendatenschutzgesetz

Wie im vorangegangen Kapitel erläutert wurde, besteht ein Arbeitsschwerpunkt des LfD darin, den Erlass von datenschutzfreundlichen Regelungen zu fördern. Das war v.a. bei der Novellierung des Landesdatenschutzgesetzes (vgl. Tz. I-2.3.1) und des Polizei- und Ordnungsbehördengesetzes (vgl. Tz. II-4.1) der Fall. Vergleichbare Bemühungen gab es aber auch mit Blick auf das vom Bundestag und der Bundesregierung angekündigte Beschäftigtendatenschutzgesetz, zu dessen Vorstufen bereits im letzten Tätigkeitsbericht Stellung genommen worden war (vgl. 22. Tb., Tz. 2.2.4). Auch im jetzigen Berichtszeitraum hat sich der LfD intensiv mit dieser Materie befasst. Dazu gehörten Stellungnahmen gegenüber der Landesregierung, Veranstaltungen mit der Zukunftsinitiative Rheinland-Pfalz, mit den Geschäftsführern der Landesvereinigung Unternehmensverbände Rheinland-Pfalz sowie mit Gewerkschaften und Parteien. Für eine Veranstaltung der Bitbuger Gespräche zum Beschäftigtendatenschutz stand der LfD beratend zur Verfügung. Ergänzt wurden diese Aktivitäten durch diverse Publikationen und öffentliche Stellungnahmen.

Weshalb hat sich der LfD so intensiv mit einer Materie befasst, für die nicht das Land, sondern der Bund zuständig ist? Zum einen, weil die Notwendigkeit eines solchen Gesetzes bei allen Fachleuten anerkannt und das Gesetz überfällig ist. Zum anderen, weil der Versuch unternommen werden muss, die scheinbar unversöhnlichen Positionen der betroffenen Seiten zusammenzuführen. Dabei gilt es auch, einem Missverständnis entgegenzuwirken. Bei dem Entwurf geht es zwar um den „Beschäftigtendatenschutz“, er setzt aber gleichsam voraus, dass die Arbeitgeberseite das Recht hat zu prüfen und sicherzustellen, dass die Arbeitnehmerinnen und Arbeitnehmer ihre vertraglichen Verpflichtungen erfüllen. Es geht deshalb nicht nur um den Schutz von Arbeitnehmerdaten, sondern auch um die Sicherstellung von Kontroll- und Überwachungsmaßnahmen. Beides muss zu einem Ausgleich gebracht werden. Ein Kompromiss ist deshalb zwingend notwendig, so wie die Dinge liegen aber wohl nur schwer erreichbar.

Gegenstand der Diskussion und Beratung ist im Wesentlichen der vom Bundesministerium des Innern im März 2010 vorgelegte Entwurf, der allerdings das angestrebte Ziel eines zeitgemäßen und verbesserten Schutzes der Beschäftigten vor Überwachung und übermäßiger Kontrolle in wesentlichen Punkten verfehlte. Zudem blieb eine ganze Reihe von Fragen und Problemen ungeklärt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder forderte deshalb in einer Entschließung vom 22. Juni 2010 („Beschäftigtendatenschutz stärken statt abbauen“) eine Nachbesserung und zwar insbesondere in den folgenden Punkten:

- Die im Gesetzentwurf vorgesehene Erlaubnis zur Datenverarbeitung bei Verhaltens- und Leistungskontrollen war zu weit gefasst und lädt zur Ausweitung der Kontrolle und Überwachung der Beschäftigten geradezu ein.
- Auch die im Entwurf vorgesehene allgemeine Erlaubnis zur Verarbeitung und Nutzung von Beschäftigtendaten zur „Verhinderung und Aufdeckung von Vertragsverletzungen zu Lasten des Arbeitgebers, Ordnungswidrigkeiten und Straftaten“ hätte den Arbeitgeberinnen und Arbeitgebern sehr weitgehende zusätzliche Befugnisse zur Auswertung und Verknüpfung unterschiedlichster Datensammlungen in die Hand gegeben. Der Gesetzgeber sollte vielmehr klarstellen, dass Maßnahmen, die zu einer ständigen Kontrolle der Beschäftigten führen oder den Betroffenen den Eindruck einer umfassenden Überwachung am Arbeitsplatz vermitteln – etwa durch ständige Videoüberwachung oder regelmäßige Aufzeichnung, Mitschnitte oder Mithören von Ferngesprächen –, weiterhin zu unterbleiben haben.
- Die Intention des Gesetzentwurfs, den Umfang der in Bewerbungsverfahren und während des Beschäftigungsverhältnisses verwendeten Daten zu begrenzen, würde auch verfehlt, wenn – wie im Entwurf vorgesehen – Arbeitgeberinnen und Arbeitgeber im Internet verfügbare Informationen generell nutzen dürfen, und zwar sogar dann, wenn diese durch Dritte ohne Kenntnis der Betroffenen und somit häufig rechtswidrig eingestellt wurden. Damit würde vom datenschutzrechtlichen Grundsatz der Direkterhebung bei den Betroffenen abgewichen und Arbeitgeberinnen und Arbeitgeber würden geradezu dazu eingeladen, im Internet und in sozialen Netzwerken systematisch nach dort vorhandenen Informationen über Bewerberinnen und Bewerber und Beschäftigte zu recherchieren.
- Der Schutz der Beschäftigten vor unangemessener Kontrolle und Überwachung ist gerade bei der zunehmenden Nutzung elektronischer Medien am Arbeitsplatz von besonderer Bedeutung. Es ist eine normenklare, strikte Begrenzung der Einsichtnahme der Arbeitgeberinnen und Arbeitgeber in die elektronische Kommunikation von Beschäftigten unter Berücksichtigung von deren schützenswerten Belangen erforderlich.
- Die im Gesetzentwurf an mehreren Stellen vorgesehene „Einwilligung“ der Beschäftigten würde zu einer erheblichen Erweiterung der (Kontroll-)Befugnisse der Arbeitgeberinnen und Arbeitgeber führen. Diese wären

jedoch rechtlich höchst zweifelhaft, weil Einwilligungen im Arbeitsverhältnis in den meisten Fällen mangels Freiwilligkeit nicht rechtswirksam erteilt werden können. Hinzu kommt, dass im Gesetzentwurf an keiner Stelle definiert wurde, welche Anforderungen an die Rechtswirksamkeit von Einwilligungen im Arbeitsverhältnis zu stellen sind.

Im Ergebnis – so die Konferenz der Datenschutzbeauftragten des Bundes und der Länder – würden die im Referentenentwurf vorgesehenen Änderungen in zentralen Bereichen des Arbeitslebens eine Verschlechterung des Datenschutzes für die Beschäftigten zur Folge haben. Die Konferenz appellierte daher an den Bundesgesetzgeber, den vorgelegten Gesetzentwurf grundlegend zu überarbeiten, jedenfalls aber deutlich zu Gunsten des Persönlichkeitsrechts der Beschäftigten zu ändern.

Dieser Appell blieb nicht ungehört, der Gesetzentwurf der Bundesregierung vom Dezember 2010 (BT-Drs. 17/4230) wies gegenüber dem Referentenentwurf deutliche Verbesserungen auf. In der öffentlichen Diskussion besonders wahrgenommen wurde etwa das grundsätzliche Verbot der heimlichen Videoüberwachung von Arbeitnehmerinnen und Arbeitnehmern. Dennoch blieben auch im Gesetzentwurf erhebliche Schwachstellen.

In ihrer Entschließung vom 17. März 2011 bekräftigte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder („Beschäftigtendatenschutz stärken statt abbauen“) daher die Notwendigkeit, durch umfassende allgemeingültige Regelungen für den Datenschutz am Arbeitsplatz mehr Rechtssicherheit zu erreichen und bestehende Schutzlücken zu schließen. Dieser Ansatz erfordere klare gesetzliche Begrenzungen der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten. Deshalb appellierte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an den Deutschen Bundestag, bei den Beratungen über Regelungen des Beschäftigtendatenschutzes insbesondere folgende Anforderungen sicherzustellen:

- Im Bewerbungsverfahren und im Beschäftigungsverhältnis müsse die Erforderlichkeit von Eignungstests und medizinischen Untersuchungen vor der Durchführung der jeweiligen Maßnahme dokumentiert werden, Eignungstests müssten ausschließlich auf wissenschaftlichen Methoden beruhen.
- Zur Aufdeckung von Straftaten und ähnlich schwerwiegenden Pflichtverletzungen dürften Beschäftigtendaten nur oberhalb normenklarer und verhältnismäßiger Einschreitschwellen erhoben und verwendet werden. Arbeitgeberinnen und Arbeitgeber dürften dabei – insbesondere verdeckte – Überwachungsmaßnahmen nur ergreifen, wenn insoweit zu dokumentierende Tatsachen vorliegen. Mit Blick auf rechtsstaatliche Anforderungen müsse die Grenze zwischen eigenverantwortlichen Recherchen der Arbeitgeberinnen und Arbeitgeber und der den Strafverfolgungsbehörden vorbehaltenen Aufgaben eindeutig bestimmt werden. Aus präventiven Gründen sei eine verdeckte Datenerhebung generell unzulässig.
- Insbesondere bezüglich der Durchführung von Screening-Verfahren seien klare materielle Kriterien – z.B. Prüfung der Verhältnismäßigkeit, Vorliegen von tatsächlichen Hinweisen auf Unregelmäßigkeiten – erforderlich. Zudem sollten Arbeitgeberinnen und Arbeitgeber verpflichtet sein, die näheren Umstände, die den Abgleich veranlassen, vorab zu dokumentieren.
- Die an verschiedenen Stellen im Gesetzentwurf der Bundesregierung vorgesehenen Regelungen zur Verhaltens- und Leistungskontrolle seien nach wie vor zu weitgehend. Der Gesetzgeber müsse hier strenge Voraussetzungen vorgeben. Die Konferenz verwies insoweit auf die gefestigte verfassungsrechtliche Rechtsprechung zum unzumutbaren Überwachungsdruck.
- Weiter forderte die Konferenz der Datenschutzbeauftragten, die offene Videoüberwachung stärker zu begrenzen und insbesondere zu verbieten, die z.B. bei der Qualitätskontrolle anfallenden Daten zur Verhaltens- und Leistungskontrolle zu nutzen und sie für Bereiche zu untersagen, die nicht nur „überwiegend“, sondern „auch“ der privaten Nutzung dienen.
- Schließlich dürfe das Petitionsrecht nicht beschränkt werden. Beschäftigte müssten sich jederzeit an die zuständige Datenschutzaufsichtsbehörde wenden können, ohne deswegen benachteiligt oder gemaßregelt zu werden.
- Gesetzliche Regelungen zum Beschäftigtendatenschutz wurden darüber hinaus angemahnt zur Personalaktenführung, zur privaten Nutzung von Telekommunikationsdiensten, zum Thema Whistleblowing, zum Beweisverwertungsverbot bei unzulässiger Datenerhebung und -verwendung sowie zum Konzerndatenschutz unter Berücksichtigung des internationalen Datenverkehrs.

Mittlerweile ist das Gesetzgebungsverfahren, nachdem vor der parlamentarischen Sommerpause noch eine umfangreiche Sachverständigenanhörung im Innenausschuss durchgeführt worden war, praktisch zum Stillstand gekommen. Mit Sorge beobachten die Datenschutzbeauftragten, dass ein Gesetzentwurf, dessen Notwendigkeit unbestreitbar ist, erneut zu scheitern droht. Dies wäre für alle Beteiligten ein schwerer Rückschlag, da der Bundesgesetzgeber in der Pflicht steht, seiner verfassungsrechtlichen Schutzfunktion gerade gegenüber Arbeitnehmerinnen und Arbeitnehmern nachzukommen.

## 3.2 Facebook

### 3.2.1 Grundsatzfragen

Beim Stichwort „soziale Netzwerke“ denken heute alle zunächst an Facebook. Innerhalb einer relativ kurzen Zeit hat sich dieses Netzwerk auch in Deutschland deutlich an die Spitze gesetzt; ca. 20 Millionen Nutzerinnen und Nutzer der derzeit weltweit 800 Millionen Mitglieder sind in Deutschland aktiv. Bei vielen Beobachterinnen und Beobachtern führt dies zu Bedenken. Sie richten sich zum einen gegen ein zu leichtsinniges und zu offenherziges Kommunikationsverhalten der Nutzerinnen und Nutzer und zum anderen gegen die maßlose Speicher- und die intransparente Verwertungspraxis des Netzwerks. Die Bereitstellung einer Kommunikations- und Distributionsplattform für interessierte Menschen ist deshalb nur die eine Seite von Facebook. Seine gigantischen Datenspeicher die andere. Nicht der Staat erscheint deshalb als Big Brother, sondern das Internetunternehmen, das weltweit über alle Staatsgrenzen hinweg agiert und das für sich einen Börsenwert reklamiert, der den Staatshaushalt vieler kleinerer Staaten übertrifft (nämlich 100 Milliarden Dollar).

Facebook ist aus mehreren Gründen ein Thema, mit dem sich der rheinland-pfälzische Datenschutzbeauftragte befassen muss. Rechtlich zwingend ist dies, weil und soweit er die Aktivitäten der rheinland-pfälzischen Unternehmen und öffentlichen Stellen zu beurteilen hat, die Facebook nutzen. Wenn diese Stellen Fanpages betreiben bzw. z.B. Social Plugins wie den Like Button für ihre eigenen Zwecke einsetzen, muss er Aussagen über die Frage der Datenschutzkonformität solcher Aktivitäten treffen können. Dies ist Teil seiner ihm gesetzlich vorgegebenen Kontroll- und Beratungsaufgaben.

Hinzu kommt, dass er die gesetzliche Aufgabe hat, die Bürgerinnen und Bürger über Gefahren der Datenverarbeitung (auch und gerade im Internet bzw. im Web 2.0) aufzuklären und ihnen dazu auch Empfehlungen zu geben.

Dies ist ganz unabhängig von einem dritten Aspekt, der allerdings rechtlich umstritten ist: die Frage, wer für die Datenschutzkontrolle von Internetangeboten (Telemedien) eines Anbieters aus dem Ausland zuständig ist. Bei einem im Ausland ansässigen Unternehmen ist die Datenschutzaufsichtsbehörde dieses Sitzlandes (bei Facebook Europe also Irland) unzweifelhaft zuständig. Daneben aber dürften auch die Datenschutzaufsichtsbehörden zuständig sein, in deren Gebiet ein solches Unternehmen eine Niederlassung betreibt (für Deutschland im Fall von Facebook also der Hamburgische Datenschutzbeauftragte). Schließlich könnten auch alle Datenschutzaufsichtsbehörden, in deren Gebiet ein solches Unternehmen Daten erhebt, eine Aufsichtszuständigkeit beanspruchen.

Der Datenschutz dieses Datengiganten ist aber unzureichend. Die amerikanische Aufsichtsbehörde (Federal Trade Commission – FTC –) hat festgestellt, dass Facebook seine Nutzerinnen und Nutzer wiederholt getäuscht und sich nicht an seine eigenen Vorgaben für den Schutz der Privatsphäre seiner Nutzerinnen und Nutzer gehalten hat (http://www.ftc.gov/opa/2011/11/privacysettlement.shtm vom 29. November 2011). Die Prüfungen des Hamburgischen Datenschutzbeauftragten sowie des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, aber auch die Anzeigen eines österreichischen Studenten (vgl. Tz. I-3.9.2) haben diese und weitere Bedenken bestätigt. Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein hat die mangelnde Transparenz bei der Erhebung und Verarbeitung von Nutzerdaten im Zusammenhang mit dem Like Button und von Fanpages beklagt (vgl. Tz. I-3.2.3, Tz. I-3.2.2 und http://www.datenschutzzentrum.de/Facebook/). Der Hamburgische Datenschutzbeauftragte hat die zentrale Sammlung der Gesichtserkennungsdaten von Facebook-Nutzerinnen und -Nutzern ohne deren Einwilligung angeprangert (vgl. Tz. I-3.2.3). Außerdem hat er festgestellt, dass Facebook Cookies einsetzt, deren Funktionsweise und Ziele trotz der Einlassungen von Facebook zweifelhaft bleiben und deren Rechtmäßigkeit dabei in Frage steht (http://www.datenschutz-hamburg.de/). Der erwähnte Student hat besonders die mangelhafte Auskunftspraxis und die unzureichenden Maßnahmen bei der Datenlöschung hervorgehoben (vgl. http://www.europe-v-Facebook.org/DE/de.html). Hinzu kommt die Gefahr von Sicherheitslücken (vgl. Tz. I-3.2.4). Inzwischen hat auch die irische Datenschutzbehörde ihre Prüfung abgeschlossen und erhebliche Mängel festgestellt.

Vor diesem Hintergrund werden in der Öffentlichkeit Forderungen laut, Facebook zu meiden und eine eventuell bestehende Mitgliedschaft zu kündigen. In diesem Kontext ist der Austritt der Bundesverbraucherschutzministerien aus Facebook zu sehen und auch die Aufforderung in einer großen deutschen Wochenzeitschrift, Facebook massenhaft den Rücken zuzukehren. Der LfD, der selbst nicht Mitglied bei Facebook ist, hat Verständnis für diese Appelle. Im Prinzip teilt er sie auch. Wer für einen vernünftigen Datenschutz ist und sichergehen will, dass die Betreiber dieser gigantischen Netzwerke ihre Datenspeicher nicht zum Schaden unserer demokratischen Ordnung nutzen, hat eigentlich keine andere Möglichkeit, als sich aus diesen Netzwerken zu verabschieden. Es gibt andere Netzwerke, die den Datenschutz eher respektieren als Facebook, und es gibt alternative Netzwerke, die ohne

zentrale Datenspeicherung auskommen. Diese sollten vom Staat gefördert werden. Dies wäre besser und näher an den Prinzipien des Grundgesetzes und der Landesverfassung als das Betreiben einer eigenen Fanpage bei Facebook. Der LfD hat sich mit entsprechenden Boykottaufrufen allerdings bisher zurückgehalten. Zu gewaltig ist der Mitgliederzuwachs bei Facebook, zu groß die Sogwirkung, die sich daraus für jeden ergibt, der noch nicht Mitglied ist. Es erscheint deshalb realitätsfremd vom „homo facebook“ zu erwarten, dass er seine virtuelle Heimat massenhaft verlässt. Die letzte Völkerwanderung fand im 6. Jahrhundert n. Chr. statt, als die Langobarden in Italien einfielen. Sicherlich wird es auch virtuelle Völkerwanderungen geben. MySpace hat dies bereits gezeigt. Es wird spannend zu beobachten sein, ob Facebook einen ähnlichen Weg gehen wird. Bis dahin appelliert der LfD an die Nutzerinnen und Nutzer von Facebook, ihre Privatsphäre durch restriktive Einstellungen im Netzwerk zu schützen. Die Anstrengung des LfD im Bereich der Medienkompetenz dienen diesem Ziel (vgl. Tz. I-4).

### 3.2.2 Fragen beim Einsatz von Fanpages durch Behörden und Unternehmen im Land

Es wird vertreten, dass Facebook Fanpages dem Betrieb eines Internetangebots vergleichbar seien. Nach dieser Ansicht unterfallen sie als Telemedium den Regelungen des Telemediengesetzes.

Facebook erstellt aus den erhobenen Nutzungsdaten über die Art und den Umfang der Nutzung der Fanpages eine Nutzungsstatistik. Diese wird, soweit es sich um angemeldete Nutzerinnen und Nutzer des Netzwerkes handelt, mit demographischen Angaben wie Alter, Geschlecht und Herkunft der jeweiligen Besucherinnen bzw. Besucher der Seite angereichert und als aggregierter Nutzungsreport den Betreiberinnen und Betreibern der Fanpages zur Verfügung gestellt („Facebook Insights“). Mit der Erstellung einer Fanpage geht insoweit auch die Beauftragung einer Nutzungsanalyse, wie sie in § 15 Abs. 3 TMG geregelt ist, einher. Der Besuch von Nutzerinnen und Nutzern auf einer Facebook Fanpage und deren dortige Aktivitäten werden von Facebook erfasst und ausgewertet. Soweit es sich bei den Nutzerinnen bzw. Nutzern um angemeldete Facebook-Mitglieder handelt, werden diese Daten mit deren Facebook-Profil verknüpft und gespeichert. Wenn man in einer Fanpage also ein Telemedium sieht, würde diese Praxis der Regelung des § 15 Abs. 3 Satz 3 TMG widersprechen, wonach Nutzungsprofile nicht mit Daten über die Trägerin bzw. den Träger des Pseudonyms zusammengeführt werden dürfen. Des Weiteren werden die Nutzerinnen und Nutzer nicht nach § 15 Abs. 3 Satz 2 bzw. § 13 Abs. 1 TMG unterrichtet, und es wird keine Widerspruchsmöglichkeit angeboten. Hinzu kommt, dass auf Fanpages ein Like Button in nicht abschaltbarer und nicht änderbarer Weise integriert ist, so dass die Gesichtspunkte zur Problematik dieser Funktionalität (vgl. Tz. I-3.2.3) alle Fanpage-Inhaberinnen und -Inhaber betreffen.

Vor diesem Hintergrund verschafft sich der LfD derzeit einen Überblick über die tatsächliche Situation bei öffentlichen Stellen in Rheinland-Pfalz. Deshalb hat er zunächst die Ressorts der Landesregierung um eine entsprechende Auskunft gebeten, die ihr eigenes Haus und den jeweils nachgeordneten, ihrer Rechtsaufsicht unterstehenden Bereich betrifft. Außerdem hat er die Kommunen und die Hochschulen im Land unmittelbar um entsprechende Auskünfte gebeten. Diese Umfrage ist derzeit noch nicht abgeschlossen. Es zeigt sich aber bereits jetzt, dass öffentliche Stellen in durchaus nennenswertem Umfang dem Sog von Facebook folgen: Etwa die Hälfte der Hochschulen und Universitäten im Land betreibt eine Fanpage; der Ministerpräsident und die Kultusministerin haben persönliche Fanpages, auch alle Fraktionsvorsitzenden und viele Abgeordneten. Auch sonstige öffentliche Stellen wie die Forstverwaltung oder die Zentralstelle IT-Management, Multimedia, E-Government und Verwaltungsmodernisierung sind bei Facebook aktiv.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Düsseldorfer Kreis haben dazu wie folgt Stellung genommen:

> „Es kann nicht sein, dass die Bürgerinnen und Bürger, die sich auf den Seiten öffentlicher Stellen informieren wollen, mit ihren Daten dafür bezahlen. Unbeschadet der rechtlichen Verantwortung sollten die öffentlichen Stellen auf solchen Plattformen keine Profilseiten oder Fanpages einrichten.“ (Entschließung „Datenschutz bei sozialen Netzwerken jetzt verwirklichen!“der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. September 2011)

Der LfD teilt diese Auffassung. Er wird sich im neuen Jahr an die öffentlichen und privaten Betreiberinnen und Betreiber von Fanpages wenden und mit ihnen das weitere Vorgehen erörtern.

### 3.2.3 Neue Features: Gesichtserkennung, Like Button, Timeline

#### ■ Gesichtserkennung

Facebook führt beim Upload von Bildern seiner Nutzerinnen und Nutzer eine automatische Gesichtserkennung durch. Dazu unterhält das

Unternehmen eine Datenbank mit biometrischen Merkmalen seiner Nutzerinnen und Nutzer. Dies entspricht nicht europäischem und deutschem Datenschutzrecht. Facebook müsste von Nutzerinnen und Nutzern explizit die Erlaubnis einholen, ihre biometrischen Merkmale zu speichern und zu verarbeiten. Um künftig sicherzustellen, dass die neue Technologie der Gesichtserkennung in einer Weise eingesetzt wird, die das informationelle Selbstbestimmungsrecht der Nutzerinnen und Nutzer achtet, hat der zuständige Hamburgische Datenschutzbeauftragte erklärt, die ihm zur Verfügung stehenden rechtlichen Instrumente einsetzen zu wollen. In Betracht kommen die Verhängung eines Bußgeldes wie auch der Erlass einer Ordnungsverfügung.

### ■ Like Button/Gefällt mir Button

Durch die Einbindung des Like Buttons auf einer Website erhält Facebook Kenntnis darüber, dass eine Nutzerin oder ein Nutzer (repräsentiert durch die IP-Adresse) diese Website aufgerufen hat. In der gegenwärtigen Realisierung erfolgt dies bereits beim Aufruf der Seite, d.h. nicht erst beim Betätigen des Buttons. Damit erhält Facebook auch Informationen über Nicht-Mitglieder. Handelt es sich bei der Nutzerin oder dem Nutzer um ein angemeldetes Facebook-Mitglied, wird diese Information über ein vorhandenes Facebook-Cookie namentlich zugeordnet. § 15 Abs. 3 TMG sieht vor, dass über die Inanspruchnahme von Telemedien durch die Nutzerinnen und Nutzer Nutzungsprofile gebildet werden dürfen, dies aber nur in pseudonymisierter Form und in Verbindung mit einer entsprechenden Unterrichtung der Betroffenen. Sie müssen zudem die Möglichkeit haben, der Bildung der Profile zu widersprechen. In der gegenwärtigen Form trägt der Like Button dem nicht Rechnung.

Vor diesem Hintergrund erscheint die Nutzung von Like Buttons durch öffentliche Stellen problematisch. Das sog. „Zwei-Klick-Verfahren“ entschärft die Problematik. Danach erscheint beim Lenken des Cursors auf einen Button eine Information über die Funktionsweise und die Folgen des Anklickens des eigentlichen Social Plugins, das erst nach dem Anklicken des ersten Buttons erscheint. Das Anliegen, die Betroffenen umfassend über die Verarbeitung ihrer Daten zu informieren, kann allerdings auch auf diese Art nicht erfüllt werden, weil Facebook bislang darüber noch keine verlässlichen und umfassenden Angaben zur Verfügung stellt.

### ■ Timeline

Facebook wirbt für seinen neuen Dienst: „Erzähle deine Lebensgeschichte“ mit einem neuartigen Profil. „Fülle diesen weiten, offenen Raum mit einem einzigartigen Bild, das dich am besten darstellt. Es ist das erste, was andere sehen, wenn sie deine Chronik besuchen.
Deine Meldungen: Teile die wichtigsten Beiträge, Fotos und Lebensereignisse in deiner Chronik. Hier kannst du deine Geschichte vom Beginn bis jetzt erzählen.“

Die Nutzerinnen und Nutzer sollen verlockt werden, Facebook als Chronik ihres Lebens mit so vielen Daten wie möglich zu nutzen. Wollen alle, die dieses Angebot grundsätzlich attraktiv finden, ihre Lebensdaten (mit Bildern und Dokumenten aller Art) wirklich einem amerikanischen Unternehmen übertragen, das v.a. an der Gewinnmaximierung interessiert ist und das sich alle Rechte an den eingestellten Inhalten übertragen lässt?

## 3.2.4 Unzureichende Maßnahmen der Datensicherung

Datensicherungsprobleme gewinnen eine grundsätzliche Dimension angesichts der Qualität der in einem sozialen Netzwerk wie Facebook gespeicherten Daten. Diese können zumindest zum Teil dem höchstpersönlichen Lebensbereich der Nutzerinnen und Nutzer zugerechnet werden und haben deshalb „Kernbereichsrelevanz“ im Sinne der Rechtsprechung des Bundesverfassungsgerichts, d.h. sie berühren den Kernbereich des grundrechtlich geschützten Persönlichkeitsrechts.

Vor diesem Hintergrund sind die bekannt gewordenen Datenskandale bzw. Datenlecks insbesondere bei Facebook von besonderer Bedeutung. Z.B. wurde im Mai 2011 eine Sicherheitslücke bekannt. Persönliche Daten wie Fotos und Chatverläufe von Facebook-Nutzerinnen und Nutzern hätten über Jahre hinweg unbefugten Dritten offen gestanden, hieß es in einem Unternehmensblog der US-Sicherheitsfirma Symantec. Es sei auch möglich, dass Unbefugte – in erster Linie Facebooks Werbekundinnen und -kunden – im Namen von angemeldeten Nutzerinnen bzw. Nutzern E-Mails verschickt hätten. Der Fehler bestand seit 2007, erst nach ca. vier Jahren wurde er beseitigt: Werbekundinnen und -kunden konnten über Jahre auf die Profile von Facebook-Anwenderinnen und -Anwendern zugreifen, Fotos ansehen, Chats mitlesen. Nach dem Hinweis der Sicherheitsfirma wurde die Datenlücke geschlossen.

Es ist nicht das erste Mal, dass Facebook von einer derartigen Sicherheitslücke betroffen ist. Ende 2010 hatte es schon einmal ein ähnlich gelagertes Problem gegeben, bei dem einige Facebook-Anwendungen die eindeutigen Profilnummern von Anwenderinnen und Anwendern an Werbefirmen und Adresshändlerinnen und -händler weiterreichten.

Versehentlich wurden den Werbetreibenden sog. „access tokens“ der Anwenderinnen und Anwender übertragen. Dabei handelt es sich quasi um Ersatzschlüssel für den Vollzugriff auf Profildaten der Facebook- Anwenderinnen und -Anwender, erklärt Symantec. Bis April hätten schätzungsweise 100.000 Facebook-Apps durch diesen Fehler Zugang zu solchen „access tokens“ gehabt. Täglich würden rund 20 Millionen Facebook-Apps installiert. Da der Fehler zudem seit der Einführung von Facebook-Apps im Jahr 2007 bestand, ist der potentielle Schaden gewaltig – zumindest theoretisch.

Im Dezember 2011 erschien die Meldung, eine Facebook-Panne ermögliche den Zugriff auf fremde Privatbilder (http://www.heise.de/newsticker/meldung/Facebook-Panne-ermoeglichte-Zugriff-auf-fremde-Privatbilder-1391237.html). Um Zugriff auch auf als privat markierte Bilder anderer Nutzerinnen und Nutzer zu erhalten, musste zunächst ein öffentliches Bild einer Nutzerin bzw. eines Nutzers als anstößig gemeldet werden. Danach bot Facebook an, noch weitere Fotos aus dem Profil als unangemessen zu markieren – dabei bekam man in einigen Fällen Zugang auch zu privaten Bildern.

Facebook erklärte, der fehlerhafte Software-Code sei nur eine begrenzte Zeit online gewesen und habe lediglich eine limitierte Zahl jüngster Fotos unter gewissen Bedingungen offen zugänglich gemacht. Das System sei vorerst deaktiviert worden und werde wieder eingeschaltet, wenn der Fehler endgültig behoben sei.

Der Blogger, der die Lücke entdeckt hatte, erklärte gegenüber dem „Wall Street Journal“, es habe sich schlicht um „entsetzliche Programmierung“ durch Facebook gehandelt. Ein anderer Kommentator betonte, der Fehler zeige, dass Facebook überhaupt kein ernsthaftes und robustes Sicherheitsmodell habe. Dies sei nicht akzeptabel für eine Firma, die so viele potenziell heikle und sensible Daten speichere.

### 3.2.5 Polizeiliche Ermittlungen in sozialen Netzwerken

Umstritten ist, unter welchen Voraussetzungen und in welchem Umfang staatliche Ermittlungsbehörden, v.a. die Polizei, in sozialen Netzwerken recherchieren dürfen.

Aus dem Urteil des Bundesverfassungsgerichts zur Online-Durchsuchung (vom 27. Februar 2008, Az. 1 BvR 370/07 und 1 BvR 595/07) ergibt sich, dass solche Ermittlungsmaßnahmen dann und soweit ohne eine spezielle Rechtsgrundlage zulässig sind, wie sie sich auf öffentlich zugängliche Inhalte des Internets beschränken und die für die Ermittlungsbehörden geltenden Rechtsgundlagen (also die entsprechenden Generalklauseln für die Datenverarbeitung) eine Speicherung und Nutzung dieser Daten erlauben.

> „Verschafft der Staat sich Kenntnis von Inhalten der Internetkommunikation auf dem dafür technisch vorgesehenen Weg, so liegt darin nur dann ein Eingriff in Art. 10 Abs. 1 GG, wenn die staatliche Stelle nicht durch Kommunikationsbeteiligte zur Kenntnisnahme autorisiert ist. Nimmt der Staat im Internet öffentlich zugängliche Kommunikationsinhalte wahr oder beteiligt er sich an öffentlich zugänglichen Kommunikationsvorgängen, greift er grundsätzlich nicht in Grundrechte ein.“
> (aus dem Urteil des Bundesverfassungsgerichts vom 27. Februar 2008, Az. 1 BvR 370/07 und 1 BvR 595/07, 5. Leitsatz, Satz 2)

Daran knüpfen sich zahlreiche Fragen an: Insbesondere umstritten ist, wie weit die „öffentlich zugänglichen“ Kommunikationsvorgänge reichen: Sind z.B. die Inhalte eines Netzwerks, zu dem man nur Zugang auf Empfehlung eines anderen Mitglieds erhält, öffentlich zugänglich? Wie sieht es mit der Verschleierung der Identität der ermittelnden Beamtinnen bzw. Beamten aus: Dürfen sie verschweigen, dass sie amtlich handeln? Dürfen sie Pseudonyme benutzen oder müssen sie als Repräsentantin oder Repräsentant ihrer Behörde handeln? Diese und viele weitere Fragen sind derzeit noch nicht geklärt. Der LfD hat zu diesem Thema Diskussionen mit der Polizei des Landes geführt; die zuständigen Arbeitskreise der Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben sich damit befasst und diskutieren derzeit ein umfangreiches Papier zu diesem Thema, das angesichts der Komplexität der Materie aber noch nicht einvernehmlich verabschiedet werden konnte.

### 3.2.6 Nutzung durch Kinder

Kinder in Europa sind heute schon ab sieben Jahren im Internet unterwegs. 38 Prozent der neun- bis 16-jährigen Internetnutzerinnen und -nutzer haben angegeben, dass sie trotz bestehender Altersbeschränkungen ein Profil in einem sozialen Netz haben (Neelie Kroes, zit. in http://www.heise.de/newsticker/meldung/IT-und-Medienunternehmen-verbuenden-sich-fuer-besseren-Kinderschutz-im-Web-1388192.html). Nach dem Ergebnis der JIM-Studie 2011 des Medienpädagogischen Forschungsverbundes Südwest (mpfs) nutzen aktuell vier Fünftel der deutschen Jugendlichen diese Plattformen zumindest mehrmals pro Woche, 57 Prozent der Internetnutzerinnen und -nutzer loggen sich täglich in ihre Community ein, ein Großteil davon sogar mehrmals täglich. Die Auswahl der Jugendlichen bei sozialen Netzwerken beschränkt sich auf wenige Anbieter, an

erster Stelle steht hier Facebook, das 72 Prozent der zwölf- bis 19-jährigen Onliner nutzen. Sind Jugendliche im Netz unterwegs, hinterlassen sie deutliche Spuren: 65 Prozent haben ein eigenes Foto oder ein Video von sich hochgeladen. Zwei Fünftel haben Bilder oder Filme von Freunden oder Familienangehörigen eingestellt (JIM-Studie 2011; vgl. http://www.mpfs.de/fileadmin/JIM-pdf11/JIM2011.pdf; Tz. I-4.11).

Nach den allgemeinen Geschäftsbedingungen von Facebook dürfen sich dort nur Nutzerinnen und Nutzer anmelden, die mindestens 13 Jahre alt sind. Das Risiko, gemobbt, belästigt oder sogar bedroht zu werden, ist für Kinder besonders groß. Der Düsseldorfer Kreis hat auf Initiative des LfD in einem gesonderten Beschluss auf diese Problematik hingewiesen und Forderungen zur Verbesserung der Situation formuliert (Beschluss vom 25. November 2010, „Minderjährige in sozialen Netzwerken wirksamer schützen“):

„Minderjährige in sozialen Netzwerken wirksamer schützen
Soziale Netzwerke spielen in unserer Lebenswirklichkeit eine zunehmend wichtige Rolle. Minderjährige beteiligen sich in großer Zahl an solchen Netzen. Ihrer besonderen Schutzbedürftigkeit muss über die Anforderungen hinaus Rechnung getragen werden, die grundsätzlich an eine datenschutzgerechte Ausgestaltung solcher Angebote zu stellen sind (vgl. Beschluss des Düsseldorfer Kreises vom 18. April 2008). Hier besteht ein erheblicher Schutz-, Aufklärungs- und Informationsbedarf:

- Das Schutzniveau sozialer Netzwerke wird wesentlich dadurch bestimmt, dass die Betreiber Standardeinstellungen vorgeben, z.B. für die Verfügbarkeit von Profildaten für Dritte. Minderjährige Nutzer haben häufig weder die Kenntnisse noch das Problembewusstsein, um solche Voreinstellungen zu ändern. Die Aufsichtsbehörden fordern die Anbieter sozialer Netzwerke auf, generell datenschutzfreundliche Standardeinstellungen für ihre Dienste zu wählen, durch welche die Privatsphäre der Nutzer möglichst umfassend geschützt wird. Diese Standardeinstellungen müssen besonders restriktiv gefasst werden, wenn sich das Portal an Minderjährige richtet oder von ihnen genutzt wird.
- Es muss erreicht werden, dass die gesetzlich bzw. durch die Betreiber vorgegebenen Grenzen für das Mindestalter der Nutzer eingehalten und wirksam überprüft werden. Dies könnte durch die Entwicklung und den Einsatz von Altersverifikationssystemen oder Bestätigungslösungen gelingen. Solche Verifikationssysteme lösen zwar ihrerseits Datenverarbeitungsvorgänge aus und müssen berücksichtigen, dass die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym möglich bleiben muss (§ 13 Abs. 6 Telemediengesetz); dies begründet aber kein Hindernis für ihren Einsatz.
- Minderjährigen und ihren Eltern wird die Einschätzung, welche der angebotenen Dienste sozialer Netzwerke altersgerecht sind, wesentlich erleichtert, wenn die Betreiber eine freiwillige Alterskennzeichnung von Internetinhalten vornehmen. Denkbar ist auch der Einsatz von Jugendschutzprogrammen, die Alterskennzeichnungen automatisch auslesen und für Minderjährige ungeeignete Inhalte sperren. Die Möglichkeiten, die der Entwurf für einen neuen Jugendmedienschutz-Staatsvertrag hierzu anbietet, müssen intensiv genutzt werden.
- Ebenso wichtig ist die Bewusstseinsbildung bei den minderjährigen Nutzem sozialer Netzwerke für die Nutzungsrisiken und für einen sorgsamen und verantwortungsbewussten Umgang mit den eigenen Daten und den respektvollen Umgang mit den Daten anderer. Die Betreiber sozialer Netzwerke, aber auch staatliche Behörden, Schulen und nicht zuletzt die Eltern stehen in der Pflicht, über bestehende datenschutzfreundliche Nutzungsmöglichkeiten aufzuklären.“

Der LfD thematisiert diese Fragen auch in unmittelbaren Gesprächen mit den Betreibern der sozialen Netzwerke, insbesondere mit Facebook. Darüber hinaus weitet er die Bildungsangebote zur Förderung der Medienkompetenz im Bereich der Schülerworkshops auch auf den Primarbereich aus und adressiert das Angebot in altersmäßig angepasster Form seit Jahresbeginn an die nahezu 1.000 Grundschulen im Land.

Zwar sind 28 große IT- und Medienunternehmen einem Aufruf der EU-Kommissarin Neelie Kroes gefolgt, gemeinsam für ein kinderfreundliches Internet zu sorgen. Die Deutsche Telekom, die RTL Group, Vodafone, Telefonica, Apple, Microsoft, Opera Software, Samsung und andere wollen innerhalb von zwölf Monaten einfachere Meldemöglichkeiten für schädliche Inhalte schaffen, altersgerechte Datenschutzeinstellungen verwenden, Inhalte klassifizieren, Material zu Kindesmissbrauch entfernen und Werkzeuge für die elterliche Kontrolle anbieten.

Fraglich bleibt aber, ob der bisher eingeschlagene Weg der Selbstverpflichtung durch die Anbieter sozialer Netzwerke weiter verfolgt werden kann. So stellt die Europäische Kommission im Juni 2011 enttäuscht fest: „Nur zwei im Auftrag der Europäischen Kommission getestete Websites zur sozialen Vernetzung (Bebo und MySpace) haben Standardeinstellungen, bei denen die Profile Minderjähriger nur den Mitgliedern auf der genehmigten Kontaktliste zugänglich sind, und nur vier Websites gewährleisten, dass Minderjährige standardmäßig nur von Freunden kontaktiert werden können (Bebo, MySpace, Netlog und SchülerVZ).“ Hier muss dringend nachgebessert werden.

### 3.2.7 Empfehlungen für Bedienstete in Bezug auf die Teilnahme an sozialen Netzwerken

Die Polizei des Landes hat Verhaltensempfehlungen für ihre Bediensteten erlassen, die das Ziel verfolgen, das Ansehen der Polizei und den Persönlichkeitsschutz der Bediensteten zu wahren, auch wenn soziale Netzwerke außerdienstlich – im privaten Umfeld – genutzt werden. Die dabei entstehenden Gefahren und die auch hier geltenden gesetzlichen Vorgaben wurden dargestellt.

Auf Anregung des LfD haben nahezu alle Ressorts der Landesregierung jeweils eigene entsprechende Empfehlungen formuliert; das Innenministerium hat zu diesem Zweck Formulierungen für das eigene Haus entwickelt, die den anderen Ressorts als Vorbild dienten (vgl. http://www.datenschutz.rlp.de/downloads/misc/Verhaltensempfehlungen_soziale_Netzwerke_-_ISIM.pdf). Der LfD hat dies begrüßt.

In der Privatwirtschaft haben alle großen Unternehmen entsprechende Richtlinien (oder „Guidelines“) erlassen, die allerdings in erster Linie das Ziel verfolgen, die Reputation des jeweiligen Unternehmens zu schützen. Auch dies belegt, wie bedeutsam diese Netzwerke geworden sind.

## 3.3 Google

### 3.3.1 Google Street View

Über den Google-Dienst Street View, seine Funktionsweise und die damit verbundenen Datenschutzfragen wurde im letzten Tätigkeitsbericht (vgl. 22. Tb., Tz. 4.1) ausführlich berichtet. Dabei wurde besonders auch auf die Aktivitäten des LfD hingewiesen, der sich v.a. um eine ausreichende Information der Bevölkerung bemüht hat. In Zusammenarbeit mit dem Verbraucherschutzministerium hat er ein Faltblatt zu diesem Dienst veröffentlicht, das in einer großen Auflage verteilt worden ist (abrufbar: unter http://www.datenschutz.rlp.de/downloads/misc/Faltblatt_Verbraucherinfo_Google_Street_View.pdf). In zwölf Pressemitteilungen hat er in diesem Zusammenhang über aktuelle Fragen informiert (http://www.datenschutz.rlp.de/de/spezialthemen.php?thema=Google-Street-View).

Nachdem Google auch in Rheinland-Pfalz die Straßen und Häuserfassaden abfotografiert hatte, stellte es die Aufnahmen der 20 größten Städte in das Internet. Dabei handelte es sich um Berlin, Bielefeld, Bochum, Bonn, Bremen, Dortmund, Dresden, Duisburg, Düsseldorf, Essen, Frankfurt am Main, Hamburg, Hannover, Köln, Leipzig, Mannheim, München, Nürnberg, Stuttgart und Wuppertal. Rheinland-pfälzische Städte waren nicht dabei.

Auf Anfrage nannte Google auch konkrete Zahlen zu den eingelegten Widersprüchen:

„Insgesamt gibt es in diesen Städten 8.458.084 Haushalte, erhalten haben wir 244.237 Anträge (gemeint sind Widersprüche). Das entspricht 2,89 Prozent der Haushalte.” Genaue Zahlen für die von Rheinland-Pfälzern eingelegten Widersprüche existieren nicht. Wenn man die Zahl von 2,89 Prozent aller Haushalte auch hier zugrunde legt, kann man von ca. 54.000 Widersprüchen ausgehen. Google speichert die Widerspruchsdaten einschließlich der Namen und Anschriften für drei Jahre. Google nannte als Begründung dafür nicht ausschließbare Klageverfahren. Allerdings hat das Unternehmen zugesichert, diese Daten nur zweckentsprechend für die Durchführung des Widerspruchs und für keine anderen Zwecke zu nutzen.

Wie dem LfD bekannt geworden ist, beabsichtigt Google bis auf Weiteres nicht, Straßenansichten von rheinland-pfälzischen Städten und Gemeinden tatsächlich im Internet zu veröffentlichen (http://www.googlewatchblog.de/2011/01/google-street-view-deutschland-2011). Unabhängig davon ist festzustellen, dass ab März 2011 wieder Google-Fahrzeuge im Land Aufnahmen gefertigt haben. Google begründet dies damit, dass „Google Maps“, also der Karten- bzw. Stadtplandienst von Google, verbessert werden solle. Es seien dieselben Autos, die auch für Google Street View genutzt worden seien. Derzeit bestünden aber keine Pläne, die aufgenommenen Bilder im Internet in Google Street View darzustellen.

Bei ihren Fahrten durch die Städte und Gemeinden unseres Landes wurden aber nicht nur fotografische Aufnahmen der Straßenzüge und der öffentlichen Plätze gefertigt. Vielmehr waren alle für Google Street View im Einsatz befindlichen Fahrzeuge mit technischen Geräten zur Kartografierung von WLAN-Netzen ausgerüstet.

Wireless Local Area Network (WLAN):
„drahtloses lokales Netzwerk“, bezeichnet ein lokales Funknetz. Es ermöglicht einen drahtlosen Zugang in das Internet. WLAN kann auch als Plattform zur Lokalisierung in Städten und Gebäuden verwendet werden. Google nutzt die Daten von WLANs zur Lokalisierung der Nutzerinnen und Nutzer, und bietet so eine Alternative zur Lokalisierung per GPS.

Bei dieser WLAN-Erhebung wurden auch Inhaltsdaten aufgefangen, die über die erfassten Funknetze übertragen worden sind. Zwar ist dies für die betroffenen Funknetze nicht kontinuierlich erfolgt, sondern aufgrund der

Tatsache, dass fünfmal in der Sekunde der Funkkanal gewechselt wurde, lediglich fragmentarisch. Angesichts der hohen Bandbreite aktueller Funknetze handelt es sich jedoch um „Fragmente“ von nennenswerter Größe.

Google selbst hat in öffentlichen Erklärungen den Sachverhalt eingeräumt. Damit sind nach Auffassung des LfD in allen Städten und vielen Gemeinden des Landes Rheinland-Pfalz die objektiven Tatbestandsmerkmale gem. § 44 Abs. 1 BDSG, § 202b StGB und § 148 Abs. 1 i.V.m § 89 TKG erfüllt worden. Auch wenn Google seit dem 6. Mai 2010 diese Datenerhebung gestoppt hat, sind die begangenen Rechtsverstöße als erheblich zu bezeichnen und deshalb auch zu ahnden. Der LfD hat als zuständige Aufsichtsbehörde bei allen acht Staatsanwaltschaften des Landes Strafantrag gegen die Verantwortlichen der Firma Google in den USA und in Deutschland gestellt.

Der Hamburgische Datenschutzbeauftragte hat die Rechtslage für seinen Bereich in entsprechender Weise beurteilt und deshalb in Hamburg ebenfalls Strafantrag gestellt. Inzwischen sind die rheinland-pfälzischen Strafanträge an die Hamburger Staatsanwaltschaft abgegeben worden, da dort zentral ermittelt wird. Bislang steht eine abschließende Verfügung seitens der Staatsanwaltschaft noch aus.

Im September 2010 hat der Bundesinnenminister zu einem Spitzengespräch eingeladen, als dessen Folge die Internetwirtschaft Anfang Dezember 2010 den Entwurf eines selbstverpflichtenden Datenschutzkodexes vorlegte (vgl. Tz. I-2.2 und Tz. I-3.2.6).

BITKOM ist der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. mit Sitz in Berlin.

Er ist das Sprachrohr der IT-, Telekommunikations- und Neue-Medien-Branche und vertritt mehr als 1.600 Unternehmen, davon über 1.000 Direktmitglieder. Hierzu gehören fast alle Großunternehmen des Bereichs sowie 700 Mittelständler. Die BITKOM-Mitglieder erwirtschaften 135 Milliarden Euro Umsatz und exportieren Hightech im Wert von 50 Milliarden Euro. BITKOM repräsentiert damit ca. 90 Prozent des deutschen ITK-Markts.

Diesen Kodex hat der BITKOM zwischenzeitlich in Kraft gesetzt, ohne die Anliegen der Datenschutzaufsichtsbehörden ausreichend zu berücksichtigen (vgl. Beschluss des Düsseldorfer Kreises vom 8. April 2011 „Datenschutz-Kodex des BITKOM für Geodatendienste unzureichend – Gesetzgeber gefordert“, abrufbar unter http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=ddk&ber=20110408Umlauf_bitkomgeo).

Die Datenschutzaufsichtsbehörden setzen sich einhellig dafür ein, dass die Betroffenen ein Recht haben, vor Veröffentlichung der Gebäudeansichten im Internet dagegen Widerspruch einzulegen. Dabei ist das Verfahren so zu gestalten, dass die verantwortlichen Unternehmen nicht erfahren, wer den Widerspruch erhoben hat, sondern lediglich wissen, dass zu einer bestimmten Adresse ein Widerspruch vorliegt. Dieses Anliegen ist vom BITKOM abgelehnt worden. Er hält es für ausreichend, dass eine Widerspruchsmöglichkeit dann besteht, wenn die Bilder bereits im Internet veröffentlicht sind und dort eingesehen und konkret bezeichnet werden können. Das Problem, dass bis zur Umsetzung von Widersprüchen die betroffenen Bildansichten von Dritten bereits vervielfältigt worden sein können, hält der Branchenverband für nicht bedeutsam.

Dem können die Datenschutzaufsichtsbehörden nicht zustimmen. Aus ihrer Sicht ist deshalb die vorliegende Selbstverpflichtung keine ausreichende Umsetzung des geltenden Rechts und hindert die Aufsichtsbehörden nicht, gegen solche Unternehmen auch mit aufsichtsbehördlichen Mitteln vorzugehen, die sich auf diesen Kodex berufen.

### 3.3.2 Google Analytics

Nach Maßgabe der im Beschluss des Düsseldorfer Kreises genannten Anforderungen war der von Google angebote Dienst „Google Analytics“ (GA) in der zunächst angebotenen Form nicht datenschutzkonform zu betreiben.

Defizitpunkte waren dabei:

- das zur Umsetzung des Widerspruchs von Google angebotene Browser-Plugin war nur für einen Teil der gängigen Browser verfügbar,
- eine Anonymisierung von IP-Adressen erfolgte nur in Teilbereichen; beim Abruf des eigentlichen GA-Scripts wurde weiterhin die vollständige Adresse übertragen,
- entgegen der ursprünglichen Aussage von Google verhinderte das Plugin nicht, dass auf dem Rechner der Nutzerinnen und Nutzer Cookies gesetzt wurden und es den Betreiberinnen und Betreibern damit auch bei ausgeübtem Widerspruch möglich war, Nutzungsprofile zu bilden,
- der von Google vorgesehene Text zur Unterrichtung der Nutzerinnen und Nutzer enthielt keinen Hinweis auf die Widerspruchsmöglichkeit nach § 15 Abs. 3 TMG,
- mit Blick auf Google als Anbieter mit Sitz in den USA war unklar, an welchem Ort die Nutzungsdaten verarbeitet werden und über welche faktischen

Kontrollmöglichkeiten die Auftraggeberinnen bzw. Auftraggeber verfügen,
- der von Google vorgesehen Mustervertrag zwischen den Websitebetreiberinnen und -betreibern und Google zur Nutzung von GA entsprach nicht den Anforderungen des § 11 BDSG.

Die Verantwortung für ein datenschutzgerechtes Internetangebot liegt bei den Betreiberinnen und Betreibern, auch wenn diese für die Reichweitenanalyse auf Dienstleisterinnen und Dienstleister zurückgreifen.

Mit Blick auf die Nutzung in Internetangeboten rheinland-pfälzischer Stellen hatte der LfD daher Unternehmen und Verwaltungen darauf hingewiesen, dass die von Google angebotene Lösung den datenschutzrechtlichen Anforderungen nicht entsprach und Internetangebote, die auf diesen Dienst zurückgreifen, Gefahr liefen, gegen datenschutzrechtliche Vorgaben zu verstoßen.

Aufgrund der durch die Diskussion ausgelösten Verunsicherung insbesondere im Bereich der Unternehmen und der wiederholten Vorstöße der Datenschutzaufsichtsbehörden hat Google sich nach anfänglichem Sträuben einem konstruktiven Dialog nicht verschlossen. Letztlich ist es in Verhandlungen der Datenschutzbehörden unter Federführung des Hamburgischen Datenschutzbeauftragten gelungen, eine datenschutzkonforme Lösung abzustimmen. So wurde Mitte 2011 eine überarbeitete Version des Analysedienstes bereit gestellt, die einen datenschutzkonformen Einsatz ermöglicht.

Diese gewährleistet insbesondere folgende Punkte:

- Den Nutzerinnen und Nutzern wird eine Möglichkeit zum Widerspruch gegen die Erfassung von Nutzungsdaten eingeräumt. Google stellt hierfür ein sog. Deaktivierungs-Add-On zur Verfügung, das in alle gängigen Browser eingebunden werden kann.
- Auf Anforderung der Websitebetreiberinnen und -betreiber wird die IP-Adresse vor jeglicher Speicherung anonymisiert, so dass darüber keine Identifizierung der Nutzerinnen bzw. Nutzer mehr möglich ist. Die Anonymisierung wird innerhalb Europas durchgeführt, d.h. es werden in der Regel keine Daten in die USA übertragen.
- Der Mustervertrag, den Google für die Websitebetreiberinnen und -betreiber bereit stellt, genügt nunmehr den Vorgaben des Bundesdatenschutzgesetzes zur Auftragsdatenverarbeitung.

Um einen datenschutzgerechten Einsatz von Google Analytics sicher zu stellen, bedarf es dabei bestimmter Einstellungen im Angebot der Websitebetreiberinnen und -betreiber.

Betreiberseitige Pflichten für einen datenschutzgerechten Einsatz von Google Analytics:

- Abschluss des Mustervertrags zur Auftragsdatenverarbeitung
- Information der Nutzerinnen und Nutzer über die Datenverarbeitung durch Google in einer Datenschutzerklärung
- Hinweis auf die Widerspruchsmöglichkeit mit Link auf das Google-Analytics Opt-out-Plugin
- Einstellungen zur IP-Anonymisierung im GA-Programmcode der betroffenen Seiten des Internetangebots
- Löschung der Altdaten durch Anlage eines neuen Google Analytics-Accounts

Hinweise:
http://www.datenschutz.rlp.de/downloads/oh/oh_google_analytics.pdf

Google Analytics Mustervertrag:
http://www.datenschutz.rlp.de/de/aktuell/2011/images/Google_Analytics_Nutzungsbedingungen_und_Regelungen_zur_Auftragsdatenverarbeitung_01.09.11.pdf

Google Analytics Deaktivierungs-Plugin:
http://tools.google.com/dlpage/gaoptout?hl=de

Das von Google zur Umsetzung eines Widerspruchs angebotene Plugin ist nunmehr für ca. 98 Prozent der in Deutschland genutzten Browser verfügbar. Dies erscheint hinreichend, da die übrigen Browser nur marginale Marktanteile haben oder singulären Zwecken dienen (Spielekonsolen). Zwar kann das Plugin damit nicht in allen vorhandenen Browsern installiert werden, es wird jedoch eine hohe Marktabdeckung erreicht und bei Bedarf stehen ausreichende Alternativen zur Verfügung.

Die auf Smartphones genutzten Browser werden nach derzeitigem Kenntnisstand allerdings weiterhin nicht erfasst. Dies hat seine Ursache darin, dass die dort genutzten Browser bislang nur zum Teil die Plugin-Technik unterstützen. Angesichts der steigenden Bedeutung der Internetnutzung via Smartphone wurde dies gegenüber Google als Punkt thematisiert, für den mittelfristig ebenfalls eine angemessene Lösung gefunden werden muss.

## 3.4 Cyber-Attacken

Auch wenn viele Unternehmen sich bei der IT-Sicherheit gut aufgestellt fühlen, stellen Angriffe auf die IT-Strukturen eine der gegenwärtig größten Gefährdungen für die

Wirtschaft dar. Zu diesem Ergebnis kommt eine Untersuchung der Arbeitsgemeinschaft für Sicherheit der Wirtschaft ASW e.V. Als besorgniserregend wird dabei insbesondere die Entwicklung der Wirtschaftsspionage gesehen. Organisierte Kriminalität, aber auch Nachrichtendienste führen nach den Erkenntnissen des Bundesamtes für Sicherheit in der Informationstechnik hoch professionelle Angriffe auf die Informationstechnik von Firmen und Behörden durch. Obwohl in der Mehrheit der Unternehmen schützenswerte oder unternehmenskritische Informationen vorliegen, findet sich nur bei wenigen ein risikoadäquates Konzept zum Schutz von Unternehmens- und Kundendaten. Die Sicherheitsvorfälle des Jahres 2011 – vielfach bereits als das „Jahr der Hacker" bezeichnet – haben vor Augen geführt, wie verwundbar Organisationen, Wirtschaft und Verwaltung in der digitalen Welt sind.

Unternehmen und Verwaltungen werden damit verstärkt Ziele sog. Cyber-Attacken. Das Risiko, Opfer einer solchen Attacke zu werden, wird dabei nicht von der Größe oder Bedeutung eines Unternehmens bestimmt, sondern von finanziellen Interessen, allgemeinen gesellschaftspolitischen Zielen oder lokalen Aspekten. Betroffen sind grundsätzlich alle Unternehmen, wobei kleine und mittlere Unternehmen häufig Nachholbedarf bei der Organisation der IT-Sicherheit haben. Eine Studie aus dem Jahr 2011 zur Lage der IT-Sicherheit im Mittelstand belegt, dass noch immer viele Unternehmen dieses Thema grob vernachlässigen.

Auch die Erkenntnisse des LfD zeigen, dass das Verständnis für die Notwendigkeit einer angemessenen IT-Sicherheit zum Teil nur gering ausgeprägt ist. So hat sich z.B. bei der Kontrolle von Online-Zugängen ergeben, dass diese erhebliche Sicherheitsdefizite aufwiesen. Bei nahezu allen Zugängen war der Einsatz von Passwörtern mangelhaft und hat bei probeweisen Anmeldeversuchen in mehreren Fällen den Zugriff auf Kundendaten ermöglicht. Meist lag die Ursache in einer eher unbekümmerten Einschätzung der Gefährdungslage im Internet, ein Aspekt, der insbesondere bei Unternehmen, deren Kerngeschäft nicht das Online-Business ist, eine Rolle spielt. Daneben war es jedoch auch die Sorge, dass eine bessere Absicherung den Nutzungskomfort beeinträchtigen könnte. Hier wurde also eine mangelnde Sicherheit bewusst in Kauf genommen und der Wettbewerb bei Kundenakquise- und Kundenbindung auf Kosten des Sicherheitsniveaus ausgetragen.

Die von dem Sicherheitsunternehmen MacAfee aufgedeckte Operation „Shady Rat", bei der über Jahre hinweg systematisch Regierungen, Organisationen und Unternehmen ausgespäht wurden, belegt, dass sich das Bild des Hackers gewandelt hat. Wer glaubt, es handele sich um blasse IT-Freaks, die, umgeben von Kaffeebechern und Pizzaschachteln im Halbdunklen in IT-Systeme eindringen, um ihre soziale Inkompetenz zu kompensieren, oder um coole IT-Gurus, die mit der latenten Arroganz der Wissenden einen Hack als intellektuelle Herausforderung betrachten, der muss sich eines Besseren belehren lassen.

Die Angriffe sind nach den Informationen des Bundeskriminalamts zielgerichteter und geschickter geworden. Internetkriminelle arbeiten auf internationaler Ebene arbeitsteilig zusammen und bieten in einer „Underground Economy" interessierten Stellen Schadprogramme oder die Nutzung krimineller IT-Infrastrukturen zum Kauf oder zur Miete an. Bei professionell ausgeübter Industriespionage stehen Produktunterlagen, Konstruktionszeichnungen oder technische Informationen im Visier der Täterinnen bzw. Täter, in anderen Fällen Unternehmens- oder Kundendaten.

Operation „Shady Rat":

http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

Ein problematischer Punkt ist aus Sicht des LfD auch die Tatsache, dass viele Unternehmen in der Frage des Zugangs zu Kundendaten durch Dienstleistende oder Zulieferernde großzügig bis sorglos sind. Kontrollen des LfD haben gezeigt, dass z.B. Callcenter, die für Unternehmen z.B. eine Kundenhotline oder einen telefonischen Notdienst betreiben, häufig Zugriff auf Kundendatenbanken erhalten, der über das Erforderliche deutlich hinausgeht. Wie problematisch dies sein kann, zeigt sich daran, dass auf diesem Weg bereits Versichertendaten von Krankenkassen abgeflossen sind. Ein anderer Fall betraf Millionen von Datensätzen, die bei einer Drogeriekette entwendet wurden; auf diese Daten konnte aufgrund einer Sicherheitslücke bei einem Dienstleister, der mit dem Versand von Newslettern betraut war, zugegriffen werden.

Die Unternehmen müssen sich bewusst werden, dass mit der Nutzung des Internets für Unternehmenszwecke Datenschutz- und Sicherheitsrisiken verbunden sind, die bereits bei der Planung von Geschäftsprozessen beachtet werden müssen. Dies betrifft nicht nur den Kernbereich des Unternehmens, sondern schließt Zuliefernde, Dienstleistende, Geschäftspartnerinnen und Geschäftspartner sowie Kundinnen und Kunden ein. Datenschutz im Unternehmen ist keine lästige Pflicht, sondern Voraussetzung für ein erfolgreiches Agieren im Netz.

Bei Online-Angeboten, Kundenportalen usw. stehen offenkundig primär Funktionalität, Benutzerfreundlichkeit, Marketinggesichtspunkte, Interaktion usw. im Vordergrund. Gerade auch mit Blick auf die vielfältigen Möglichkeiten im Internet hinken Sicherheit und Datenschutz häufig hinterher. Teilweise auch deswegen, weil aufgrund der Abstraktheit mancher Sicherheitsfragen diese verdrängt werden. Was man nicht versteht, wird als unwichtig eingeordnet. Menschlich vielleicht verständlich, im Ernstfall jedoch fatal.

Mangelndes Sicherheitsbewusstsein bzw. das Fehlen angemessener Sicherheitskonzepte spielt auch eine Rolle bei der Einschätzung, inwieweit sog. „Innentäter“ ein Risiko darstellen, sei es durch vorsätzlich missbräuchliches Handeln oder durch Nachlässigkeit. Häufig fehlt es nach Einschätzung des LfD an Mechanismen, mit denen missbräuchliche Zugriffe erkannt werden können. Vorhandene Sicherheitskonzepte zielen oftmals lediglich auf die IT-Infrastruktur und tragen den Risiken auf Anwendungsebene oder in den Geschäftsprozessen nicht Rechnung.

Die IT-Sicherheitslage im Mittelstand 2011. Eine Studie der Initiative „Deutschland sicher im Netz“

http://www.sicher-im-netz.de/files/documents/unternehmen/studie_itsicherheitslage_mittelstand_2011.pdf

Im Frühjahr 2003 erarbeitete der IT-Ausschuss der Landesregierung unter Beteiligung des LfD Leitlinien zur IT-Sicherheit in der Landesverwaltung. Diese wurden durch den Beschluss „Planung und Realisierung der IT-Sicherheit“ des Ministerrates (vgl. MinBl. vom 4. Juni 2003) verbindlich festgelegt. Die tatsächliche Umsetzung erfolgte jedoch zunächst nur zögerlich, so dass der LfD in den vergangenen Tätigkeitsberichten wiederholt die geforderten Maßnahmen anmahnte (vgl. 22. Tb., Tz. 13.4; 21. Tb., Tz. 21.2.1).

Im aktuellen Berichtszeitraum erfolgte nun die vom LfD geforderte Umsetzung u.a. durch:

- Benennung von IT-Sicherheitsbeauftragten in den Ressorts,
- Erstellung einer Informationsplattform zur IT-Sicherheit durch den Landesbetrieb Daten und Information (LDI) und
- Bildung einer Arbeitsgruppe unter Beteiligung der IT-Sicherheitsbeauftragten, der IT-Zentralstelle, des LDI und des LfD zum Aufbau eines Computer Emergency Response Teams (CERT-rlp).

Nach fast zweijähriger Planungsphase nahm das CERT-rlp am 4. Juli 2011 seinen Betrieb auf. Der LfD steht in laufendem Kontakt zum LDI als Kopfstelle des CERT und wird dessen Tätigkeit weiterhin verfolgen.

Die Sicherheitsleitlinien sind für rheinland-pfälzische Stellen aus dem rlp-Netz über folgenden Link abrufbar: https://www.it-sicherheit.rlp.de/fileadmin/ldi/IT-Sicherheit/PDF-Dokumente/Rundschreiben_der_Landesregierung_vom_7-5-2003.pdf

## 3.5 Der Staatstrojaner

Im Zusammenhang mit dem Urteil des Bundesverfassungsgerichts zur Online-Durchsuchung vom Februar 2008 hatte der LfD in seinem Datenschutzbericht 2008/2009 auch die sog. Quellen-TKÜ thematisiert, also die Möglichkeit, Internettelefonate vor bzw. nach der Verschlüsselung in den EDV-Geräten der Beteiligten abhören zu können (vgl. 22. Tb., Tz. 7.3). Für solche Maßnahmen gibt es – sofern sie zu präventiven Zwecken eingesetzt werden – im rheinland-pfälzischen Polizei- und Ordnungsbehördengesetz eine ausreichende Rechtsgrundlage. Für Zwecke der Strafverfolgung berufen sich die Sicherheitsbehörden auf § 100a StPO, was von den Datenschutzbeauftragten allerdings in Frage gestellt wird.

Die Quellen-TKÜ für Zwecke der Strafverfolgung geriet in die öffentliche Diskussion, als der Chaos Computer Club im Oktober 2011 die Analyse eines Trojaners veröffentlichte, der offenbar von einer staatlichen Stelle auf der Festplatte eines Betroffenen installiert worden war. Aufgrund seiner Untersuchung kam der Chaos Computer Club zu schwerwiegenden Vorwürfen: Die eingesetzte Technik erlaube sehr viel mehr als gesetzlich erlaubt sei. Es sei nicht zu kontrollieren, was tatsächlich geschehe, wenn ein solcher Trojaner eingesetzt werde. Zudem sei es Dritten möglich, über Schwachstellen den Trojaner selbst für ihre Zwecke unbemerkt zu nutzen.

Diese Analyse führte zu einer intensiven Diskussion, nicht nur in den Medien, sondern auch in den Parlamenten. Im Wesentlichen ging es um den Vorwurf, die Sicherheitsbehörden seien nicht in der Lage, das von ihnen eingesetzte Instrumentarium zu beurteilen und zu beherrschen. Im Landtag wurden in diesem Zusammenhang zwei Kleine Anfragen gestellt (LT-Drs. 16/534 und 16/560).

Der LfD hatte unmittelbar nach Erscheinen der Pressemeldungen das Innenministerium um Mitteilung gebeten, ob und in welchem Umfang eine vergleichbare Software auch in Rheinland-Pfalz zum Einsatz gekommen sei. Zeitnah wurden mehrere Gespräche mit dem Innenministerium und dem Landeskriminalamt geführt. Daraus ergab sich, dass im November 2010 auch in Rheinland-

Pfalz Maßnahmen für die Durchführung einer Quellen-TKÜ zum Zwecke der Strafverfolgung auf der Grundlage von § 100a StPO getroffen worden sind.

Hintergrund war ein Ermittlungsverfahren wegen schweren Raubes. Da die rheinland-pfälzische Polizei im November 2010 nicht über die notwendige Hard- und Software für die Durchführung einer Quellen-TKÜ verfügte, hatte sie das Bundeskriminalamt um Amtshilfe gebeten. Dieses beauftragte die Firma DigiTask, auf der Grundlage der Vorgaben des richterlichen Beschlusses eine individuelle Überwachungssoftware für diese Quellen-TKÜ zu entwickeln. Das Bundeskriminalamt hat die Software zuvor auf die Funktionalitäten der im richterlichen Beschluss enthaltenen Vorgaben geprüft und dabei festgestellt, dass der Funktionsumfang der Software nicht über die Vorgaben des richterlichen Beschlusses und der beim Hersteller DigiTask beauftragten Funktionen hinausging. Die eingesetzte Version des „Trojaners“ war nicht mit der identisch, die vom Chaos Computer Club analysiert worden ist: Einige Punkte, insbesondere zur technischen Sicherheit, waren gegenüber dieser Version verbessert worden.

In mehreren Gesprächen mit dem LfD betonten die Sicherheitsbehörden, dass es notwendig sei, auch die über das Internet geführte Telekommunikation abhören zu können. Davon ist z.B. die Sprachtelefonie mithilfe von Skype ebenso wie der Versand von E-Mails betroffen. In einer Zeit, in der etwa 50 Prozent der Telefongespräche über das Internet abgewickelt werden, würde es gerade bei der Verfolgung schwerer Kriminalität auf eine Verhinderung der Strafverfolgung hinauslaufen, wenn ein solches Instrument nicht zur Verfügung stünde.

Der LfD verschließt sich dieser Auffassung nicht. Allerdings ist festzuhalten: Grundlage des Einsatzes einer Technik, die in private Computer der Bürgerinnen und Bürger unbemerkt eindringt und damit nicht nur in das Fernemeldegeheimnis, sondern auch in das „Computer-Grundrecht“ eingreift, muss ein Gesetz sein, das folgende Voraussetzungen regelt:

- es muss in seiner Anwendung auf schwerste Kriminalität begrenzt sein;
- es sind technisch-organisatorische Vorkehrungen vorzuschreiben, welche die Datenerhebung allein auf Kommunikationsdaten beschränken und durch die Datenverarbeitungsvorgänge revisionssicher nachvollziehbar erfolgen;
- zur Sicherung des Kernbereichs der privaten Lebensgestaltung ist ein wirksames Verfahren vorzusehen;
- der technische Datenschutz muss besonders betont werden, damit insbesondere verhindert wird, dass die sicherheitsbehördlichen Instrumente durch Dritte missbraucht werden.

Derzeit fehlt ein solches Gesetz für den Bereich der Strafverfolgung. §§ 100a, 100b StPO reichen dafür – auch mit ausführlichen richterlichen Anordnungen – nicht aus. Die Datenschutzbeauftragten des Bundes und der Länder haben bereits im März 2011 die Entschließung „Ohne gesetzliche Grundlage keine Telekommunikationsüberwachung auf Endgeräten“ verabschiedet, in der entsprechende Forderungen erhoben werden. Leider sind zwischenzeitlich keine Schritte zur Umsetzung eingeleitet worden. Diese sind überfällig. Außerdem muss aufgrund der nunmehr gewonnenen Erkenntnisse auch erwogen werden, für den Bereich der Justiz Strukturen zu schaffen, durch die den Richerinnen und Richtern das nötige Know-how bei der Entscheidungsfindung zur Verfügung gestellt wird (vgl. Tz. II-8.2.5).

Der LfD begrüßt das derzeit bestehende Moratorium, wonach die Sicherheitsbehörden bis auf Weiteres auf den Einsatz entsprechender Abhörsoftware verzichten. Dieses Moratorium darf erst nach Erlass bundesgesetzlicher Regelungen aufgehoben werden, die den o.g. Anforderungen entsprechen.

Für künftige Maßnahmen der Quellen-TKÜ in Rheinland-Pfalz muss außerdem sichergestellt sein, dass eine ausschließlich auf den Einzelfall abgestimmte Software zum Einsatz kommt, bei der die technischen Funktionalitäten den gesetzlichen Anforderungen und der richterlichen Anordnung entsprechen. Hierzu will die Landesregierung die erforderlichen technischen und organisatorischen Datenschutzmaßnahmen weiter konkretisieren und die verbindliche Realisierung solcher Anforderungen festlegen. Deshalb hat sich am 31. Oktober 2011 eine gemeinsame Gesprächsrunde von Vertreterinnen und Vertretern des LfD, des Ministeriums der Justiz und für Verbraucherschutz, des Ministeriums des Innern, für Sport und Infrastruktur und des Landeskriminalamtes mit der Thematik befasst und hierbei insbesondere Erfordernisse im Hinblick auf die Schaffung verfahrenssichernder Regelungen erörtert. Es wurde vereinbart, dass das Landeskriminalamt zeitnah den Entwurf von Verfahrensregelungen sowie eines Datenschutzkonzeptes erarbeitet. Dem LfD wird hierbei Gelegenheit gegeben, seine Vorstellungen einzubringen. Bis zur Erstellung solcher Festlegungen soll kein Trojaner im Land eingesetzt werden.

Am 20. Oktober 2011 hat sich auch die Innenministerkonferenz mit dem Themenkomplex Quellen-TKÜ befasst. Hierbei hat der Bundesminister des Innern über seine

Entscheidung berichtet, wonach der Bund beim Bundeskriminalamt ein Kompetenzzentrum einrichten wird. Dort soll in Eigenentwicklung eine Software für die Durchführung von Quellen-TKÜ erstellt werden. Der Bund hat den Ländern angeboten, sich an dem Kompetenzzentrum zu beteiligen. Eine Arbeitsgruppe soll ein Gesamtkonzept für ein Kompetenzzentrum im Bundeskriminalamt zum Einsatz und zur Eigenprogrammierung einer Software sowie zur Zertifizierung durch ein externes Expertengremium erstellen.

### 3.6 Das digitale Krankenhaus

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder verabschiedete auf ihrer 78. Sitzung im Oktober 2009 eine Entschließung („Krankenhausinformationssysteme datenschutzgerecht gestalten!“), in der die Betreiber und Hersteller von Krankenhausinformationssystemen (KIS) zu einer datenschutzgerechteren Ausgestaltung der im Krankenhausbetrieb eingesetzten Verfahren aufgefordert wurden. Beweggründe hierfür waren sowohl der zunehmende Einsatz entsprechender IT-Produkte im Klinikalltag als auch diverse von den Datenschutzbeauftragten im Rahmen ihrer Tätigkeit festgestellte Defizite bei der automatisierten Verarbeitung von Patientendaten durch Krankenhäuser.

Eine von der Konferenz eingesetzte Arbeitsgruppe fasste in einem ersten Schritt die sich aus den geltenden datenschutzrechtlichen Vorgaben ergebenden allgemeingültigen normativen Eckpunkte für die Datenverarbeitung im Krankenhausbereich zusammen und leitete daraus konkrete technische Handlungsbeispiele für die Ausgestaltung und den Betrieb von KIS ab. In die Orientierungshilfe flossen auch die Ergebnisse zweier Expertenanhörungen von KIS-Betreibern und KIS-Herstellern ein. Das Papier, das die bestehenden rechtlichen Vorgaben nicht ersetzt und daher auch keine eigene Rechtsqualität besitzt, wurde im März 2011 auf der 81. Sitzung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder formell verabschiedet (vgl. http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=dsb&ber=081_kis).

Auf der Grundlage der rechtlichen Vorgaben des Datenschutzes und der ärztlichen Schweigepflicht bildet die Orientierungshilfe, die mittlerweile auch im Bereich der kirchlichen Datenschutzbeauftragten zustimmend zur Kenntnis genommen wurde, den Maßstab für die Beratungs- und Kontrolltätigkeit der staatlichen Datenschutzaufsicht. Deren Handlungsspielräume bleiben gleichwohl unangetastet. Werden Defizite im Vergleich zu den Inhalten der Orientierungshilfe festgestellt, sollen diese unter Wahrung der Patientensicherheit in einer angemessenen Übergangszeit und in einem geordneten Prozess mit den Betreibern und den Systemherstellern ausgeräumt werden. Angesichts des dynamischen Wandels der Strukturen und Arbeitsprozesse in den Krankenhäusern, aber auch der daraus resultierenden Anforderungen an die eingesetzten IT-Verfahren, soll das Dokument zudem auch künftig fortgeschrieben werden.

Die Orientierungshilfe war Gegenstand mehrerer Gespräche zwischen der Arbeitsgruppe der Datenschutzkonferenz und der Deutschen Krankenhausgesellschaft. Nach anfänglichem Widerstand reduzierten sich die von der Deutschen Krankenhausgesellschaft erhobenen inhaltlichen Bedenken gegen das Papier im Wesentlichen auf zwei Punkte: die Hinweispflicht der Krankenhäuser auf das den Patientinnen und Patienten auch aus der Sicht der Deutschen Krankenhausgesellschaft zustehende Widerspruchsrecht gegen die Hinzuziehung von Vorbehandlungsakten sowie die Pflicht zur Protokollierung von lesenden Zugriffen auf die Verfahren. Hierzu sowie zur Angemessenheit und Umsetzbarkeit der aus der Orientierungshilfe resultierenden Anforderungen wird der Dialog mit der Deutschen Krankenhausgesellschaft auch künftig fortgesetzt.

Der LfD unterstützt das mit der Orientierungshilfe verbundene Anliegen durch zahlreiche Maßnahmen auf Landesebene.

In mehreren Gesprächen mit Vertreterinnen und Vertretern der Krankenhausgesellschaft Rheinland-Pfalz erörterte der LfD Inhalt und Zielrichtung der von der Datenschutzkonferenz im März 2011 veröffentlichten Orientierungshilfe. Übereinstimmend begrüßten die Beteiligten das mit dem Papier verbundene Anliegen einer generellen Stärkung des Datenschutzes im Krankenhaus. Inhaltlich teilte die Krankenhausgesellschaft Rheinland-Pfalz die von der Deutschen Krankenhausgesellschaft zu der Orientierungshilfe abgegebene Bewertung. Zugleich erklärte sie sich grundsätzlich bereit, die seitens des LfD nach der Veröffentlichung der Orientierungshilfe ins Auge gefassten Maßnahmen zur Verbesserung des Datenschutzes im Klinikbereich zu unterstützen.

Gemeinsam mit den auf dem Gebiet des Landes Rheinland-Pfalz zuständigen Datenschutzbeauftragten der evangelischen und katholischen Kirchen stellte der LfD die besondere Bedeutung des Datenschutzes im Krankenhausbetrieb und die hierzu erstellte Orientierungshilfe heraus. Unter Betonung der jeweiligen Zuständigkeitsgrenzen qualifizierten die Datenschutzbeauftragten das Papier einvernehmlich als taugliche Grundlage zur Stärkung des Datenschutzes beim Einsatz von IT-Verfahren im Bereich der Krankenhäuser. Sowohl die

Konferenz der katholischen Datenschutzbeauftragten in Deutschland als auch das entsprechende Gremium im Bereich der evangelischen Kirchen nahmen in eigenen Beschlüssen im Mai 2011 die Orientierungshilfe zustimmend zur Kenntnis.

In einer ganztägigen Informationsveranstaltung stellte der LfD im Juni 2011 der Fachöffentlichkeit die Orientierungshilfe und das damit verbundene Anliegen vor. An der Veranstaltung nahmen Vertreterinnen und Vertreter nahezu aller rheinland-pfälzischer Krankenhäuser und deren Verbände sowie Vertreterinnen und Vertreter aus Politik, Wirtschaft und Kirchen teil. Grundkonsens aller Beiträge war die ausdrückliche Bereitschaft, trägerübergreifend ein vergleichbares und angemessenes Datenschutzniveau in den jeweiligen Einrichtungen sicherzustellen. Die von den Datenschutzbeauftragten vorgelegte Orientierungshilfe wurde dabei übereinstimmend als geeignete und längst überfällige erste Richtschnur begrüßt.

Infolge der öffentlichen Präsentation der Orientierungshilfe regte der größte rheinland-pfälzische Krankenhausträger im psychiatrisch-psychotherapeutischen und neurologischen Bereich die Durchführung eines Referenzprojekts in diesem Zusammenhang an. Diesem Wunsch kam der LfD gerne nach. Bis zum Frühjahr 2012 wollen die Projektbeteiligten gemeinsam den Umsetzungsstand und die Realisierbarkeit der in der Orientierungshilfe verankerten Anforderungen an die datenschutzgerechte Ausgestaltung und den Betrieb von KIS überprüfen. Dazu wurden die in der Orientierungshilfe enthaltenen Inhalte in einzelne Arbeitspakete aufgeteilt und sukzessive mit den zur Zeit in den einzelnen Einrichtungen des Trägers eingesetzten Systemen verglichen. Untersucht werden sollen u.a. die Praxistauglichkeit einzelner Anforderungen aus der Orientierungshilfe sowie die Vereinbarkeit zwischen optimaler Behandlungsqualität und angemessenem Datenschutzniveau im Krankenhaus. An den Gesprächen sind neben den IT-Abteilungen auch die Datenschutzbeauftragten der betroffenen Einrichtungen beteiligt. Eine zwischen dem LfD und der Krankenhausgesellschaft Rheinland-Pfalz eingerichtete Arbeitsgruppe wird das Projekt aufgrund dessen landesweiter Bedeutung begleiten.

Schließlich hat der LfD im November 2011 bei den seiner Zuständigkeit unterliegenden Krankenhäusern eine Befragung zum aktuellen Einsatz von KIS gestartet. Bis zum Jahresende 2011 sind die Häuser aufgefordert, dem LfD u.a. Angaben zu den von ihnen eingesetzten Produkten und den zugrunde liegenden technisch-organisatorischen Maßnahmen wie z.B. konkreter Zugriffs- und Berechtigungskonzepte oder geeigneter Instrumente zur Archivierung, Löschung und Protokollierung mitzuteilen. Von dem Ergebnis der Ist-Analyse verspricht sich der LfD neben Informationen zum Verbreitungsgrad bestimmter IT-Produkte in den rheinland-pfälzischen Einrichtungen insbesondere Anhaltspunkte für ein möglicherweise bestehendes übergreifendes Verbesserungspotential einzelner Verfahren sowie verwertbare Erkenntnisse für die im Jahre 2012 geplante Fortschreibung der Orientierungshilfe.

Mit der Orientierungshilfe Krankenhausinformationssysteme ist das Thema „Datenschutz im Krankenhaus“ wieder in die öffentliche Diskussion gerückt. Auch wenn es dabei zu durchaus unterschiedlichen inhaltlichen Bewertungen der in dem Papier formulierten Anforderungen kam, waren sich doch in einer Hinsicht alle Kommentatoren einig: endlich befassen sich Betreiber und Hersteller von Krankenhausinformationssystemen gleichzeitig und gemeinsam mit der datenschutzgerechten Ausgestaltung der im Krankenhaus genutzten IT, ohne bei möglicherweise vorliegenden Defiziten auf die Versäumnisse des anderen hinzuweisen. Es bleibt zu hoffen, dass die mit der Veröffentlichung der Orientierungshilfe erzeugte Dynamik auch bei der weiteren Umsetzung des dahinter stehenden Anliegens in der Praxis zu konstruktiven und nachhaltigen Lösungen führt.

## 3.7 Im Fokus: rheinland-pfälzische Unternehmen

Die betrieblichen Datenschutzbeauftragten sind das Rückgrat des Datenschutzes in der Privatwirtschaft. Mit ihrer Qualität und ihrem Engagement steht und fällt der Datenschutz in den Betrieben. Deshalb hat der LfD, der seit drei Jahren auch Datenschutzaufsichtsbehörde für ca. 200.000 rheinland-pfälzische Unternehmen ist, nach dem Vorbild anderer Länder bei insgesamt 1.500 größeren Unternehmen in Rheinland-Pfalz seit Mai 2011 eine Umfrage durchgeführt. Diese waren mit der Bitte angeschrieben worden, Auskünfte über ihre betrieblichen Datenschutzbeauftragten, deren Qualifikation und Aufgabenwahrnehmung zu geben.

Mehr als 93 Prozent der befragten Unternehmen meldeten ihren „Datenschutzstatus“ an den LfD zurück, was als beeindruckendes Zeichen der Kooperationsbereitschaft zu werten ist und sicherlich auch durch die gute Unterstützung der Umfrageaktion durch rheinland-pfälzische Industrie- und Handelskammern möglich wurde. Die größeren rheinland-pfälzischen Unternehmen kommen danach ihrer Pflicht zur Bestellung betrieblicher Datenschutzbeauftragter in hohem Umfang nach. Allerdings brauchen diese teilweise noch mehr Unterstützung und Fortbildung und auch ein größeres Zeitbudget, um ihre verantwortungsvolle Aufgabe zu erfüllen.

Die einzelnen Ergebnisse der Umfrage (nachzulesen unter http://www.datenschutz.rlp.de/de/aktuell/2011/images/PE_LfD_betrDSB_Presse.pdf) sind zum Teil ermutigend, zum Teil Anlass, die bisherigen Bemühungen um einen besseren Datenschutz und eine größere Datensicherheit noch weiter zu verstärken.

92 Prozent der Unternehmen haben dem Gesetz entsprechend betriebliche Datenschutzbeauftragte bestellt, allerdings stammen mehr als 12 Prozent aus Betriebsbereichen, bei denen Interessenkonflikte mit den Aufgaben der Datenschutzbeauftragten vorprogrammiert sind. Dies gilt etwa für Mitglieder der Geschäftsführung oder Leiterinnen und Leiter der IT-Abteilung. Niemand kann sich selbst kontrollieren und beraten, Datenschutzbeauftragte müssen daher unabhängig sein. Nachholbedarf gibt es auch bei der Aus- und regelmäßigen Fortbildung der Datenschutzbeauftragten, zudem wird ihnen im Betrieb häufig nur ein sehr schmales Zeitbudget in Sachen Datenschutz zugestanden. Das wird der gewachsenen Bedeutung und der Vielfalt der Datenschutzthemen – vom Arbeitnehmerdatenschutz bis Facebook, von Kundendatenbanken bis zur Videoüberwachung – nicht mehr gerecht.

Ein schöner „Nebeneffekt“ der Umfrage: Allein durch die Kontaktaufnahme mit den Unternehmen wurden zwischenzeitlich mehr als 120 neue betriebliche Datenschutzbeauftragte bestellt. Verblüffend ist allerdings, dass die Unternehmen keinen Unterstützungsbedarf durch den LfD in Fragen der Datensicherheit sehen. Obwohl 2011 als das „Jahr der Hacker“ in die Geschichte eingehen wird, obwohl selbst Weltkonzerne wie Sony oder staatliche Behörden wie der deutsche Zoll vor Angriffen aus dem Netz nicht gefeit sind, geben 97,5 Prozent der befragten Unternehmen an, keinen Beratungsbedarf zu haben. Entweder haben die Betriebe die Befürchtung, bei einer Beratung durch den LfD kontrolliert zu werden, oder sie unterschätzen die Datensicherheitsprobleme.

Ziel des LfD wird es sein, die Verantwortlichen in den Betrieben weiter zu sensibilisieren und die Zusammenarbeit mit den betrieblichen Datenschutzbeauftragten auch beim Thema Datensicherheit zu verstärken. Dafür ist auch die Unterstützung der Kammern und der Unternehmerverbände wichtig.

## 3.8 Vernetzter Datenschutz

Mit der wachsenden Bedeutung des Datenschutzes als Querschnittmaterie nimmt auch die Zahl seiner „Akteure“ weiter zu. Um das Datenschutzniveau bemühen sich nicht nur staatliche Stellen wie die Parlamente oder die Datenschutzbeauftragten, auch gesellschaftliche Einrichtungen wie die Berufsverbände der Datenschutzbeauftragten (BvD), der Chaos Computer Club oder der AK Vorratsdatenspeicherung wirken an der Entwicklung des Datenschutzes in Deutschland intensiv mit. Gar nicht zu überschätzen ist schließlich die Rolle der betrieblichen und behördlichen Datenschutzbeauftragten, die vor Ort in den Unternehmen und Verwaltungsstellen das tatsächliche Niveau des Datenschutzes wesentlich bestimmen. Teilweise betreten sogar „ungebetene Akteure“ wie die Stiftung Datenschutz das Feld (vgl. Tz. I-2.2); damit droht eine ohnehin schon schwer überschaubare Lage noch unübersichtlicher zu werden.

Deshalb besteht eine ganz wesentliche Aufgabe des LfD darin, für eine Koordinierung und Vernetzung der unterschiedlichen Akteurinnen und Akteure in Rheinland-Pfalz und darüber hinaus Sorge zu tragen. Der Landtag hat durch eine entsprechende Erweiterung der Aufgabenbeschreibung des LfD reagiert, seit dem März 2011 ist er auch damit beauftragt, mit den für die Überwachung des Datenschutzes in nicht-öffentlichen Stellen zuständigen betrieblichen Datenschutzbeauftragten Verbindungen aufzubauen und zu halten sowie auf die Verwirklichung des Datenschutzes nach einheitlichen Grundsätzen hinzuwirken (§ 24 Abs. 7 LDSG; vgl. Tz. I-2.3.1).

Die Aufgabe der Vernetzung der Datenschutzakteurinnen und -akteure nimmt der LfD bereits seit Jahren sehr ernst, effektiver Datenschutz ist nur vernetzt möglich. So koordiniert sich der LfD mit den Kolleginnen und Kollegen aus Bund und Ländern in der zweimal im Jahr tagenden Datenschutzkonferenz, für den nicht-öffentlichen Bereich fand die Koordinierung bislang im sog. Düsseldorfer Kreis statt. Um den Abstimmungsaufwand für die beteiligten Landesdatenschutzbeauftragten in Grenzen zu halten, wurde im Herbst 2011 beschlossen, dass der Düsseldorfer Kreis zukünftig als unterstützendes Gremium der Datenschutzkonferenz zuarbeitet. Besonders eng arbeitet der LfD seit Jahren mit seinem hessischen Kollegen zusammen, diese Kooperation soll in den nächsten Jahren noch erheblich verstärkt werden. Das Bemühen um einen zukunftsweisenden europäischen Rechtsrahmen für den Datenschutz ist nur eines von zahlreichen gemeinsamen Tätigkeitsfeldern.

Die mit den behördlichen Datenschutzbeauftragten traditionell durchgeführten Tagungen und Veranstaltungen (vgl. 22. Tb., Tz. 3.4.2) wurden auch im Berichtszeitraum in Kooperation mit den Ministerien, den kommunalen Spitzenverbänden und Kommunen sowie den Hochschulen erfolgreich fortgeführt. Die jährliche Tagung der kommunalen Datenschutzbeauftragten fand bereits zum fünften Mal seit dem ersten Treffen im Jahr 2007 statt, sie

hat sich etabliert. Insbesondere die Vernetzung mit den 1.500 schulischen Datenschutzbeauftragten sowie den über 200 kommunalen Datenschutzbeauftragten trägt Früchte.

Zur weiteren Förderung der Kommunikation wurde ein Online-Forum beim LfD eingerichtet. Innerhalb geschlossener Nutzergruppen können die Mitglieder gemeinsam und mit den Mitarbeiterinnen und Mitarbeitern des LfD in der Praxis auftretende Fragestellungen fachlich diskutieren sowie Erfahrungen und Unterlagen austauschen. Bislang nutzen rund 300 Personen das Forum.

Die guten Kontakte zu den betrieblichen Datenschutzbeauftragten in den rheinland-pfälzischen Unternehmen (vgl. 22. Tb., Tz. 3.4.3) wurden weiter ausgebaut und verstärkt. Neben dem intensiven Austausch mit den betrieblichen Datenschutzbeauftragten großer rheinland-pfälzischer Unternehmen kommen dabei die mittleren und kleinen Betriebe keineswegs zu kurz, hier unterstützt der LfD die sog. Erfahrungsaustauschkreise der betrieblichen Datenschutzbeauftragten mit Rat und Tat.

## 3.9 Information und Beratung

### 3.9.1 Aktivitäten des LfD

Die Digitalisierung des Alltags und die damit verbundene Registrierung und Kommerzialisierung unserer Alltagsaktivitäten stellt die betroffenen Bürgerinnen und Bürger vor besondere Herausforderungen, zumal sie längst nicht mehr nur Objekte der Datenverarbeitung sind, sondern durch ihr Tun und Unterlassen zahllose Daten von sich preisgeben und zwar nicht nur im Internet. Daraus ergibt sich – was alle Untersuchungen bestätigen – ein großer Informations- und Beratungsbedarf der Bürgerinnen und Bürger, dem der Landesgesetzgeber in seiner Novellierung des Landesdatenschutzgesetzes auch ausdrücklich Rechnung getragen hat. In dem bereits wiederholt zitierten § 29 Abs. 8 LDSG wird der LfD ausdrücklich dazu verpflichtet, die Bürgerinnen und Bürger zu informieren und zu beraten.

Der LfD ist dieser Aufgabe auf vielfältige Weise nachgekommen. Dazu gehört v.a. die Information der Öffentlichkeit im Wege von Presseerklärungen und Pressekonferenzen. Im Berichtszeitraum wurde in über 100 Presseerklärungen über alle wesentlichen Datenschutzvorgänge im Lande, im Bund und auf europäischer Ebene informiert. Hinzu kommen eine Vielzahl von öffentlichen Veranstaltungen, sei es aus Anlass des Europäischen Datenschutztages, des Safer Internet Day oder aus anderen Anlässen. Die Besucherzahlen belegen das große Interesse, das dem Datenschutz mittlerweile entgegengebracht wird. 200 bis 300 Teilnehmerinnen und Teilnehmer waren nicht die Ausnahme, sondern die Regel. Informationsmaterialien, die zum Teil in Kooperation mit dem Bildungs- und dem Verbraucherschutzministerium erstellt wurden, ergänzen die Informationsanstrengungen des LfD.

Ebenso wichtig wie die öffentlichen Informationen war und ist aber auch die persönliche Beratung, die im Berichtszeitraum von Hunderten von Bürgerinnen und Bürgern nachgefragt worden war, wobei es immer wieder um die Frage ging, wie man sich im Internet richtig verhält und was man dort tunlichst unterlassen soll. In aller Regel gingen die Beratungs- und Informationswünsche von Erwachsenen aus. Die entsprechende Erziehung und Bildung von Kindern und Jugendlichen war ein eigener Arbeitsschwerpunkt des LfD. Die entsprechende Zusammenfassung findet sich unter Tz. I-4.

### 3.9.2 Informationen zur „Verhaltenskontrolle 2.0“

Das Spektrum notwendiger Informationen ist breit. Immer häufiger wird die Frage gestellt, wer die Datenspuren im Internet lesen kann, was sie verraten und wie man sie vermeidet. Dazu seien auch an dieser Stelle ein paar Informationen zusammengefasst:

Um welche Datenspuren geht es dabei? Zunächst um die Internetprotokoll-, kurz IP-Adresse. Sie wird bei jedem Klick mitgeschickt und verrät einiges über die Nutzerinnen und Nutzer. Oft lässt sie sich ziemlich genau dem Wohnort zuordnen oder jedenfalls der Region, aus der man kommt. In Verbindung mit den Angaben, die der Browser mitschickt, ist erkennbar, woher die Nutzerinnen und Nutzer kommen. Falls sie schon einmal gefragt haben, warum ihnen in der Regel deutsche Werbung präsentiert wird und keine Anzeigen auf Französisch oder Spanisch – hier liegt die Antwort!

IP-Adressen werden benötigt, um die Datenpakete im Internet zuzustellen. Sie werden den Nutzerinnen und Nutzern von ihrem jeweiligen Internetprovider zugewiesen und stellen nach Auffassung der Datenschutzbeauftragten ein grundsätzlich personenbeziehbares Datum dar. Dies deshalb, weil nicht nur der Provider in der Lage ist, die IP-Adresse einer Nutzerin bzw. einem Nutzer zuzuordnen, sondern auch alle Anbiererinnen und Anbieter einer Website, auf der sich Nutzerinnen bzw. Nutzer registrieren oder anmelden oder wo sie Namen oder Adressen hinterlassen. Zwar wird der Personenbezug in vielen Fällen durch eine dynamische, d.h. wechselnde Vergabe von IP-Adressen relativiert, mit Vergabe der künftigen

IPv6-Adressen entfällt jedoch diese technische Notwendigkeit und ein einmal hergestellter Personenbezug kann dauerhaft bestehen bleiben (vgl. Tz. II-1.5).

Über sog. Proxy-Server können sich Nutzerinnen und Nutzer hinter einer anderen IP-Adresse sozusagen verstecken. Anstelle ihrer IP-Adresse wird für den Aufruf der gewünschten Internetseite die Adresse des Proxy-Servers verwendet. Manche Suchmaschinen bieten bereits eine eingebaute Proxy-Funktionalität (vgl. Kasten „Datenspuren vermeiden“).

IP-Geolokalisierung: http://www.utrace.de/

Browser ist im Übrigen nicht gleich Browser, so wie meist kein Wagen dem andern gleicht. Die auf deutschen Straßen zugelassenen Fahrzeuge des Typs VW Golf unterscheiden sich in Baujahr, Farbe, Ausstattung, Aufklebern, Schrammen oder Roststellen. Bei den Browsern sind dies Version, Konfiguration, Sprach-einstellung oder Bildschirmauflösung. Viele haben dadurch einen digitalen Fingerabdruck, anhand dessen sie im Internet wiedererkannt werden können. Der Browser verrät zudem über den sog. „Referrer“ jeder besuchten Seite, auf welcher Internetseite Nutzerinnen und Nutzer zuvor gewesen sind.

Browser-Fingerabdruck: http://panopticlick.eff.org/

Jedes Mal, wenn eine Internetseite aufgerufen wird, erzeugt dies eine Datenspur. Ob man in Google, Bing oder Yahoo etwas sucht, sich ein Video ansieht oder einen Blog liest – meist wird dies protokolliert. Zwar ist daraus nicht direkt erkennbar, welche Person dahinter steht, dies kann sich jedoch schnell ändern. Im Jahr 2006 stellte der Dienst America Online (AOL) 20 Millionen Anfragen ins Internet, die von 650.000 Nutzerinnen und Nutzern an seine Suchmaschine gestellt wurden. Nach kurzer Zeit hatte die „New York Times“ darin Thelma Arnold aus Lilburn, Texas, ausfindig gemacht, die sich u.a. über die Krankheiten ihrer Bekannten im Internet informierte und über Möglichkeiten, der Inkontinenz ihres Hundes auf dem Sofa Herr zu werden. Thelma Arnolds voller Name war nicht in den Daten enthalten, aber über ihre IP-Adresse, Suchbegriffe und -gewohnheiten konnte sie von der „New York Times“ binnen weniger Tage identifiziert werden (vgl. http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all).

AOL Suchanfragen-Datenbank: http://www.aolstalker.com/

Was Suchmaschinen und Diensteanbieter alles über ihre Nutzerinnen und Nutzer wissen, lässt sich am Beispiel von Google über dessen Dienst „Dashboard“ erkennen. Für alle Nutzerinnen und Nutzer, die sich bei Google für einen der zahlreichen Dienste registrieren (z.B. Google Mail, Calendar, Groups, Blogger, Text & Tabellen, Picasa, oder YouTube) zeigt das Dashboard, wonach über Google gesucht wurde, welche Orte oder Routen auf Google Maps von Interesse waren, wie sich die Internetaktivitäten monatlich, wöchentlich oder täglich verteilen und vieles mehr. Google als „der Konzern, der mehr über Sie weiß als Sie selbst“, wie „Der Spiegel“ im Januar 2010 titelte.

Ähnliches gilt für Facebook. Wie umfangreich der Datenbestand von Facebook ist, hat sich über den von einem österreichischen Studenten geltend gemachten Auskunftsanspruch ergeben (vgl. Tz. I-3.2.1). Auf dessen Internetseite http://www.europe-v-facebook.org/ ist erkennbar, was Facebook über die Profildaten und die sonstigen, von Nutzerinnen und Nutzern direkt bereit gestellten Daten hinaus speichert. Es handelt sich dabei um Angaben über deren Aufenthaltsorte und Aktivitäten, ihre abgelehnten und angenommenen Freundschaftsanfragen sowie entfernte Freunde, genutzte Anwendungen, alle im Internet jemals „geliketen“ Seiten oder Beiträge, Einladungen, Teilnahmen und Absagen zu Events, verschickte Nachrichten, auch wenn diese gelöscht wurden, Chats, Benachrichtigungen, Markierungen in Fotos, auch wenn diese nachträglich entfernt wurden, die GPS-Koordinaten und Zeitpunkte vorhandener Fotos, Logindaten, -zeitpunkte und -geräte und anderes mehr.

Google Dashboard: http://www.google.com/dashboard/
Facebook-Datenbestand: http://www.europe-v-facebook.org/DE/Datenbestand/datenbestand.html

Verräterisch sind insbesondere auch „Cookies“, kleine Dateien, die von den besuchten Websites auf dem Nutzerrechner abgelegt und beim nächsten Besuch ausgelesen werden. Häufig werden Cookies dabei nicht allein von der konkret aufgerufenen Website gesetzt, sondern über dort eingebundene Werbung auch von Werbevermarktern wie z.B. Doubleclick. Beim Besuch einer weiteren Seite, die mit Werbung beschickt wird, kann über diese „Drittanbieter-Cookies“ erkannt werden, auf welchen Seiten die Nutzerinnen und Nutzer zuvor waren. Wenn man die Cookies zusammen nimmt, ergibt sich ein recht gutes Bild über deren Interessen. Zwar lassen sich die Cookies im Browser löschen und es lässt sich festlegen, ob überhaupt Cookies und ggf. auf welchen Seiten akzeptiert werden sollen. Allerdings gilt dies nur für normale Cookies; sog. Flash-Cookies, die auch deutlich mehr an Informationen aufnehmen können, können auf diesem Weg nicht beeinflusst werden. Möglich ist jedoch, diese auf dem Umweg über eine Konfigurationsseite im Internet zu löschen (vgl. Kasten „Datenspuren vermeiden“).

Ähnlich ist es mit der Chronik bzw. der Verlaufsanzeige des Browsers. Wer darauf geachtet hat, dem ist möglicherweise aufgefallen, dass auf Websites benutzte Links die Farbe wechseln können, und dass dies so geblieben ist, wenn die Website nach einiger Zeit erneut besucht wird. Die Information, was die Nutzerinnen und Nutzer sich bei ihrem letzten Besuch angesehen haben, wurde offenkundig gespeichert, konkret: in der Browser-Chronik. Diese Information kann aber von allen Seiten, die besucht werden, ausgewertet werden. Je länger eine Browser-Chronik zurückreicht, desto mehr verrät sie über die Nutzungsgewohnheiten der Surferinnen und Surfer.

Test Browserchronik:
http://www.zendas.de/service/browserdaten/css_hack.html
http://www.whattheinternetknowsaboutyou.com/

Auch viele Smartphones sind neugierig, bzw. die Apps, die auf ihnen laufen. Nach einer Untersuchung der Technischen Universität Wien greift ein Drittel dieser Programme auf die Standortdaten der Nutzerinnen und Nutzer zu, viele auch auf das Adressbuch oder die Kontaktliste; in vielen Fällen, ohne die Nutzerinnen und Nutzer vorher ausreichend zu informieren oder danach zu fragen. Selbstverständlich muss eine Navigationsanwendung oder solche, die Kinos, Apotheken, Briefkästen oder Restaurants in der Umgebung anzeigen, wissen, wo sich die Nutzerinnen und Nutzer befinden. Aber braucht ein Spiel diese Information? Und wozu braucht es ungefragt die Einträge aus dem Adressbuch? – Eine ganze Menge an Informationen also, und wie das obige Beispiel von Thelma Arnold zeigt, können sie in der Zusammenschau häufig einer bestimmten Person zugeordnet werden.

Wenn man das so nicht möchte, was kann man tun? Vieles hat man selbst in der Hand, insbesondere das, was man in sozialen Netzwerken usw. über sich preisgibt. Wie man dort sich und andere schützen kann, was es zu beachten gilt und an wen man sich wenden kann, wenn man Unterstützung braucht, erfährt man auf den Seiten des LfD unter http://www.datenschutz.rlp.de/de/jugend.php.

Steuern kann man auch, ob, wann und wer erfährt, wo man sich gerade befindet. Schließlich muss die GPS- oder WLAN-Funktion des Smartphones ja nicht dauerhaft aktiv sein, und wenn sie abgeschaltet sind, kann auch keine Applikation ungefragt auf Standortdaten zugreifen.

Auch für Cookies und die Chronik des Browsers kann man selbst festlegen, ob man diese will oder nicht oder dass diese Daten von Zeit zu Zeit gelöscht werden. Die meisten Browser bieten einen „Privatmodus“ an, der dafür sorgt, dass solche Datenspuren vermieden werden. Bei anderen Punkten ist die Sache nicht so einfach, weil manches technisch bedingt ist. Aber auch hier lassen sich Datenspuren zumindest reduzieren. So gibt es datenschutzfreundliche Suchmaschinen, die die IP-Adressen der Nutzerinnen und Nutzer anonymisieren oder gar nicht erst speichern. Wenn man diese Dinge berücksichtigt, dann erfährt am Ende niemand, dass eigentlich ein Hund vor dem Rechner sitzt.

Datenspuren vermeiden
Cookies:
http://wiki.jappy.de/wiki/Tutorial:Cookies#Problembehebung

Flash-Cookies:
http://www.macromedia.com/support/documentation/de/flashplayer/help/settings_manager09.html

Datenschutzfreundliche Suchmaschinen (incl. Proxy)
http://www.ixquick.de/
http://www.startpage.com/

Anonym Surfen:
http://www.torproject.org/

Präsentationen zum Thema:
- „Datenspuren im Internet – und wie man sie vermeiden kann“
- „Verhaltensforschung 2.0 – Was Online-Werber über uns wissen wollen“
- „Tracking Tools – Möglichkeiten und Grenzen“

abrufbar im Internetangebot des LfD unter
http://www.datenschutz.rlp.de/de/service.php?submenu=downloads

# 4. Datenschutz als Bildungs- und Erziehungsaufgabe

Durch die millionenfache Nutzung von Google, Facebook und Co. hinterlassen die Menschen eine riesige Menge an Daten und Datenspuren. Zum Teil geschieht dies bewusst, zum Teil unbewusst. Aber selbst wenn es bewusst geschieht, wissen die meisten Nutzerinnen und Nutzer oft nicht, was mit ihren Daten unternommen wird. Es besteht deshalb ein großes Informationsdefizit. Dies zeigen alle einschlägigen Untersuchungen. Notwendig ist deshalb eine breite Wissensvermittlung. Dazu gehört auch die Vermittlung von Handlungsalternativen. Insoweit ist der Datenschutz eine Bildungs- und Erziehungsaufgabe. Darauf hat der LfD bereits in seinem letzten Tätigkeitsbericht hingewiesen (vgl. 22. Tb., Tz. 3.1). Seinerzeit waren die entsprechenden Aufgabenbeschreibungen aber weniger eine Zustandsumschreibung als eine politische Forderung. Heute ist diese Forderung allseits akzeptiert und auf dem Weg umgesetzt zu werden.

## 4.1 Politischer Konsens

Die 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im September 2011 auf Betreiben des LfD eine Entschließung „Datenschutz als Bindungsaufgabe“ verabschiedet. Darin heißt es:

„Um dieser Entwicklung entgegenzuwirken, muss der Datenschutz auch als Bildungsaufgabe verstanden und praktiziert werden. Es genügt nicht, allein auf rechtliche Regelungen sowie auf datenschutzfreundliche technische Voreinstellungen und Anwendungen zu setzen. Die digitale Aufklärung ist unverzichtbar als Teil einer Datenschutzkultur des 21. Jahrhunderts. Sie beinhaltet zum einen die Vermittlung von Wissen und zum anderen die Entwicklung eines wachen, wertebezogenen Datenschutzbewusstseins. So wie Bildung eine gesamtgesellschaftliche Aufgabe ist, so ist auch die Bildung im Hinblick auf die Datenschutzfragen unserer Zeit eine Aufgabe, die nicht nur dem Staat, sondern ebenso der Wirtschaft und der Zivilgesellschaft wie auch den Eltern im Verhältnis zu ihren Kindern obliegt.
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt deshalb und unterstützt vielfältige Überlegungen und Aktivitäten, die sich stärker als bisher um eine größere Datenschutzkompetenz der Internetnutzenden bemühen.
Die Datenschutzkonferenz hält die bisherigen Bemühungen allerdings noch nicht für ausreichend. Will man die Internetnutzer dazu befähigen, Vorteile und Gefahren von Internetangeboten abzuwägen und selbstverantwortlich zu entscheiden, in welchem Umfange sie am digitalen Leben teilhaben wollen, sind weitergehende und nachhaltige Anstrengungen notwendig. V.a. ist sicherzustellen, dass

1. dabei viel intensiver als bisher die Möglichkeiten des Selbstdatenschutzes, der verantwortungsvolle Umgang mit den Daten anderer und die individuellen und gesellschaftlichen Auswirkungen einer leichtfertigen Nutzung des Internets thematisiert werden,
2. sich die schulischen und außerschulischen Programme und Projekte zur Förderung von Medienkompetenz nicht auf Fragen des Jugendmedienschutzes und des Urheberrechts beschränken, sondern den Datenschutz als wesentlichen Bestandteil mit einbeziehen,
3. Medien- und Datenschutzkompetenz entweder in einem eigenständigen Schulfach oder in einem Fächerspektrum mit Leitfächern verpflichtend zu verankern ist,
4. die Vermittlung von Datenschutz als integraler Bestandteil von Medienkompetenz ausdrücklich in den Bildungsstandards und Lehrplänen verankert wird und dass die entsprechenden Anforderungen bewertungs- bzw. prüfungsrelevant ausgestaltet werden und
5. Medien- und Datenschutzkompetenz und insbesondere die digitale Aufklärung zum verbindlichen Gegenstand der Lehrerausbildung gemacht werden.

Digitale Aufklärung und Erziehung zum Datenschutz bestimmen letztlich auch über den Stellenwert, den Privatsphäre und Persönlichkeitsrecht und damit Menschenwürde und Demokratie künftig in der internetgeprägten Gesellschaft insgesamt haben werden.“

Auch eine Reihe von Landesparlamenten hat sich diesen Forderungen im Grundsatz angeschlossen. Zu ihnen zählt v.a. der rheinland-pfälzische Landtag, der in einer gemeinsamen Entschließung aller Fraktionen den Datenschutz ebenfalls als Bildungs- und Erziehungsauftrag umschrieben hat (vgl. LT-Drs. 15/5417). In dieser Entschließung heißt es:

„Zuweilen geben Nutzer ihre Daten freiwillig preis, oft auch unbewusst. Häufig wissen sie nicht, was mit den Daten geschieht, die sie im Netz oder in der realen Welt hinterlassen. Diese Entwicklung geht mit einer Kommerzialisierung der Privatsphäre einher und führt zu einer massiven Grenzverschiebung zwischen Privatheit und Öffentlichkeit. Dies hat erhebliche Konsequenzen für den Einzelnen und die Gesellschaft insgesamt. Diese Konsequenzen werden in der Zukunft noch gravierender sein, wenn das ‚Internet der Dinge' und die RFID-Technologie noch tiefere Eingriffe in unsere Privatsphäre ermöglichen werden. Vor diesem Hintergrund werden Verbraucherschutz, Jugendmedienschutz und Datenschutz immer wichtiger. Deshalb müssen auch die Medienkompetenz und das Datenschutzbewusstsein der Bürger jeden Alters verbessert werden. Weder das eine, noch das andere kann verordnet werden. Beides muss erlernt werden.“

Auch die Enquete-Kommission „Verantwortung in der medialen Welt“ hat dieses Thema aufgegriffen. In ihrem Abschlussbericht (vgl. LT-Drs. 15/5300) hat sie Folgendes festgestellt:

„Die intensive Nutzung sozialer Netzwerke wie SchülerVZ, WKW und Facebook sowie weiterer Internetdienste wirft zunehmend grundlegende Fragen des Schutzes persönlicher Daten und damit des Grundrechts auf informationelle Selbstbestimmung auf. Dabei geht es um die Risiken und Gefahren, die sich aus der Nutzung des Internets für das Datenschutzgrundrecht ergeben. Diese Risiken hängen v.a. mit den Datenspuren zusammen, die jeder im Netz hinterlässt und die von Dritten – legal und illegal – genutzt werden können, und zwar auf unbegrenzte Zeit. Darüber sind Schülerinnen und Schüler zu informieren und aufzuklären. Ihnen muss außerdem vermittelt werden, welche Möglichkeiten sie haben, um diesen Gefahren selbst begegnen zu können. Dabei geht es im Wesentlichen um den sogenannten Selbstdatenschutz, der auf vielfältige Weise realisiert werden kann. Im Internetangebot des LfD, das spezielle Informationen für Schulen und Jugendliche vorhält, sind die wichtigsten Hilfen genannt, mit denen man die eigene Privatsphäre schützen kann.“

Hervorzuheben ist außerdem, dass sich auch die Kultusministerkonferenz auf Anregung des LfD mit dem Thema „Medienbildung in der Schule“ befasst und auf Vorschlag des LfD dabei auch den Datenschutz thematisieren wird. In dem zur Beschlussfassung vorliegenden Entwurf heißt es:

„Medienbildung befähigt zur Datensparsamkeit und zur Vermeidung von Datenspuren und fördert die digitale Sicherheit der persönlichen Kommunikation. Insoweit trägt Medienbildung auch zur eigenverantwortlichen informationellen Selbstbestimmung und zum persönlichen Datenschutz bei.“

und

„Durch die hohe Verfügbarkeit von digitalen Medien und deren zunehmende Interaktivität stehen die Schulen auch vor neuen rechtlichen Herausforderungen: V.a. auf den Gebieten Datenschutz, Jugendschutz und Persönlichkeitsrecht, Urheber- und Lizenzrecht müssen Schülerinnen und Schüler, Lehrkräfte, Schulleitungen und Eltern sensibilisiert und unterstützt werden. Hierzu eignen sich etwa schulische Multiplikatorennetzwerke. Eine Zusammenarbeit mit anderen staatlichen Einrichtungen, zum Beispiel den Landesbeauftragten für Datenschutz oder den Beauftragten für Kriminalprävention, kann hierbei hilfreich sein.“

## 4.2 Kooperation mit dem Bildungsministerium

Soweit es um die schulische Erziehung zum Datenschutz geht, lassen sich die notwendigen Maßnahmen nur in enger Zusammenarbeit mit dem zuständigen Ministerium realisieren. Die Kooperation zwischen LfD und dem Bildungsministerium ist in Rheinland-Pfalz mittlerweile selbstverständlich geworden. Sie findet auf vielen Gebieten statt. In Kooperation mit dem LfD wurde für die Schulen eine Richtlinie zur Verbraucherbildung erarbeitet. Zu den dort thematisierten Kernkompetenzen gehört auch der Datenschutz. Insoweit heißt es:

„Aufgrund der technologischen, jugend-, arbeitsmarkt-, gesellschafts- und bildungspolitischen Veränderungen kommt der Förderung von Medien-, Informations-, Kommunikations- und Datenschutzkompetenz eine entscheidende Bedeutung zu. In diesem Zusammenhang spielen das Recht auf informationelle Selbstbestimmung, die Verantwortung im Umgang mit persönlichen Daten und die Fähigkeit, verschiedene Formen kommerzieller Inhalte und Kommunikation kritisch zu bewerten und zu analysieren, eine entscheidende Rolle. Das Medienverhalten von Kindern und Jugendlichen zeichnet sich zwar durch technische bzw. Handhabungskompetenzen aus. Ihre Fähigkeit und/oder Motivation, das eigene Medienhandeln und Medieninhalte kritisch zu hinterfragen, ist hingegen oftmals weniger stark ausgeprägt. Deshalb sind sie sich vielfach nicht bewusst, welche Datenspuren sie bei ihren alltäglichen Aktivitäten hinterlassen und welche Konsequenzen diese digitalen Spuren haben können. Kinder und Jugendliche sind deshalb über den Wert ihrer Privatsphäre und über die Gefahren aufzuklären, die ihrer Privatsphäre v.a. durch bestimmte Internetdienste und ihr digitales Verhalten drohen. Notwendig ist es auch, sie über ihre Rechte und die Möglichkeiten des Selbstdatenschutzes zu informieren. Nur wenn ihnen diese Rechte und Möglichkeiten bewusst sind, werden sie in der Lage sein, die Kontrolle über ihre eigenen Daten zu behalten. Wichtiger als jede technische Lösung bleibt dabei die nachhaltige Verankerung der Grundsätze Datenvermeidung und Datensparsamkeit. Kindern und Jugendlichen muss außerdem vermittelt werden, dass es auch bei der Nutzung des Internets Verpflichtungen gibt, etwa gegenüber anderen Personen und deren persönlichen Daten, und dass auch ihr eigenes Online-Verhalten ethischen Ansprüchen genügen muss.“ (http://verbraucherbildung.bildung-rp.de/fileadmin/user_upload/verbraucherbildung.bildung-rp.de/Materialien/Richtlinie_VB.pdf)

Gemeinsam sollen auch die Lehrpläne daraufhin überprüft werden, ob der Datenschutz darin hinreichend thematisiert ist und wo ggf. Überarbeitungen notwendig sind.

In einer Arbeitsgruppe, die sich mit dem von der Enquete-Kommission „Verantwortung in der digitalen Welt“ verlangten und von den Koalitionspartnern vereinbarten sog. Medienkompass befasst, ist auch der LfD vertreten. Gleiches gilt für eine Steuerungsgruppe des Arbeitskreises „Medienkompetenz“.

Schließlich werden die vom LfD angebotenen Datenschutzworkshops vom Ministerium begleitet und mitfinanziert.

### 4.3 Schulische Veranstaltungen zum Datenschutz

Im Mittelpunkt der Datenschutzangebote, die den rheinland-pfälzischen Schulen vom LfD unterbreitet werden, stehen die Schülerworkshops „Datenschutz und Datenverantwortung“. Seit September 2010 bietet der LfD den weiterführenden Schulen im Lande diese Workshops an. Sie sind auf eine Dauer von zwei bis vier Unterrichtsstunden angelegt und richten sich an Schülerinnen und Schüler der Klassen sechs bis neun. Das Angebot ist für die Schulen kostenlos und wird aus eigenen Mitteln und mit Unterstützung des Ministeriums für Bildung, Wissenschaft, Weiterbildung und Kultur finanziert.

Standardmäßig werden in den Workshops folgende Inhalte vermittelt:

- Datenschutz als Bürgerrecht
- Fragen des Selbstdatenschutzes
- Bedeutung der Privatsphäre
- Online-Ethik und Datenverantwortung
- aktuelle datenschutzpolitische Themen (z.B. Google Street View, Datenschutz bei Facebook, Datendiebstahl bei Sony, etc.)

Thematische Schwerpunkte können von den Schulen mit den jeweiligen Referentinnen und Referenten nach den Bedürfnissen vor Ort abgestimmt werden.

Bislang wurden über 250 Workshops in knapp 100 Schulen durchgeführt. Ob Gymnasium, Realschule, Integrierte Gesamtschule, Hauptschule oder Schulen mit Förderschwerpunkten – die Referentinnen und Referenten des LfD haben Schulen in ganz Rheinland-Pfalz besucht. Die Reaktion auf dieses Angebot ist durchweg positiv. Viele Schulen bekunden nach der Durchführung des Workshops Interesse an Folgeveranstaltungen. Auf diesem Wege hat der LfD in weniger als einem Jahr mehr als 6.000 Schülerinnen und Schüler erreicht. Bis Mitte des kommenden Jahres wird der LfD sicherlich rund 10.000 Schülerinnen und Schüler über aktuelle Datenschutzfragen informiert und mit ihnen über den verantwortungsvollen Umgang mit den eigenen Daten und den rücksichtsvollen Umgang mit den Daten anderer diskutiert haben.

Dies geschieht mit Hilfe von sog. freien Mitarbeiterinnen und Mitarbeitern, die pädagogisch vorgebildet sind, von der Dienststelle des LfD in Datenschutzfragen besonders geschult werden und mit einschlägigen Unterrichtsmaterialien ausgestattet sind. Ein geschlossenes Forum im Internetangebot des LfD bietet diesen Mitarbeiterinnen und Mitarbeitern die Möglichkeit, Erfahrungen miteinander auszutauschen und dem LfD die Gelegenheit, den freien Mitarbeiterinnen und Mitarbeitern aktuelle Informationen über den Datenschutz zur Verfügung zu stellen.

Mit Beginn des neuen Jahres werden diese Mitarbeiterinnen und Mitarbeiter auch für Elternabende zur Verfügung stehen. Dafür werden sie wiederum besonders geschult und entlohnt. Die entsprechenden Haushaltsmittel werden vom Bildungsministerium gesondert zur Verfügung gestellt. Koordiniert und weiterentwickelt werden diese Aktivitäten von einem Medienpädagogen, der mit einer Zweidrittelstelle zur Dienststelle des LfD abgeordnet ist.

Aus dem vom LfD verliehenen Wissenschaftspreis (vgl. Tz. II-6.2.3) ist darüber hinaus eine Unterrichtseinheit zum Thema „RFID und Datenschutz“ hervorgegangen, bei der am Institut für Physik der Mainzer Universität Schülerinnen und Schüler entsprechender Leistungskurse in einer ganztägigen Schulveranstaltung Grundkenntnisse zur RFID-Technologie und ihren datenschutzrechtlichen Risiken vermittelt werden.

Die Datenschutzangebote des LfD ergänzen die entsprechenden Veranstaltungen der Schulen, die sich aber überwiegend eher mit Fragen des Jugendmedienschutzes befassen und den Datenschutz nur am Rande thematisieren, was sicherlich auch damit zusammenhängt, dass die Lehrkräfte bisher noch nicht einschlägig ausgebildet worden sind. Vergleichbares lässt sich wohl auch für andere Bundesländer feststellen. Deshalb sind eine Reihe der Datenschutzbeauftragten in den Ländern dabei, vergleichbare Angebote in ihrem Zuständigkeitsbereich zu entwickeln und anzubieten. Dabei besteht Einigkeit, dass die Datenschutzbeauftragten der Länder die Schulen als externe Spezialisten in Datenschutzfragen nur unterstützen können. Erziehung in Fragen der informationellen Selbstverantwortung und Selbstbestimmung ist und bleibt in erster Linie eine Aufgabe der Schulen selbst.

## 4.4 Kooperation des LfD mit IBM und dem Bundesverband der Datenschutzbeauftragten (BvD)

Medienbildung ist gerade mit Blick auf den Datenschutz eine gesamtgesellschaftliche Aufgabe, die nur im Zusammenwirken von Staat, Gesellschaft und Wirtschaft bewältigt werden kann. Der LfD hat deshalb im vergangenen Jahr mit IBM Deutschland und dem Berufsverband der Datenschutzbeauftragten (BvD) eine gemeinsame Initiative mit dem Ziel gestartet, jungen Menschen ein waches Datenschutzbewusstsein zu vermitteln. In dieser Inititative werden die Datenschutzworkshops des LfD mit dem Projekt des BvD „Datenschutz geht zur Schule“ verknüpft. Mitglieder des BvD sind im Rahmen dieses Projektes ebenfalls in den Schulen unterwegs und bieten dort Unterrichtseinheiten zum Datenschutz an. IBM-Mitarbeiterinnen und -Mitarbeiter und IBM-Pensionärinnen und -Pensionäre beteiligen sich aus Anlass des 100. Geburtstags von IBM ehrenamtlich an dieser Initiative. Dies bietet ihnen die Chance, ihre beruflichen Fähigkeiten und Kenntnisse im Umgang mit Daten, Internettechnologie und Sicherheitskonzepten für eine gesellschaftliche Aufgabe zu nutzen.

## 4.5 Unterrichts- und Informationsmaterialien

Der LfD hat darüber hinaus eine Reihe von Informationsmaterialien erstellt, die auch an Schulen Verwendung finden. Darunter befindet sich eine Broschüre über das richtige Verhalten in sozialen Netzwerken. Sie wurde in einer Auflage von 20.000 Exemplaren an rheinland-pfälzischen Schulen verteilt und auch von Schulen anderer Länder angefordert.

Ein weiteres Angebot an die Schulen und Bildungseinrichtungen des Landes ist die Möglichkeit, die Materialien, die rund um die Schülerworkshops erarbeitet wurden, in der jeweils aktuellen Fassung aus dem Internetangebot des LfD herunterzuladen (http://www.datenschutz.rlp.de/downloads/misc/Schuelerworkshops/Multiplikatorenworkshop.pdf).

Im Rahmen der EU-Initiative „klicksafe“ wurde dem Arbeitskreis Datenschutz und Bildung die Möglichkeit eingeräumt, an der Erstellung und Bearbeitung verschiedener Unterrichtsmodule mitzuarbeiten. Besonders dem Datenschutz und dem richtigen Umgang mit sozialen Netzwerken wurde dabei ein Hauptaugenmerk zuteil (https://www.klicksafe.de/cms/upload/user-data/pdf/klicksafe_Materialien/Zusatzmodul_LH__Datenschutz_klicksafe.pdf und https://www.klicksafe.de/cms/upload/user-data/pdf/klicksafe_Materialien/LH_Zusatzmodul_Social_Communities.pdf).

## 4.6 Lehrerfortbildung

Nach wie vor stehen die Mitarbeiterinnen und Mitarbeiter des LfD für Fortbildungsveranstaltungen im Bereich des Datenschutzes zur Verfügung. Abgesehen von Fortbildungen, die sich thematisch an behördliche und betriebliche Datenschutzbeauftragte richten, ging es schwerpunktmäßig um die Fortbildung der Lehrkräfte und hier v.a. um die schulischen Datenschutzbeauftragten. Angesichts von über 40.000 Lehrkräften im Land sind diese als Multiplikatorinnen und Multiplikatoren für Fortbildungen im Kollegium unverzichtbar.

Die Lehrerfortbildung erfolgt in enger Kooperation mit dem am 1. August 2010 gegründeten Pädagogischen Landesinstitut Rheinland-Pfalz (PL). Darin sind die bisherigen Pädagogischen Service-Einrichtungen, nämlich das Institut für schulische Fortbildung und schulpsychologische Beratung (ifb), das Pädagogische Zentrum (PZ) und das Landesmedienzentrum (LMZ), zusammengeführt worden. Folgende Veranstaltungen fanden im Berichtszeitraum statt:

Für schulische Datenschutzbeauftragte wurde unter dem Titel „Datenschutz 2.0 – Aktuelles für Datenschutzbeauftragte an Schulen“ eine ganztägige Fortbildung zu rechtlichen und technischen Datenschutzthemen angeboten. Aufgrund der großen Nachfrage wird die Veranstaltung künftig mindestens einmal jährlich stattfinden.

Anlässlich einer Veranstaltung des PL für die Jugendmedienschutzberaterinnen und -berater, die meist auch das Amt der schulischen Datenschutzbeauftragten ausüben, bot der LfD einen Workshop mit dem Titel an „Schule.Medien.Recht. – Datenschutz im Zeitalter von Facebook & Co“, bei der Datenschutz- und Medienkompetenzfragen erörtert werden konnten.

In der Reihe „Pädagogen, Psychologen und Juristen im Gespräch“ fand eine Fortbildung zum Thema „Cybermobbing“ statt, bei der Mitarbeiterinnen und Mitarbeiter des LfD über die rechtlichen Fragen, die mit „Cybermobbing“ im Zusammenhang stehen, informierten.

## 4.7 Datenschutz in der außerschulischen Jugendhilfe

In unserem digitalen Zeitalter sind auch im außerschulischen Bereich Medienbildung und Bildung zum Datenschutz notwendig. Entsprechende Überlegungen werden zur Zeit mit dem zuständigen Jugendministerium konkretisiert, wobei beabsichtigt ist, v.a. die in der außerschulischen Jugendhilfe ehrenamtlich oder hauptamtlich Tätigen entsprechend weiterzubilden.

## 4.8 Zusammenarbeit mit den Medien

Mit Vertreterinnen und Vertretern von ZDF und SWR wurde die Möglichkeit erörtert, in den Sendeformaten, die sich speziell an Kinder wenden – wie „Logo“ und „Pur+“ – verstärkt auch Datenschutzthemen anzusprechen und dabei auf die Unterstützung des LfD zurückzugreifen. Seitens der Leiterin der Hauptabteilung „Kinder und Jugend“ des ZDF wurde dies auch zugesagt. Darüber hinaus gibt es Kontakte mit der Jugendzeitschrift „Bravo“, den Datenschutz jugendgerecht auch in diesem Medium zu präsentieren. Schließlich finden derzeit auch Gespräche mit dem ZDF statt, um in Anlehnung an die ARD-Reihe „Der 7. Sinn“ ein vergleichbares Format für den Datenschutz im Online-Angebot des ZDF zu präsentieren.

## 4.9 Veranstaltungen

Das Thema Datenschutz als Bildungsaufgabe wurde im Berichtszeitraum von einer ganzen Reihe von Veranstaltungen aufgegriffen. Zum Teil wurden diese auch vom LfD mit veranstaltet. Insoweit waren Kooperationspartner v.a. die Universität Koblenz-Landau und die Universität Trier. Mit der Universität Trier (Lehrstuhl Prof. Robbers) wurde am 6. Mai 2011 ein Datenschutzseminar zum Thema „Datenschutz und Internet“ angeboten. Die unter der Schirmherrschaft von Staatsministerin Doris Ahnen stehende Veranstaltung kombinierte Fachvorträge aus dem universitären Bereich – etwa zur „individuellen Verantwortung im Massenmedium Internet“ oder zu praktischen Fragen des sog. Datenklaus – mit Vorträgen von Studierenden der Universität. Vor einer großen Zahl von Schülerinnen und Schülern der Gymnasien und Berufsschulen der Region Trier konnte das so aktualisierte Wissen aus den Plenarvorträgen in Kleingruppenarbeit weiter vertieft werden. Die entsprechenden Themen waren im Vorfeld auf der Grundlage einer Umfrage bei den Schulen ausgearbeitet worden.

Am 6. September 2011 hat der LfD gemeinsam mit der Universität Koblenz-Landau zu einem wissenschaftlichen Workshop „Datenschutz als Bildungsaufgabe“ auf den Campus in Koblenz eingeladen, an dem über 150 Personen aus Wissenschaft, Verwaltung und Schulen teilgenommen haben. Hochrangige Wissenschaftlerinnen und Wissenschaftler aus den Fachgebieten Informatik, Recht, politische Philosophie, Betriebswirtschaft, kognitive Psychologie und Pädagogik haben ihr Wissen zum Themenkreis „Privatheit und Öffentlichkeit“ beigetragen. Praktische Erfahrungen aus Datenschutzprogrammen und gesundheitspolitischen Aufklärungskampagnen rundeten den Workshop ab.

Das ausführliche Programm des Workshops sowie die Foliensätze der Referentinnen und Referenten sind – soweit verfügbar – unter http://www.uni-koblenz-landau.de/koblenz/fb4/institute/iwvi/agtroitzsch/dsbeauftragter/WS-DS-Bildung dokumentiert. Die einzelnen Beiträge des Workshops werden zudem in der Zeitschrift „Datenschutz und Datensicherheit“ (DuD 2/2012) veröffentlicht.

## 4.10 Junior-Beirat

Beim LfD wurde im November 2010 ein sog. Junior-Beirat eingerichtet. Ihm gehören zunächst die Medien-Scouts des Gymnasiums an der Heinzenwies in Idar-Oberstein an. Weitere Medien-Scouts aus anderen rheinland-pfälzischen Schulen werden im Laufe der Zeit noch in den Junior-Beirat berufen werden.

Bei diesem Gremium handelt es sich um ein bundesweit bisher einmaliges Projekt. Es soll einerseits dafür sorgen, dass die Medien-Scouts die für ihre Arbeit in den Schulen notwendigen datenschutzrelevanten Informationen erhalten. Andererseits wird der LfD auf diesem Weg unmittelbar über die datenschutzrelevanten Probleme von Jugendlichen informiert. Um diesen Informationsaustausch zu gewährleisten, soll der Junior-Beirat mindestens einmal im Jahr, bei Bedarf auch öfter zusammen kommen. Außerdem wird den Medien-Scouts ein vom LfD eingerichtetes Internetforum zur Verfügung gestellt, um sich zwischen den Sitzungen auszutauschen oder Fragen an den LfD zu stellen. Die Auftaktsitzung zeigte, dass die Medien-Scouts die Erforderlichkeit einsehen, die Schülerinnen und Schüler über die Risiken und Gefahren der Internetnutzung aufzuklären. Bei der täglichen Arbeit ist es ihnen aber v.a. wichtig, dass ihre Angebote besser in den Schulen kommuniziert werden. Anfang des Jahres 2012 wird die nächste Sitzung des Junior-Beirates stattfinden.

## 4.11 Arbeitskreis Datenschutz und Bildung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Im letzten Datenschutzbericht wurden bereits die Aufgabenschwerpunkte des Arbeitskreises Datenschutz und Bildung ausführlich dargestellt (vgl. 22. Tb., Tz. 3.1.6). Im Berichtszeitraum fanden insgesamt vier weitere Sitzungen unter Vorsitz des LfD statt. Zahlreiche Expertinnen und Experten hatten Gelegenheit, vor dem Arbeitskreis über ihre Aktivitäten zu berichten. Herauszuheben ist Frau MdB Tabea Rößner, die als Mitglied der Enquete-Kommission des Deutschen Bundestages „Internet und digitale Gesellschaft“ über die Arbeit der Enquete-Kommission berichtete und Möglichkeiten einer Zusammenarbeit mit den Datenschutzbeauftragten aufzeigte. Aufgrund der intensiven Zusammenarbeit des Arbeitskreises mit Vertreterinnen und Vertretern der Kultusministerkonferenz konnte erreicht werden, dass sich diese mit dem Thema „Medienbildung in der Schule“ auseinandersetzt und in Kürze ein entsprechendes Papier veröffentlichen wird (vgl. Tz. I-4.1). Weiterhin wurde im Berichtszeitraum das mit Unterstützung des Arbeitskreises erstellte „klicksafe“-Unterrichtsmaterial aktualisiert. Auf die Zusatzmodule „Ich bin öffentlich ganz privat – Datenschutz und Persönlichkeitsrechte im Web“ und „Social Communities“ sei an dieser Stelle besonders hingewiesen (abrufbar unter http://www.klicksafe.de/materialien/). Des Weiteren ist es dem Arbeitskreis gelungen, dass bei der Befragung der Jugendlichen im Rahmen der JIM-Studie 2011 auch Datenschutzthemen aufgenommen wurden (vgl. Tz. I-3.2.6). Nach dem Ergebnis dieser Studie (http://www.mpfs.de/?id=225) sind Jugendliche im Umgang mit ihren Daten durchaus sensibler geworden: 79 Prozent der Befragten gab an, bei der Nutzung sozialer Netzwerke die Privacy-Option des Anbieters genutzt zu haben. Dies zeigt, dass die Aufklärungsbemühungen der Datenschutzbeauftragten und der anderen im Bildungswesen Tätigen Früchte tragen und fortgesetzt werden müssen.

# II. Ausgewählte Ergebnisse aus der Prüfungs- und Beratungstätigkeit des LfD

## 1. Medien und Telekommunikation

### 1.1 Datenschutz bei der Erhebung von Rundfunkgebühren – Rundfunkbeitragsstaatsvertrag

Mit dem 15. Rundfunkänderungsstaatsvertrag, dessen wesentlicher Teil der neue Rundfunkbeitragsstaatsvertrag ist, haben die Landesregierungen einen Systemwechsel bei der Finanzierung des öffentlich-rechtlichen Rundfunks vereinbart. Ab 2013 soll diese nicht mehr durch eine gerätebezogene Abgabe erfolgen, sondern durch einen wohnungs- bzw. betriebsbezogenen Beitrag, der für jede Wohnung nur einmal, unabhängig von der Art und Anzahl der betriebenen Empfangsgeräte, zu entrichten ist und den Betriebe gestaffelt nach ihrer Mitarbeiterzahl bezahlen sollen. Der Modellwechsel eröffnet die Möglichkeit, die datenschutzrechtlich relevanten Befugnisse beim Gebühreneinzug auf das erforderliche Maß zu begrenzen und den Grundsatz der Datensparsamkeit und -vermeidung bei der Beitragserhebung umzusetzen.

Der Staatsvertrag entspricht dem aber nach der Auffassung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder nicht (so ihre Entschließung „Rundfunkfinanzierung: Systemwechsel nutzen für mehr statt weniger Datenschutz!“ vom 11. Oktober 2010; vgl. http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=dsb&ber=079-080_rundfunkfinanzierung).

Der Landtag hat am 22. September 2011 eine Anhörung u.a. auch zu den datenschutzrechtlichen Fragen dieses neuen Gebührenmodells durchgeführt; der LfD hat dort angeregt, die folgenden Regelungen zum Datenschutz der Betroffenen in die gem. § 9 Abs. 2 des Rundfunkbeitragsstaatsvertrags zu erlassende Satzung aufzunehmen:

1. Die Datenerhebungen ohne Beteiligung der Betroffenen sind auf den Zweck der Identifizierung bislang unbekannter Beitragspflichtiger zu beschränken.

2. Die öffentlichen Stellen, die ohne Beteiligung der Betroffenen Auskünfte erteilen sollen, sind möglichst abschließend zu benennen.

3. Eine Datenerhebung bei privaten Stellen ohne Beteiligung der Betroffenen ist auf Adresshandelsunternehmen zum Zweck der Aufdeckung unbekannter Beitragsfälle zu beschränken, Datenerhebungen bei anderen privaten Stellen sind ausdrücklich auszuschließen.

4. Die Betroffenen sind darüber zu unterrichten, welche Daten die Rundfunkanstalten von welchen Stellen ohne Beteiligung der Betroffenen erhoben haben.

5. Das Schwärzen irrelevanter Informationen auf den Leistungsbescheiden, die zum Zweck der Beitragsermäßigung bzw. Beitragsbefreiung vorgelegt werden, ist ausdrücklich zu gestatten.

6. Es sind die Fallgruppen der Abmeldung und die dafür jeweils typischerweise erforderlichen Nachweise ausdrücklich zu benennen, um auszuschließen, dass zur Begründung der Abmeldung überschießende Informationen erhoben werden, wodurch unangemessen in die Privatsphäre der Betroffenen eingedrungen würde.

7. Die Art der von den Rundfunkanstalten auf Dritte übertragbaren Aufgaben und die in Betracht kommenden Auftragnehmerinnen und Auftragnehmer sind möglichst konkret zu benennen; es muss verhindert werden, dass die Rundfunkanstalten ihre hoheitlichen Aufgaben in unangemessenem Umfang privatisieren.

8. Es ist zu verhindern, dass die Daten der Gebühreneinzugszentrale (GEZ) bzw. ihrer Nachfolgeorganisation einem bundesweiten Melderegister gleichkommen; deshalb muss erreicht werden, dass die Rundfunkanstalten nur im erforderlichen Umfang auf die Daten von anderen Rundfunkanstalten – auch innerhalb der GEZ bzw. ihrer Nachfolgeorganisation – zugreifen können.

9. Es ist eine spezielle Regelung über die Gewährleistung der Sicherheit der über die Beitragsschuldnerinnen und -schuldner gespeicherten Daten durch eine Verpflichtung zur Auditierung der Verfahren innerhalb der GEZ bzw. ihrer Nachfolgeorganisation zu schaffen.

Über diese Forderungen wurde im Oktober 2011 mit Vertreterinnen und Vertretern von Landesrundfunkanstalten und der Staatskanzleien einiger Länder beraten. Dabei wurde zwar deutlich, dass die Rundfunkanstalten einigen Punkten nicht zustimmen und weiteren Erörterungsbedarf haben; es wurde aber auch deutlich, dass durchaus Chancen bestehen, den Weg der Satzungsregelung für Verbesserungen des Datenschutzes zu nutzen. Diesem Ziel dienen weitere Gespräche unter Beteiligung des LfD, die derzeit noch nicht abgeschlossen sind.

Wesentliche Anliegen des LfD wurden vom Landtag in einer Entschließung aufgegriffen (LT-Drs. 16/556). Dazu gehört, dass in die vorgesehene Evaluierung des

15. Rundfunkänderungsstaatsvertrags die Frage einbezogen wird, wie sich die datenschutzrechtlich bedeutsamen Regelungen des Rundfunkbeitragsstaatsvertrages bewährt haben. Die Ergebnisse der Evaluierung sollen in den folgenden Novellierungen des Rundfunkstaatsvertrages berücksichtigt werden, damit eine Stärkung von Datenschutzaspekten erfolgt. Dabei ist insbesondere der Verzicht auf den Abgleich von Daten mit nicht-öffentlichen Stellen (Adresshandelsunternehmen) zu prüfen.

Darüber hinaus ist auf ein datenschutzgerechtes Verfahren bei Anträgen auf Beitragsermäßigung hinzuwirken. Die Antragstellerinnen und Antragsteller müssen der GEZ einen Bescheid eines Sozialleistungsträgers vorlegen, der als Nachweis für ihren Antragsgrund (etwa Schwerbehinderung o.ä.) dient. Dieser Bescheid enthält im Regelfall detaillierte Informationen über die gesundheitlichen oder wirtschaftlichen Verhältnisse der Antragstellerinnen und Antragsteller. Wenn die Sozialleistungsträger eine inhaltlich auf das für die GEZ wichtige Ergebnis beschränkte Bescheinigung ausstellen (eine sog. „Drittbescheinigung"), ist das Problem gelöst. Dazu sind aber – v.a. aus Kostengründen – noch nicht alle in Betracht kommenden Stellen bereit. Der LfD wird sich im Zusammenwirken mit der Landesregierung darum bemühen, diese Schwierigkeiten beim Ausstellen von „Drittbescheinigungen" zu beseitigen.

## 1.2 Eine Datenpanne der Landesregierung

Im Zusammenhang mit dem Nürburgring-Untersuchungsausschuss ließ die zuständige Regierungsbeauftragte durch das Technikreferat des Umweltministeriums ein Extranet einrichten. In diesem Extranet waren für die Mitarbeiterinnen und Mitarbeiter der Regierungsbeauftragten folgende Unterlagen verfügbar:

Im Extranet waren verfügbar

- die Einladungen zu den jeweiligen Sitzungen des Untersuchungsausschusses (ohne Anlagen),
- die Vorlagen des Untersuchungsausschusses Nrn. 1 bis 120,
- Presseartikel zum Thema Nürburgring. Dieser Bereich war der Umfangreichste des Angebots.

In den Vorlagen waren zum Teil personenbezogene Daten verschiedener Beteiligter genannt. Sämtliche Vorlagen wurden vom Untersuchungsausschuss vertraulich behandelt.

Im Mai 2011 wurde das Internetangebot der Landesregierung als Folge ihrer Neuorganisation neu strukturiert. In diesem Zusammenhang wurde der gesamte Internetdatenbestand des Ministeriums unter Einschluss des Extranets kopiert, um an der Kopie arbeiten zu können. Dieser Kopiervorgang beseitigte die Konfigurationseinstellungen des Extranet „Nürburgring". In der Folge waren die ursprünglich geschützten Websites von jedermann abrufbar. Voraussetzung war zwar die Eingabe des erforderlichen Pfades; dies war bei der Nutzung entsprechender Suchmaschinentreffer allerdings leicht möglich gewesen, da die Angaben im Inhaltsverzeichnis durch Suchmaschinen auswertbar gewesen waren. Diese Möglichkeit des allgemeinen Zugriffs auf die Inhaltsdaten des Extranets wurde erst mit der Veröffentlichung dieses Sachverhalts in einem Artikel der „Rheinpfalz" am 2. November 2011 bekannt und dann sofort gesperrt.

Die damit zusammenhängenden Vorgänge hat der LfD im Wesentlichen wie folgt bewertet: Das Versehen, das unmittelbar zur öffentlichen Zugänglichmachung von vertraulichen Daten führte, hatte aus der Sicht des LfD eine nicht unwesentliche Ursache in einem strukturellen Mangel. Das Extranet wurde nicht als besonders zu schützender Teil des in Rede stehenden Internetangebots begriffen und behandelt. Dies wiederum kann als Folge der mangelnden Dokumentation und als Folge der fehlenden Risikoabschätzung angesehen werden, die gesetzlich in §§ 4 und 9 LDSG vorgeschrieben sind. Auch deshalb wohl wurde bei der Umgestaltung des Internetangebots die Gefahr übersehen, die im Vorgang des Kopierens und des Wiederaufspielens des Internetangebots des Umweltministeriums in Bezug auf den Zugang zu den Inhalten des Extranets lag. Im Ergebnis kam der LfD nicht umhin, die festgestellten Verstöße gegen datenschutzrechtliche Regelungen gem. § 25 Abs. 1 LDSG zu beanstanden.

Vor diesem Hintergrund hat der LfD für künftige vergleichbare Fälle die Landesregierung auf folgende Punkte hingewiesen:

- Bei der Einrichtung von besonderen Stellen der Landesregierung (Regierungsbeauftragten u.ä.), die eine eigene Aufgabe mit einem eigenen Stab zu erfüllen haben und außerhalb der Ressortverantwortlichkeiten angesiedelt sind, ist der Aspekt des Datenschutzes bereits bei der Einrichtung zu beachten. Wenn diese Stellen mit personenbezogenen Daten umgehen sollen, ist zu prüfen, ob behördliche Datenschutzbeauftragte zu bestellen sind.
- Soweit zur Datenverarbeitung einer solchen Stelle Mittel anderer öffentlicher Stellen eingesetzt werden sollen, sind die Anforderungen des § 4 LDSG (Auftragsdatenverarbeitung) zu beachten.
- Die Nutzung der Internetstruktur zur internen Kommunikation bedarf besonderer Aufmerksamkeit.

Bei besonders schützenswerten Daten ist eine Vorabkontrolle gem. § 9 Abs. 5 LDSG durchzuführen.
- Auch der Frage der Speicherdauer, also der Löschung personenbezogener Daten in internen Netzen ist besondere Aufmerksamkeit zu widmen; dies gilt besonders für Daten, deren Vertraulichkeit oder Schutzbedürftigkeit hoch ist.
- Generell ist darauf zu achten, dass die Anforderungen des § 9 LDSG bei Internetangeboten umgesetzt werden, wenn ihre Inhalte personenbezogene Daten umfassen.
- Im Fall einer Datenpanne sind alle Möglichkeiten zu nutzen, um das Ausmaß von unberechtigten Zugriffen nachträglich feststellen zu können. Vorhandene Zugriffsprotokollierungen sind zu diesem Zweck zeitnah umfassend auszuwerten; eine Löschung kommt erst nach solchen Auswertungen in Betracht.

Der LfD wird sich – auch aufgrund der in diesem Kontext deutlich gewordenen Aspekte – darum bemühen, die Gesichtspunkte eines angemessenen Datenschutzmanagements, der Risikofolgenabschätzung und der Erstellung von Datenschutzkonzepten bei der Internetnutzung durch öffentliche Stellen, insbesondere aber durch die Landesregierung, in einem Gespräch mit allen betroffenen Stellen zu vertiefen. Als Ergebnis sollten die bestehenden Dienstanweisungen zum Datenschutz um Regelungen ergänzt werden, die es allen Beteiligten erleichtern, das Internet datenschutzgerecht einzurichten und zu nutzen.

## 1.3 Profilneurosen – der datenschutzkonforme Betrieb von Web-Analysediensten

Wie viele Zugriffe erfährt mein Internetangebot? Was interessiert die Nutzerinnen bzw. Nutzer und was nicht? Wie lange bleiben sie? Wohin springen sie ab? Kommen sie wieder? Diese und andere Fragen sind für die Betreiberinnen und Betreiber eines Internetangebots häufig von fundamentalem Interesse, das über eine Reihe von Analyseinstrumenten befriedigt werden soll. Andererseits birgt die Auswertung von Nutzungsdaten die Gefahr gläserner Nutzerinnen und Nutzer. Der Gesetzgeber hat beidem in Form des § 15 Abs. 3 TMG Rechnung getragen, indem er für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien die Bildung von Nutzungsprofilen erlaubt, sofern diese pseudonym erstellt werden und Nutzerinnen und Nutzer nicht widersprechen.

Die Datenschutzaufsichtsbehörden haben in einer Beschluss vom November 2009 die Anforderungen des Telemediengesetzes und der allgemeinen Datenschutzregelungen dargestellt, die für eine datenschutzkonforme Ausgestaltung dieser sog. Reichweitenanalyse zu berücksichtigen sind.

„Anforderungen an die datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internetangeboten“

- Bildung von Nutzungsprofilen nur unter Pseudonym
- Widerspruchsmöglichkeit gegen Nutzungsprofile
- Hinweis auf Nutzungsprofile und Widerspruchsmöglichkeit in der Datenschutzerklärung
- Verbot der Zusammenführung von Nutzungsdaten mit Identitätsdaten
- Auswertung nur anhand anonymisierter IP-Adressen
- Einwilligung für die Verarbeitung personenbezogener Daten, soweit nicht für Abrechungszwecke oder die Erbringung des Telemediums erforderlich
- Löschung der Nutzungsdaten auf Verlangen der Nutzerinnen und Nutzer

Beschluss des Düsseldorfer Kreises vom 26./27. November 2009

http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=ddk&ber=20091127_inetreichweite

Im Blickpunkt der Datenschutzbeauftragten standen aufgrund ihrer Marktbedeutung im Bereich der Wirtschaft und Verwaltung in diesem Zusammenhang insbesondere zwei Analyseinstrumente – „Google Analytics“ der Google Inc. sowie die Open Source-Lösung „Piwik Web Analytics“.

### 1.3.1 Google Analytics

Der von Google angebotene Dienst zur Nutzungsanalyse von Internetangeboten nahm in der Diskussion breiten Raum ein. Aufgrund der dadurch insbesondere in der Wirtschaft ausgelösten Verunsicherung hat Google sich nach anfänglichem Sträuben einem konstruktiven Dialog nicht verschlossen. In Verhandlungen der Datenschutzbehörden unter Federführung des Hamburgischen Datenschutzbeauftragten ist es letztlich gelungen, eine datenschutzkonforme Lösung abzustimmen (vgl. Tz. I-3.3.2).

### 1.3.2 Piwik Web Analytics

Im Gegensatz zu Google Analytics, bei dem die Websitebetreiberinnen und -betreiber auf einen von Google angebotenen Dienst zurückgreifen, kann die Open Source-Lösung „Piwik Web Analytics“ vollständig auf der IT-Struktur der Anbieterinnen bzw. Anbieter und unter deren alleiniger Kontrolle betrieben werden. Auch Piwik blieb in einer zunächst angebotenen Version hinter dem Anfor-

derungskatalog der Datenschutzaufsichtsbehörden zurück. In einem Projekt der Piwik-Entwicklung und des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein wurden die bestehenden Defizite jedoch aufgearbeitet und in der aktuell verfügbaren Version bereinigt.

Die zentralen Anforderungen für einen datenschutzkonformen Einsatz von Piwik sind folgende:

- Die in den Nutzungsdaten enthaltene IP-Adresse ist vor der Speicherung und Auswertung über das Piwik-Plugin „AnonymizeIP“ um die beiden letzten Stellen zu kürzen (z.B. 82.165.xxx.xxx),
- die Lebensdauer von Cookies, die über die Dauer der Sitzung hinaus auf dem Rechner der Nutzerinnen und Nutzer gespeichert werden, ist auf eine Woche zu begrenzen,
- die standardmäßige Auswertung der Angaben, welches Internetangebot von Nutzerinnen und Nutzern zuvor in Anspruch genommen wurde (Referrer), ist zu deaktivieren,
- die Nutzerinnen und Nutzer sind im Rahmen einer Datenschutzerklärung auf den Einsatz von Piwik, Art, Umfang und Zweck der Verarbeitung von Nutzungsdaten sowie auf ihre hiergegen bestehende Widerspruchsmöglichkeit hinzuweisen (vgl. § 15 Abs. 3 i.V.m § 13 Abs. 1 TMG; ein entsprechender Entwurf wird gegenwärtig im Ministerium des Innern, für Sport und Infrastruktur erarbeitet und soll allen Ressorts zur Verfügung gestellt werden),
- für die Ausübung eines Widerspruchs nach § 15 Abs. 3 TMG ist eine technische Möglichkeit in Form des von Piwik angebotenen Opt-Out-Cookies vorzusehen.

Zur Umsetzung wird auf die Anleitung zum datenschutzkonformen Einsatz von Piwik des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein verwiesen.

Für die Datenschutzerklärung und die Widerspruchsmöglichkeit sind aus Sicht des LfD die von der Rechtsprechung für die Angaben nach § 5 Abs. 1 TMG entwickelten Grundsätze analog anzuwenden, d.h. sie sollen leicht erkennbar und unmittelbar erreichbar sein. Dies bedeutet, dass sie nach maximal zwei Mausklicks zur Verfügung stehen. Eine Praxis, bei der die über Piwik erhobenen Nutzungsdaten nach einem Monat gelöscht und lediglich die 500 häufigsten sowie summarisch die sonstigen Seitenaufrufe archiviert werden, begegnet aus Sicht des LfD keinen Bedenken.

Die im Bereich der Landesregierung eingesetzte Piwik-Installation genügte diesen Anforderungen zunächst nur in Teilen. Defizite bestanden insbesondere hinsichtlich der Datenschutzerklärungen und der Bereitstellung einer Widerspruchsmöglichkeit. Zwischenzeitlich wurde diese angepasst; ausstehende Nachbesserungen sollen zeitnah erfolgen.

Die Verantwortung für eine datenschutzkonforme Ausgestaltung des Verfahrens liegt, auch bei der Einbindung Dienstleistender, nach § 4 Abs. 1 LDSG i.V.m. § 2 Nr. 1 TMG beim jeweiligen Anbieter, d.h. der Verwaltung, welche das Internetangebot betreibt. Dort, wo Verwaltungen auf den Landesbetrieb Daten und Information als Dienstleister zurückgreifen, wird künftig durch die dort zentral betriebenen Piwik-Verfahren eine einheitliche Umsetzung der genannten Anforderungen gewährleistet. Soweit Verwaltungen selbst oder über andere Dienstleistende Piwik betreiben, muss die Datenschutzkonformität jeweils separat geprüft werden.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
„Anleitung zum datenschutzkonformen Einsatz von Piwik“
https://www.datenschutzzentrum.de/tracking/piwik/.

## 1.4 Logbuch – Protokollierung von Zugriffen auf Webserver

Nach § 13 Abs. 4 TMG haben Diensteanbieterinnen und -anbieter durch technische und organisatorische Vorkehrungen sicherzustellen, dass die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht werden. Sie dürfen nach § 15 Abs. 1 TMG nur erhoben und verwendet werden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. § 15 TMG verbietet somit die Speicherung von IP-Adressen für andere Zwecke, da sie unter Umständen einer bestimmten Nutzerin oder einem bestimmten Nutzer zugeordnet werden können und damit personenbezogene Daten sind (vgl. Tz. II-1.5).

Eine Protokollierung der Zugriffe in entsprechenden Logdateien des Webservers darf damit nur ohne die Speicherung der vollständigen IP-Adresse bzw. sonstiger, identifizierender Merkmale erfolgen. Die IP-Adresse ist vor jeglicher Auswertung so zu kürzen, dass eine Personenbeziehbarkeit ausgeschlossen ist.

Für die beim Landesbetrieb Daten und Information betriebenen Internetangebote wurde mit diesem eine Verfahrensweise abgestimmt, nach der auf Windows-Webservern durch eine Programmroutine das letzte Byte der zugreifenden IP-Adresse in den Logfiles entfernt wird; auf Linux-Webservern wird die IP-Adresse des anfragenden

Rechners um das letzte Byte gekürzt, bevor die Daten in die Logdatei geschrieben werden. Damit wird in beiden Fällen gewährleistet, dass eine Auswertung der Protokolldaten nur mit anonymisierten Daten erfolgt. Mit dieser Verfahrensweise wird aus Sicht des LfD den Anforderungen aus § 15 Abs. 1 TMG entsprochen.

Hinweise des LfD zu einer datenschutzkonformen Protokollierung von Webzugriffen (http://www.datenschutz.rlp.de/downloads/oh/info_webserverlogfiles.pdf).

Soweit im Rahmen der Diskussion geltend gemacht wurde, dass eine Speicherung der vollständigen IP-Adresse zur Abwehr oder Aufklärung von Angriffen auf die IT-Struktur notwendig sei, hat der LfD folgenden Standpunkt vertreten:

Hinsichtlich einer Speicherung von IP-Adressen zum Schutz von IT-Systemen gegen unerlaubte Zugriffe enthält das Telemediengesetz keine Regelungen. Entsprechende Maßnahmen mit dem Ziel, Angriffe zeitnah zu erkennen bzw. ihnen zeitnah zu begegnen, dienen aus seiner Sicht jedoch der Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungssysteme und lassen sich auf § 12 Abs. 3 TMG i.V.m. §§ 9 Abs. 2, 13 Abs. 6 LDSG bzw. in analoger Anwendung auf § 100 Abs. 1 TKG stützen. Danach kommt eine vorübergehende Speicherung der vollständigen IP-Adresse als technische Vorkehrung zum Schutz der Datenverarbeitungssysteme gegen Angriffe und zum Erkennen, Eingrenzen oder Beseitigen entsprechender Störungen in Betracht. Voraussetzung ist,

- dass diese Verbindungsdaten nicht auf den Webservern, sondern auf den am zentralen Internetübergang betriebenen Sicherheitseinrichtungen (z.B. Firewall) gespeichert werden,
- die Speicherungsfrist sieben Tage nicht überschreitet; dieser Zeitraum reicht nach Auffassung des LfD aus, um Angriffe und Störungen zu erkennen, einzugrenzen und zu beseitigen und um sich künftig gegen unerlaubte Zugriffe zu schützen; nach Ablauf der sieben Tage ist, um eine personenbezogene Speicherung auszuschließen, die weitere Speicherung der IP-Adresse nur verkürzt (z.B. begrenzt auf die ersten drei Bytes) zulässig,
- dass sichergestellt wird, dass auf die gespeicherten Verbindungsdaten nur von Personen zugegriffen werden kann, die mit der Sicherstellung eines ordnungsgemäßen Betrieb befasst sind.

## 1.5 IPv6 – Numerologie der Privatsphäre

IP-Adressen sind begehrt. Alle, die im Internet unterwegs sind, gleich ob als Anbieterin und Anbieter oder Nutzerin und Nutzer, benötigen eine IP-Adresse. Sie wird einem vom jeweiligen Internetanbieter zugewiesen; im Fall, dass man ein eigenes Angebot vorhält, als dauerhafte, statische Adresse, zum Surfen oder für die Nutzung anderer Dienste temporär. Angesichts der Wachstumsraten des Internets und der beschränkten Zahl möglicher Adressen war absehbar, dass diese eines Tages ausgehen würden. Zwar konnte dieser Tag durch die von den Providern praktizierte dynamische Adressvergabe hinausgeschoben werden, doch Mitte 2011 wurde die letzte noch freie IP-Adresse vergeben. Die dynamische Vergabe von Adressen brachte als Nebenprodukt auch einen Datenschutzvorteil: dadurch, dass den Nutzerinnen und Nutzern aus einem Pool aktuell nicht genutzter Adressen vorübergehend eine freie Adresse zugewiesen wurde, waren die sie im Netz mit wechselnden IP-Adressen unterwegs und verwischten damit einen Teil ihrer Datenspuren.

An der Schwelle zum „Internet der Dinge“, in dem neben Computern und Smartphones über kurz oder lang auch Sensoren, Energiezähler, Haushaltsgeräte, RFID-bestückte Objekte und Alltagsgeräte bis hin zu Rolladensteuerungen oder Rasensprengern ins Internet eingebunden werden, war allerdings auch die dynamische Vergabe keine Lösung auf Dauer. Mit dem Internet Protocol Version 6 (IPv6) wurde daher ein neues Adressierungsverfahren eingeführt, das eine nahezu unbegrenzte Anzahl von statischen IP-Adressen zur Verfügung stellt und es theoretisch erlaubt, jedem Sandkorn auf der Erde eine eigene IP-Adresse dauerhaft zuzuweisen. Durch eine solche Vergabe statischer Adressen können Internetnutzende identifiziert und ihre Aktivitäten unabhängig von Cookies, Zählpixeln oder Browserprofilen websiteübergreifend zu individuellen Nutzungsprofilen zusammen geführt werden.

IPv6-Adresse:
2001:0db8:85a3:08d3 : 1319:8a2e:0370:7347
Präfix Interface identifier

Dies kann anhand beider Bestandteile der IPv6-Adressen erfolgen, des von den Internetprovidern bereitgestellten Präfixes als auch des gerätespezifischen Interface Identifiers. Für beide müssen daher datenschutzfreundliche Mechanismen zur Verfügung stehen, die es erlauben, weitgehende Anonymität zu wahren. Möglich ist dies für das Präfix z.B. dadurch, dass dieses weiterhin dynamisch vergeben wird oder die Nutzerinnen und Nutzer auf Wunsch wechselnde Präfixe erhalten. Beim Interface Identifier, der als Bestandteil eine weltweit eindeutige

Geräteinformation enthält (MAC-Adresse), besteht die Möglichkeit, diese über die sog. Privacy Extensions durch eine zufällige Zeichenfolge zu ersetzen und so die Zuordnung der Internetnutzung zu einem bestimmten Gerät (z.B. einem Smartphone) zu verhindern.

Privacy Extensions

Ob und wie die Privacy Extensions für die verschiedenen Betriebssysteme aktiviert werden können, ist unter folgendem Link beschrieben:

http://www.heise.de/netze/artikel/IPv6-Privacy-Extensions-einschalten-1204783.html

Viele Betreiberinnen und Betreiber sowie Anwenderinnen und Anwender stellen gegenwärtig ihre Netzwerktechnik auf das Internetprotokoll Version 6 um. Die Datenschutzbeauftragten des Bundes und der Länder haben daher in einer Entschließung gefordert, dass die Migration von IPv4 zu IPv6 nicht zu einer Verschlechterung des Datenschutzes führen darf. Internetanbieterinnen und -anbieter sowie Herstellerinnen und Hersteller sollten ihre Produkte datenschutzgerecht gestalten (privacy by design) und dementsprechende Voreinstellungen wählen (privacy by default). Internetnutzerinnen und -nutzer sollten bei der Beschaffung von Hard- und Software sowie beim Abschluss von Verträgen auf diese Aspekte besonders achten.

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28/.29. September 2011

„Einführung von IPv6 steht bevor: Datenschutz ins Netz einbauen!“

http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=dsb&ber=082_ipv6

## 1.6 Information anytime and anywhere – Einsatz mobiler Endgeräte

„Information at your fingertips“ lautete der Titel eines Vortrags von Microsoftchef Bill Gates, mit dem er im November 1994 seine Vision von der Zukunft vorstellte. Dargestellt wurde sie anhand eines Films um die Aufklärung eines Kunstschmuggels mit der Hilfe futuristischer Kommunikationsmittel. Die Gegenspieler der Schmugglerbande, ein Schüler und seine Mutter, recherchierten dabei von der Küche aus im „Cyberspace“ alle Details zur präkolumbianischen Kunst. Nachdem der Junge bei einer Verfolgungsjagd von einem Auto angefahren wurde, kommunizierte die Besatzung des Krankenwagens noch während der Fahrt über eine Videoverbindung mit der Klinik die Diagnose und leitete die optimale Behandlung des Jungen ein. Die Polizei verschaffte sich schon von unterwegs einen Überblick vom Tatort und steuerte den Einsatzcomputer mit Sprachbefehlen.

Video „Information at Your Fingertips“ from Bill Gates' Comdex Keynote 1994
http://blip.tv/buecherwurm/video-information-at-your-fingertips-from-bill-gates-comdex-keynote-1994-2149597

Gates versprach seinen Zuhörern, dass sich diese Technik binnen zehn Jahren natürlich in unser Leben einfügen werde. Man kann darüber streiten, wie viel Wahrheit in dieser Prophezeiung steckte, doch spätestens mit der Verbreitung von Smartphones und Tablet-PCs im Massenmarkt ist die Vision ubiquitärer, nur einen Fingertipp entfernter Informations- und Kommunikationsmöglichkeiten Realität geworden.

Unter Federführung der Zentralstelle IT und Beteiligung des LfD wurde für die rheinland-pfälzische Landesverwaltung eine Strategie für die mobile Sprach- und Datenkommunikation entwickelt. In diesem Zusammenhang läuft seit Dezember 2010 ein Pilotversuch, bei dem für einen ausgewählten Personenkreis (z.B. Amtsleitung, Ministerbüro, Presseabteilung) Lösungen auf der Grundlage der Blackberry BES-Infrastruktur bereit gestellt werden. Ein ebenfalls vorgesehener Pilotversuch zur Erprobung von iOS-basierten Geräten (Apple iPad/iPhone) wurde aufgrund von Sicherheitsbedenken zunächst zurückgestellt.

Landesstrategie zum mobilen E-Mail-Zugriff

https://www.it-sicherheit.rlp.de/it-sicherheit-rlp/berichte/mobiler-e-mail-zugriff/ (Zugriff nur aus dem rlp-Netz)

Hinsichtlich der Zugriffsmöglichkeiten der Firma RIM auf die über die Blackberry Enterprise Services-Infrastruktur übertragenen Daten sind weiterhin Fragen offen. Aus Sicht des LfD kommt diese Lösung daher gegenwärtig nur für die Bereiche in Betracht, die von der Verschlusssachenanweisung nicht erfasst werden bzw. nicht als sensitive Regierungskommunikation unterhalb von Verschlusssachen einzustufen sind. Für darüber hinausgehende Einsatzbereiche bedarf es einer zusätzlichen Verschlüsselung der Daten, bevor diese über eine von Auftraggeberin bzw. Auftraggeber nicht kontrollierbare Infrastruktur des Anbieters geleitet werden. Die qualitativen Anforderungen an die jeweilige kryptografische Lösung sind an den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik auszurichten (IT-Grundschutzkataloge Maßnahme M 2.164).

Einer der Kernpunkte der Landesstrategie ist, dass dienstlich bereit gestellte Geräte zum Einsatz kommen, die entsprechend den Sicherheitsvorgaben konfiguriert und administriert werden können. Nur so lassen sich die zentralen Gesichtspunkte

- Schutz der auf dem Endgerät gespeicherten Daten,
- Sicherstellung einer vertraulichen und vertrauenswürdigen Kommunikation,
- Schutz vorhandener IT- und Netzwerkstrukturen der Dienststelle,
- Administration der Endgeräte und Löschung im Falle des Verlusts

verlässlich gewährleisten. Mit der breiten Verfügbarkeit von Smartphones im Consumerbereich steigt allerdings der Druck auf die IT-Abteilungen, neben Blackberry-Systemen auch Systeme anderer Hersteller und insbesondere eine gemischte dienstlich bzw. private Nutzung der Geräte zuzulassen. Auch gibt es in der Wirtschaft unter dem Schlagwort „Bring your own device“ eine Entwicklung, die den Einsatz privater Geräte für geschäftliche Zwecke propagiert.

Aus Sicht des LfD sollten jedoch grundsätzlich nur dienstlich bereit gestellte Geräte zum Einsatz kommen, wie dies auch in den Fällen der Tele- oder Heimarbeit gehandhabt wird. Insbesondere auf der Leitungsebene mögen im Einzelfall Rahmenbedingungen vorliegen, die ein Abweichen von den Vorgaben des Landesstandards nach sich ziehen können. Um Sicherheitsbeeinträchtigungen zu vermeiden, muss ein Einsatz privater Geräte auf Bereiche beschränkt bleiben, die verlässlich durch organisatorische Regelungen gehandhabt werden können. „Information at your fingertips“ bedeutet auch Fingerspitzengefühl für Datenschutz- und Sicherheitsbelange.

Bei der Nutzung privater Geräte hat die Dienststelle letzten Endes nicht die vollständige bzw. alleinige Verfügungsgewalt. Ihr Einsatz kommt damit aus Sicht des LfD nur ausnahmsweise in Betracht. Ein denkbarer Einsatzbereich ist die Sprachkommunikation, bei der sich keine Sicherheitsfragen für das rlp-Netz stellen; hier ist eine Umleitung von Gesprächen auf das private Mobiltelefon der Amtsleitung möglich. Dies gilt auch für die Synchronisation von Kontakten oder Terminen, jedenfalls soweit diese Angaben datenschutzrechtlich nicht sensibel sind. Dabei muss jedoch sichergestellt sein, dass von der Synchronisierung selbst keine Gefährdungen für den dienstlichen PC ausgehen (Virenschutz etc.). Die Synchronisation von E-Mails oder die Speicherung von Dokumenten mit personenbezogenen Daten kommt nur in Betracht, wenn die Anforderungen aus der Landesstrategie erfüllt werden können.

# 2. Wirtschaft

## 2.1 Entwicklung der Eingaben und Kontrollen im privatwirtschaftlichen Bereich

Auch wenn der staatliche Datenschutz seinen Ursprung im Schutz der Bürgerinnen und Bürger vor übermäßigem behördlichen Informationsinteresse hat – die Leitentscheidung des Bundesverfassungsgerichts zum Datenschutz befasste sich mit der Volkszählung 1982 –, so hat sich mittlerweile das Gefährdungspotential doch deutlich in den privaten Sektor verlagert (vgl. 22. Tb., Tz. 5.1). Die Vielzahl der Datenschutzskandale der vergangenen Jahre – Deutsche Telekom, Deutsche Bahn und Lidl und Co. – haben zu der Einsicht geführt, dass das Grundrecht auf informationelle Selbstbestimmung heute besonders durch die Privatwirtschaft gefährdet wird. Das Wort des ehemaligen Präsidenten des Bundesverfassungsgerichts, Prof. Dr. Papier, der vor den Gefahren eines „Super-GAUs des Datenschutzes“ in der Privatwirtschaft warnte, hat immer noch Bestand und Berechtigung.

Dies zeigt auch die Entwicklung der Eingaben von Bürgerinnen und Bürgern an den LfD. Nach § 29 LDSG können sich alle Betroffenen jederzeit unmittelbar an den LfD mit ihren Fragen, Bitten und Beschwerden wenden – und sie tun dies in weiter wachsendem Maße: Bewegte sich die Zahl der Eingaben an die Aufsichts- und Dienstleistungsdirektion im Jahre 2008 noch im zweistelligen Bereich, so gingen beim LfD seit Aufnahme seiner Tätigkeit im privatwirtschaftlichen Bereich bereits im ersten Jahr mehr als 1.000 Eingaben ein, in mehr als 300 Fällen führten diese Eingaben zu weitergehenden Ermittlungen und umfangreichen Stellungnahmen des LfD. In den vergangenen zwei Jahren setzte sich diese Entwicklung auf hohem Niveau fort. 2010 erreichten den LfD 390 schriftliche und 1.016 mündliche Eingaben (insgesamt: 1.406), im Jahre 2011 wuchs die Zahl der Petitionen auf mehr als 1.500 an (310 schriftliche, 1.235 mündliche Eingaben).

Schwerpunkte der Eingaben sind dabei stets die Bereiche Arbeitnehmerdatenschutz, Videoüberwachung, Internetnutzung, Adresshandel, Wirtschaftsauskunfteien sowie Fragen zur Tätigkeit der betrieblichen Datenschutzbeauftragten.

Schätzungsweise über 200.000 private geschäftsmäßig tätige datenverarbeitende Stellen sind in Rheinland-Pfalz ansässig. Eine lückenlose flächendeckende Überwachung und Kontrolle ist angesichts der zur Verfügung stehenden personellen und sächlichen Ausstattung des LfD – auch nach der personellen Aufstockung im Jahre 2009 – unmöglich. Auch helfen gesetzgeberische Maßnahmen alleine nicht weiter, wenn ihre Einhaltung nicht ausreichend kontrolliert und Verstöße nicht unterbunden werden können. Die Datenschutzaufsichtsbehörden müssen daher auch zukünftig organisatorisch, personell und finanziell in die Lage versetzt werden, ihren Beratungs- und Kontrollaufgaben unabhängig und wirkungsvoll nachkommen zu können.

Generell ist festzustellen, dass sich die Datenschutzprobleme im Bereich der Privatwirtschaft parallel zur exponentiellen Entwicklung der Kommunikationstechnik in immer kürzeren Zeiträumen steigern. Riesige Datenbestände mit teils sensiblen Informationen entstehen bei immer mehr privaten Unternehmen und keineswegs nur bei Amazon oder Google. Die Miniaturisierung von Speichern macht das unbefugte Kopieren und Übermitteln immer leichter, damit werden auch missbräuchlich Datenverwendungen in immer neuen Dimensionen möglich. Hinzu kommen die neuen Gefahren im Internet, insbesondere durch das Web 2.0, durch eine lückenlose Erfassung des Nutzungsverhaltens, durch Identitätsdiebstähle, Phishing oder virtuellen Exhibitionismus. Gerade im Jahre 2011, dem „Jahr der Hacker“, wurde vielen Unternehmen, aber auch deren Kundinnen und Kunden sowie Mitarbeiterinnen und Mitarbeitern deutlich vor Augen geführt, dass der Datenhunger Krimineller auch vor kleinen und mittelständischen Unternehmen nicht halt macht. Zugleich mussten viele Bürgerinnen und Bürger erfahren, dass der eigene sorgsame Umgang mit persönlichen Daten keineswegs davor schützt, dass Dritte unbefugt auf sie zugreifen. Vielmehr sind wir alle abhängig davon, dass unsere Dienstleisterinnen und Dienstleister und Vertragspartnerinnen und -partner, aber auch alle staatlichen Stellen Vorkehrungen für eine effektive Datensicherheit treffen.

In dieser Situation kann die Kontroll- und Aufsichtstätigkeit der staatlichen Aufsichtsbehörde nur „Grundbedarfe“ abdecken, mehr als die stichprobenartige Untersuchung datenschutzrechtlicher Problemfelder in wenigen Schwerpunktgebieten sind weder personell noch finanziell möglich. Umso wichtiger war es für den LfD, von Anfang an Netzwerke zu bilden, die Beratungsleistungen auszubauen und durch zahlreiche Vorträge zum Thema Datenschutz Multiplikatoren zu erreichen (vgl. Tz. I-3.8 und Tz. I-3.9).

Eine herausgehobene Stellung spielen dabei nach wie vor die betrieblichen Datenschutzbeauftragten, die als „Außenstellen“ des Datenschutzes für ein möglichst hohes Niveau des Datenschutzes in den Betrieben verantwortlich sind. Aus diesem Grunde hat der LfD die groß angelegte Umfrage bei 1.500 Unternehmen in Rheinland-Pfalz schwerpunktmäßig auf die betrieblichen Datenschutzbeauftragten, ihre Ausstattung, Ausbildung und Tätigkeits-

gebiete ausgerichtet (vgl. Tz. I-3.7). Auch in diesem Zusammenhang wurde der Kontakt zu den institutionellen Ansprechpartnern ausgeweitet und vertieft: Die Industrie- und Handelskammern, die Handwerkskammern, aber auch die Kammern der freien Berufe (Ärztekammern, Rechtsanwaltskammern, Notarkammern) sind „natürliche Verbündete“ des LfD bei der Verbesserung des Datenschutzniveaus in Rheinland-Pfalz.

Auch die Kontakte zu den „Erfahrungsaustausch-Kreisen“ der betrieblichen Datenschutzbeauftragten (Erfa-Kreise) wurden weiter intensiviert, durch eigene Informationsveranstaltungen in Mainz, Koblenz und Ludwigshafen wurde die Netzwerkbildung in diesem Bereich weiter gefördert.

Neben der notwendigen aufsichtbehördlichen Tätigkeit wird der LfD auch zukünftig das Schwergewicht seiner Bemühungen auf Kooperation und Beratung im Bereich der Privatwirtschaft legen. Entscheidend für das Niveau des Datenschutzes in den Unternehmen ist weniger die gesetzgeberische und aufsichtbehördliche Tätigkeit des Staates, sondern das Engagement und die Durchsetzungsfähigkeit der betrieblichen Datenschutzbeauftragten.

Wichtige Kooperationspartnerinnen und -partner der Datenschützerinnen und Datenschützer bleiben weiterhin die Verbraucherschützerinnen und Verbraucherschützer. Häufig arbeiten sie, wenn auch mit unterschiedlichen Ansätzen, an denselben Problemen, etwa an der Bekämpfung von betrügerischen Vertragsabschlüssen im Internet oder dem Schutz Minderjähriger in sozialen Netzwerken. Aus diesem Grund sind der LfD und die Verbraucherschutzzentrale Rheinland-Pfalz entschlossen, auf den gemeinsamen Tätigkeitsfeldern die Kräfte zu bündeln. So informiert die Verbraucherschutzzentrale bereits in Absprache mit dem LfD die Verbraucherinnen und Verbraucher über ihre Möglichkeiten, datenschutzrechtliche Auskunfts- und Löschungsansprüche gegenüber gewerblichen Anbieterinnen und Anbietern durchzusetzen (vgl. Tz. II-3.1.2). Umgekehrt kann der LfD bei der Klärung der Rechtmäßigkeit von Vertragsanbahnungen (sog. cold calls) und bei der Ermittlung der für Werbemaßnahmen verantwortlichen Stellen wichtige Unterstützung leisten.

## 2.2 Videoüberwachung

### 2.2.1 Videoüberwachung allgemein

Schon in seinem 22. Tätigkeitsbericht hat der LfD auf das Schwerpunktthema „Videoüberwachung“ hingewiesen und erste Schlussfolgerungen hierzu gezogen (vgl. 22. Tb., Tz. 3.2). Durch spektakuläre Aktionen wie die zur „Mainzer Videomeile“ hat er diese Thematik weitergeführt – auf einer Strecke von gerade einmal 400 Metern wurden in der Mainzer Fußgängerzone in Einkaufspassagen und Supermärkten, in Banken und an Geldautomaten auf öffentlichen Plätzen, in Restaurants und Cafés 100 Videokameras ausgemacht und unter reger Beteiligung von Verbraucherinnen und Verbrauchern sowie von Vertreterinnen und Vertretern der Presse auf einem Rundgang „besichtigt”.

Zigtausende Videokameras werden zur Zeit zur Überwachung von Supermärkten und Kaufhäusern, von Einkaufspassagen und Tankstellen, von Bahnhöfen und Sparkassen, aber auch von Schulen und Hochschulen, von Gerichten und städtischen Bussen in Rheinland-Pfalz eingesetzt. Nach § 6b BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Insbesondere muss die Videoüberwachung erforderlich sein, und die schutzwürdigen Interessen der Betroffenen müssen durch entsprechende technische und organisatorische Maßnahmen ausreichend geschützt werden. Mittlerweile sind aufgrund der technologischen Fortentwicklung diese Kameras häufig nicht mehr als solche zu erkennen, sondern ähneln kleinen Lampen mit wenigen Zentimetern Durchmesser. Auch trennen uns nur noch ein paar Entwicklungsschritte von einer „intelligenten Videoüberwachung“, die Gesichter erkennen und auf bestimmte „auffällige“ Bewegungen von „Zielpersonen“ reagieren kann. Insbesondere die datenmäßige Vernetzung der Kameras ist in Teilbereichen bereits machbar. So gesehen stehen wir an einem Scheideweg: Entweder die unkontrollierte und unkontrollierbare Ausbreitung der Videoüberwachung hinzunehmen, die unser Privatleben weiter einschränken und unser Verhalten zunehmend beeinflussen wird, oder aber gegenzusteuern.

Grundlage einer Zurückdrängung der sich epidemisch ausbreitenden Videoüberwachungsanlagen muss zunächst eine Analyse der aktuellen Situation in Rheinland-Pfalz sein. Deswegen führte der LfD in den Jahren 2008 und 2009 eine breit angelegte, in ihrem Umfang bundesweit einmalige Umfrage zur Videoüberwachung durch die öffentliche Hand durch (vgl. 22. Tb., Tz. 3.2). Insgesamt wurden dabei 2.673 öffentliche Stellen in Rheinland-Pfalz befragt, zusammen mit Stichproben im privaten Bereich, etwa bei Tankstellen und Sparkassen, wurden Informationen zu insgesamt mehr als 6.000 Stellen erhoben. Im Ergebnis wurden dabei mehr als 3.000 Kameras öffentlicher Stellen und mehr als 8.500

Kameras im privaten Bereich dokumentiert. Auf Basis der gut fundierten Schätzung, dass allenfalls jede zehnte Überwachungskamera sich in öffentlicher Hand befindet, ist daher für Rheinland-Pfalz von 30.000 bis 50.000 Überwachungskameras auszugehen. Diese Zahl ist im Berichtszeitraum mit Sicherheit weiter angestiegen, die Kombination aus Preisverfall und Miniaturisierung der Technik haben zwischenzeitlich dazu geführt, dass von mehr als 50.000 Überwachungskameras in Rheinland-Pfalz auszugehen ist. Dies spiegelt sich auch im weiteren Anstieg der Nachfragen und Beschwerden zu diesem Thema beim LfD wieder, etwa ein Drittel der mehr als 1.500 Eingaben an die Aufsichtsbehörde betreffen den Bereich Videoüberwachung.

Bei seinen Kontrollen stellt der LfD gerade hier gravierende Missstände fest, die häufigsten datenschutzrechtlichen Mängel finden sich im Bereich der Hinweispflichten (vgl. § 6b Abs. 2 BDSG). Häufig fehlen die Hinweisschilder ganz, regelmäßig sind sie nicht zur Kennzeichnung des Überwachungsbereichs, sondern unterhalb der Kamera angebracht; in vielen Fällen fehlt zudem der vorgeschriebene Hinweis auf die verantwortliche Stelle. Regelmäßig fehlen auch Videoüberwachungskonzepte, welche vor Inbetriebnahme der Anlage verpflichtend zu erstellen sind (vgl. § 6b Abs. 1 Nr. 3, Abs. 3 BDSG). Insbesondere fehlt es häufig an der Festlegung bestimmter Zwecke der Videoüberwachung, die eine aufsichtsbehördliche Kontrolle der Rechtmäßigkeit der Videoüberwachung erst ermöglichen. Wird Videoüberwachung in Form der Aufzeichnung betrieben, so finden sich regelmäßig Verstöße gegen die Höchstspeicherdauer der Videoaufzeichnung. Eine Überschreitung der maximalen Grenze von 48 Stunden Speicherdauer führt regelmäßig zur Unverhältnismäßigkeit der Videoüberwachung (vgl. Tz. II-2.2.2).

Oft ist die Videoüberwachung sinnvoll, etwa in Parkhäusern, Supermärkten und wohl auch in Bahnhöfen. Allerdings breitet sie sich weiter in rasantem Tempo und weitgehend unkontrolliert aus – auch in Bereichen, in denen man sich bisher unbeobachtet aufhalten konnte, wie etwa in Arztpraxen oder in der Gastronomie, im Schienennahverkehr und in der privaten Nachbarschaft.
Der LfD hat deshalb strengere gesetzliche Vorraussetzungen für die Zulässigkeit der Videoüberwachung gefordert und dem Parlament hierzu entsprechende Vorschläge unterbreitet. Im staatlichen Bereich wurden den Behörden Orientierungshilfen an die Hand gegeben, um eine rechtskonforme und zurückhaltende Anwendung der Videoüberwachung zu ermöglichen. Noch wichtiger ist es aber, dass die Bürgerinnen und Bürger mit offenen Augen durch ihren Alltag gehen und nicht klaglos akzeptieren, wenn in ihrer Eisdiele, im Schwimmbad, in Toilettenbereichen oder im Zug nach Hause Videokameras installiert werden.

### Schlussfolgerungen des LfD

Den Vorteilen der Videoüberwachung insbesondere bei der Diebstahlsvorbeugung und ihrem (beschränkten) Nutzen zur Aufklärung von Straftaten stehen erhebliche Nachteile gegenüber: Zu nennen ist hier insbesondere der Überwachungs- und Anpassungsdruck, der durch die Videoüberwachung entsteht; neben der Gefahr eines allgemeinen Voyeurismus ist durch die Installation von Videoüberwachungsanlagen auch eine Lähmung der Hilfsbereitschaft und des Verantwortungsgefühls in der Bevölkerung zu beobachten. Positive Wirkungen der Videoüberwachung werden häufig dadurch gemindert, dass bloße Verlagerungseffekte auftreten, außerdem ist eine zweckmäßig durchgeführte Videoüberwachung technisch anspruchsvoll und äußerst kostspielig.

Insgesamt lässt sich die Videoüberwachung daher datenschutzrechtlich wie folgt bewerten:

- Jede Videoüberwachung ist ein Eingriff in das Persönlichkeitsrecht, denn alle Menschen haben das Grundrecht, sich in der Öffentlichkeit zu bewegen, ohne dass ihr Verhalten durch Kameras aufgezeichnet wird.
- Die Videoüberwachung erfasst unvermeidbar völlig unverdächtige Menschen mit ihren individuellen Verhaltensweisen.
- Daher ist Videoüberwachung immer begründungsbedürftig und darf nur offen erfolgen, sie ist stets auf das notwendige Maß zu beschränken und bedarf in zeitlicher Hinsicht der regelmäßigen Überprüfung (jährliche Evaluationspflichten).
- Vor der Einrichtung einer Videoüberwachung müssen alle Alternativen hierzu geprüft und bewertet werden. Videoüberwachung kann nur die ultima ratio sein.
- Jede Einrichtung einer Videoüberwachung muss der datenschutzrechtlichen Vorabkontrolle unterzogen werden (§ 4d Abs. 5 BDSG), gleichzeitig ist die Berufung eines behördlichen bzw. betrieblichen Datenschutzbeauftragten vor Installation der Videoüberwachung verpflichtend.
- Der Zweck der Videoüberwachung muss konkret vor der Überwachung schriftlich festgelegt werden.
- Während der Videoüberwachung müssen die Zweckbindung, die differenzierte Abstufung zwischen Aufnahmearten, die deutliche Erkennbarkeit der Videoüberwachung sowie die Löschung der Daten binnen kurzer Fristen strikt und dauerhaft sichergestellt werden.
- Rechtskonforme Videoüberwachung ist planungsintensiv, kostspielig, aufwändig und nur begrenzt effektiv. Videoüberwachung ist nur bei optimaler technischer und personeller Ausführung erfolgversprechend und daher verhältnismäßig.
- Die Beweislast für die Zulässigkeit der Videoüberwachung liegt bei den Betreiberinnen und Betreibern.

- Die flächendeckende Videoüberwachung muss verhindert werden, da die Gefahr besteht, dass diese Entwicklung zu einer Überwachungsinfrastruktur führt.
- Mögliche Rechtsverletzungen können aus personellen Gründen nur unzureichend staatlich geahndet werden (Vollzugsdefizit). Effektiver Rechtsschutz der Betroffenen wird auch nicht durch die Zivilgerichte gewährt.

### 2.2.2 Videoüberwachung an Tankstellen

Eine Studie des LfD zum Einsatz von Videoüberwachungsanlagen in Rheinland-Pfalz befasste sich u.a. mit dem Einsatz dieser modernen Überwachungstechnik an Tankstellen (http://www.datenschutz.rlp.de/de/presseartikel.php?pm=pm2009071501). Nach dem Ergebnis dieser Studie findet an nahezu allen Tankstellen in Rheinland-Pfalz eine regelmäßig flächendeckend ausgebaute Videoüberwachung mit teilweise bis zu zehn Kameras und mehr statt. Soweit sich diese Videoüberwachung nicht auf den Tankbereich beschränkt, findet auch eine Überwachung der Kundinnen und Kunden in den Tankstellenshops statt; hier ist auch eine Überwachung der Mitarbeiterinnen und Mitarbeiter möglich.

Wegen dieser „alltäglichen“ Videoüberwachung an Tankstellen wendete sich der LfD im Januar 2010 an die mehr als 750 Tankstellenbetreiberinnen und -betreiber in Rheinland-Pfalz und informierte sie über ihre Rechtspflichten als „verantwortliche Stellen“ nach dem Bundesdatenschutzgesetz.

Soweit Tankstellenbetreiberinnen und -betreiber sich durch den Einsatz von Videoüberwachungstechnik vor Benzin- und Ladendiebstählen schützen wollen, handelt es sich dabei um durchaus berechtigte und schützenswerte Interessen. Allerdings darf diese Videoüberwachung nur im Einklang mit dem Gesetz, hier insbesondere mit dem Bundesdatenschutzgesetz stattfinden. Einschlägig ist nicht nur § 6b BDSG, welcher die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen regelt, sondern auch § 4d BDSG, welcher Meldepflichten sowie die besondere Pflicht einer datenschutzrechtlichen Vorabkontrolle (§ 4d Abs. 5 BDSG) in sensiblen Bereichen vorsieht. Die außerordentliche Intensität der Videoüberwachung bringt für die Tankstellen insbesondere die gesetzliche Verpflichtung mit sich, sehr sorgsam und korrekt bei der Erhebung, Speicherung und Nutzung der Videoaufnahmen vorzugehen. Dabei geht es nicht um einen Formalismus, sondern um den Schutz der Bürgerrechte von Kundinnen und Kunden sowie Mitarbeiterinnen und Mitarbeitern.

Bereits die Videoüberwachung von Zapfsäulen zur Verhinderung von Benzindiebstählen stellt eine solche besonders risikoreiche Form der Datenverarbeitung dar, da per Videoüberwachung das Verhalten der Kundinnen und Kunden analysiert und gespeichert wird (§ 4d Abs. 5 Satz 2 Nr. 2 BDSG). Hierfür sieht das Gesetz zwingend eine sog. Vorabkontrolle vor, für die gemäß § 4d Abs. 6 BDSG betriebliche Beauftragte für den Datenschutz zuständig sind. Solche betrieblichen Datenschutzbeauftragte sind gem. § 4f Abs. 1 Satz 6 BDSG unabhängig von der Größe und Beschäftigtenzahl der verantwortlichen Stelle zu bestellen. Mit ihrer Bestellung soll sichergestellt werden, dass die Verantwortlichen im Unternehmen durch eine Datenschutzfachkraft bei der Umsetzung der durchaus komplexen Materie des Datenschutzes unterstützt und beraten werden. Die Datenschutzbeauftragten sollen die zentrale Anlaufstelle für alle Belange des Datenschutzes im Betrieb sein. Gemäß § 4f Abs. 2 BDSG darf hierzu nur bestellt werden, wer die zur Erfüllung der Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Es kann auch eine Person außerhalb der verantwortlichen Stelle mit dieser Aufgabe betraut werden.

Nach Eingang der Rückmeldungen durch die Tankstellenbetreiberinnen und -betreiber ergab sich für den LfD das folgende Bild: Die aktuell intensivste und nahezu flächendeckende Form der Videoüberwachung in Rheinland-Pfalz findet zur Zeit an den Tankstellen statt. Dort wird nicht nur der gesamte Tankvorgang – häufig mit einer Vielzahl von Kameras – auf höchstem technischen Niveau aufgezeichnet, hier wird auch in den angeschlossenen Ladenshops und insbesondere im Kassenbereich der Tankstellen massiv videoüberwacht. Ziel dieser Videoüberwachung ist dabei immer die Identifizierung der Kundinnen und Kunden – unabhängig davon, ob sie sich auffällig oder völlig normal benehmen. Je nach Zahlungsart werden zu den Videoaufzeichnungen an den Tankstellen dann auch noch Bankverbindungs- und Kreditkartendaten hinzu erhoben, um das Verhalten von Kundinnen und Kunden detailliert dokumentieren zu können.

Eine zulässige Videoüberwachung bedarf des datenschutzrechtlichen Sachverstandes. Hier sind die einzelnen Tankstellenbetreiberinnen und -betreiber häufig überfordert. Besonders ärgerlich war aus Sicht des LfD, dass viele Mineralölkonzerne, obwohl sie selbst die Komplettausstattung der Tankstellen mit Videoüberwachungsanlagen durchführten, die Verantwortung für deren Betrieb allein bei den einzelnen Tankstellenpächterinnen und -pächtern sehen. Eine solche Position verhinderte aus Sicht des LfD eine Tankstellen übergreifende Gesamtlösung der Problematik. Die Aufsichtsbehörde sah sich so gezwungen, sich mit nahezu jeder einzelnen Tankstelle in Rheinland-Pfalz auseinanderzusetzen.

Einzelne Mineralölkonzerne verhielten sich allerdings von Anfang an kooperativ und verantwortungsvoll. In Kooperation mit dem LfD suchten – und fanden – sie datenschutzgerechte und zweckmäßige Lösungen: So erwies es sich für die Aral AG als gangbarer Weg, das eigene Bezirksleiternetz für die datenschutzkonforme Ausgestaltung der Videoüberwachung zu nutzen. Dem hat sich mittlerweile auch ConocoPhillips angeschlossen, im Herbst 2011 hat auch Shell damit begonnen, im eigenen Netz ein adäquates Datenschutzkonzept anzubieten.

Die „Aktion Tankstelle“ ist also auf gutem Weg. Mittlerweile haben viele Tankstellenpächterinnen und -pächter betriebliche Datenschutzbeauftragte bestellt, um die Videoüberwachung auf legale Füße zu stellen. Wo das Know-how fehlt, unterstützt der LfD die Betreiberinnen und Betreiber durch Fortbildungsangebote, die etwa in Kooperation mit der Industrie- und Handelskammer Koblenz angeboten werden. Berichte in Fachmagazinen wie dem „tankstellen markt“ und Kooperationen mit Tankstellenverbänden wie dem Deutsch-Österreichischen Tankstellenverband, mit dem eine „Checkliste Videoüberwachung an Tankstellen“ erarbeitet wurde, runden das Beratungsangebot des LfD ab. So kann Datenschutz pragmatisch umgesetzt werden: Mit Nachdruck, wenn es um die Aufklärungsarbeit geht – aber immer auch kooperativ, wenn die verantwortlichen Stellen ihre Pflichten erkannt haben.

## 2.3 Veröffentlichung von Agrarsubventionen

Im Datenschutzbericht 2008/2009 (vgl. 22. Tb., Tz. 5.7) war bereits darauf hingewiesen worden, dass der LfD die Veröffentlichung der Empfängerinnen und Empfänger von Agrarsubventionen im Internet mit Namen, Wohnort sowie Art und Höhe der Fördermittel beanstandet hatte, auch gegenüber dem Oberverwaltungsgericht, das sich wie andere Gerichte auch mit dieser Angelegenheit zu befassen hatte. Allerdings war das Oberverwaltungsgericht nicht der Auffassung des LfD gefolgt und hatte die Veröffentlichung im Internet zugelassen. Mit Urteil vom 9. November 2011 entschied dann der Europäische Gerichtshof zugunsten der Landwirtinnen und Landwirte. Die Veröffentlichung von Subventionsdaten natürlicher Personen im Internet sei unrechtmäßig, und die entsprechenden Vorschriften seien ungültig. Der Europäische Gerichtshof macht in seinem Urteil deutlich, dass Veröffentlichungen im Internet nicht einseitig die Ziele der Veröffentlichung berücksichtigen dürfen, sondern vielmehr in ausgewogener Gewichtung auch die Rechte der von der Veröffentlichung Betroffenen zu berücksichtigen haben. Die mit der Veröffentlichung von Subventionsdaten verfolgte Transparenz bei der Verwendung von Gemeinschaftsmitteln ist ein wichtiger und im europäischen Verfassungsrecht verankerter Grundsatz. Durch Transparenz soll eine stärkere öffentliche Kontrolle der verwendeten Mittel ermöglicht und damit die Wirtschaftlichkeit der Haushaltsführung verbessert werden. Diesem Gebot stehen allerdings bei einer Internetveröffentlichung die Rechte der betroffenen Subventionsempfängerinnen und -empfänger gegenüber. Die Internetveröffentlichung greift in das verfassungsmäßig garantierte Recht jeder natürlichen Person auf Schutz der sie betreffenden personenbezogenen Daten ein. Dieses Recht kann zwar eingeschränkt werden, allerdings muss die Einschränkung gesetzlich vorgesehen sein, sein Wesensgehalt geachtet werden und die Einschränkung unter Wahrung des Grundsatzes der Verhältnismäßigkeit erforderlich sein.

Dass die Regelungen zur Internetveröffentlichung von Agrarsubventionsdaten Ausfluss einer verhältnismäßigen Abwägung zwischen den Transparenzzielen auf der einen und den Interessen der Betroffenen auf der anderen Seite sind, vermochte der Europäische Gerichtshof nicht festzustellen.

Insbesondere war den Vorschriften nicht zu entnehmen, dass die erfolgte uneingeschränkte Veröffentlichung zur Erreichung des Ziels erforderlich war. Ein transparentes und wirklichkeitsgetreues Bild der Verwendung von Subventionsgeldern ließe sich nach Einschätzung des Europäischen Gerichtshofs auch durch eine beschränkte Veröffentlichung erreichen (Urteil des Europäischen Gerichtshofs vom 9. November 2010, Az. C-92/09, C-93/09; vgl. Tz. I-2.1.2).

## 2.4 Datenschutz und Anti-Doping-System

Eine Reihe von Spitzensportlerinnen und -sportlern hat sich im Herbst 2010 an den LfD mit der Bitte gewandt, sie bei der Wahrung ihrer Persönlichkeitsrechte mit Blick auf Anti-Doping-Kontrollmaßnahmen zu unterstützen. Ihre Unterwerfung unter den Nationalen Anti-Doping-Code der Nationalen Anti-Doping-Agentur Deutschland (NADA) führe zu einer unerträglichen Verletzung ihrer Intim- und Privatsphäre. Auf Grundlage umfangreicher und sehr detaillierter Darstellungen der Anti-Doping-Kontrollpraxis hat der LfD im Rahmen seiner gesetzlichen Aufgaben eine datenschutzrechtliche Bewertung des Nationalen Anti-Doping-Codes 2009 vorgenommen.

Hierbei kam er zum Ergebnis, dass sich die Kontrollmaßnahmen nicht auf wirksame Einwilligungserklärungen der Sportlerinnen und Sportler stützen können. Eine freie Entscheidung der Betroffenen im Sinne von § 4a Abs. 1 Satz 1 BDSG liegt offensichtlich nicht vor. Im Rahmen ihrer gewählten beruflichen Betätigung als Profisportlerin

oder -sportler hängt ihre berufliche Existenz davon ab, bei nationalen oder internationalen Wettkämpfen startberechtigt zu sein. Die Erteilung einer solchen Startberechtigung wird über die beteiligten Vereine bzw. Sportfachverbände von der Unterwerfung unter den Nationalen Anti-Doping-Code abhängig gemacht; die Verweigerung der Teilnahme am internationalen Anti-Doping-Kampf führt notwendig zum Ausschluss von Veranstaltungen im Sportbereich und kommt damit im Ergebnis einem Berufsverbot gleich. Den Athletinnen und Athleten, die sich gegen die „freiwillige" Teilnahme am Anti-Doping-System entscheiden, wird damit die wirtschaftliche Lebensgrundlage entzogen. Auf dieser Basis von einer freien Entscheidung der Athletinnen und Athleten zu sprechen, wäre sachfremd.

Einer wirksamen Einwilligung steht zudem in den Fällen, in denen die Athletinnen und Athleten sich als Beschäftigte im Sinne von § 3 Abs. 11 BDSG betätigen, die fehlende Einwilligungsfähigkeit der Betroffenen entgegen. Im Bereich des Arbeitnehmerdatenschutzes ist seit langem sowohl arbeitsgerichtlich als auch datenschutzrechtlich anerkannt, dass aufgrund des erheblich sozialen Gefälles und der unterschiedlichen wirtschaftlichen Handlungsmöglichkeiten der Vertragsparteien der erklärten Einwilligung von Beschäftigten keine rechtfertigende Funktion zukommen kann. Im Rahmen vorgefundener arbeitsvertraglicher Konstellationen steht den Beschäftigten regelmäßig nicht die Möglichkeit offen, ihre berechtigten Interessen einschließlich ihrer Persönlichkeitsrechte im Rahmen von Vertragsgestaltungen wirksam durchzusetzen. Aus diesem Grund hat der Bundesgesetzgeber im laufenden Gesetzgebungsverfahren zur Novellierung des Bundesdatenschutzgesetzes die Einwilligungsfähigkeit von Beschäftigten grundsätzlich ausgeschlossen (vgl. § 32l Abs. 1 BDSG-Entwurf, BR-Drs. 535/10) und lässt solche nur im Rahmen ausdrücklicher gesetzlicher Bestimmungen zu.

Mangels wirksamer Einwilligung sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch Anti-Doping-Organisationen damit nur zulässig, soweit sie durch das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift ausdrücklich erlaubt sind. Da der Bundesgesetzgeber bisher davon Abstand genommen hat, ein Anti-Doping-Gesetz zu erlassen, welches insbesondere auch die Persönlichkeitsrechte der Athletinnen und Athleten zu schützen bestimmt wäre, kann eine hinreichende Rechtsgrundlage für die datenverarbeitenden Vorgänge der Anti-Doping-Organisationen nur im Bundesdatenschutzgesetz selbst gefunden werden. Dem Welt-Anti-Doping-Code kommt mangels innerstaatlicher Verbindlichkeit als Rechtsvorschrift i.S.v. § 4 Abs. 1 BDSG insoweit keine Bedeutung zu.

Auf Grundlage der vorliegenden Statuten und Standards der NADA lässt sich jedoch die Sachlage klären, ob Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Verarbeitung und der Nutzung überwiegt, ob also insbesondere die Persönlichkeitsrechte der Athletinnen und Athleten dem Vollzug des Nationalen Anti-Doping-Codes entgegenstehen.

Aus den vielfältigen Beeinträchtigungen der Persönlichkeitsrechte der Athletinnen und Athleten durch ihre Unterwerfung unter den Nationalen Anti-Doping-Code lassen sich sechs besonders augenfällige Problembereiche herausgreifen:

- Die Meldepflichten gem. Art. 5.3 NADC,
- die Durchführung der Doping-Kontrollen gem. Art. 5.4 NADC,
- Datenübermittlungen zwischen Anti-Doping-Organisationen nach Art. 14.1 NADC,
- Meldungen an staatliche Ermittlungsbehörden gem. Art. 14.2 NADC,
- Veröffentlichungen personenbezogener Daten der Sportlerinnen und Sportler gem. Art. 14.3 NADC
- sowie die Verwertung erhobener Daten für Maßnahmen mit Sanktionscharakter.

Insgesamt lässt sich daher feststellen, dass der Nationale Anti-Doping-Code in vielfältiger Weise in überwiegende schutzwürdige Interessen der Betroffenen eingreift, was eine datenschutzrechtliche Rechtfertigung der Datenerhebung und -verarbeitung nach § 28 Abs. 1 Nr. 2 BDSG ausschließt. Mangels rechtlicher Grundlage der Datenerhebungen und -verarbeitung der Anti-Doping-Organisationen sind diese damit als rechtswidrig einzustufen.

Erste im Dezember 2010 geführte Gespräche mit der NADA, zu dem der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen eingeladen hatte, verliefen konstruktiv und weiterführend. Die Datenschützer erkannten durchaus an, dass die NADA bereits in der Vergangenheit gezeigt habe, dass ihr der Datenschutz ein Anliegen ist. Darüber hinaus wurde deutlich, dass ihr an einer weiteren Verbesserung des Datenschutzes liegt. Die NADA machte bereits im ersten Gespräch ihre Bereitschaft deutlich, dem Schutz von Jugendlichen künftig noch mehr Gewicht beizumessen. Sie ließ darüber hinaus erkennen, dass künftig eine Vertreterin bzw. ein Vertreter der Datenschutzbeauftragten in die nationalen Beratungen zur Novellierung des Welt-Anti-Doping-Codes eingebunden werde. Dies schließe die Arbeit an der Modifizierung der Meldepflichten der Athletinnen und Athleten ein. Einigkeit bestand auch darüber, das bei der NADA vorhandene

Ombudssystem zu verbessern und zu einer Anlaufstelle für die Sportlerinnen und Sportler auszubauen.

Im Juli 2011 forderten die Landesdatenschutzbeauftragten von Schleswig-Holstein und Rheinland-Pfalz vom Gesetzgeber auf Bundesebene, ein Gesetz zum Anti-Doping-System in Angriff zu nehmen, das die Privatsphäre der Sportlerinnen und Sportler bei Doping-Kontrollen sichert. Die Datenschutzbeauftragten kamen in einer Analyse des Anti-Doping-Verfahrens in Deutschland zu dem Ergebnis, dass das von der NADA und der Welt-Anti-Doping-Agentur geregelte und praktizierte Verfahren grundlegenden Anforderungen des Datenschutzes nicht genügt (https://www.datenschutzzentrum.de/allgemein/20110726-positionspapier-dopingbekaempfung.html): Die Pflicht, die tägliche Erreichbarkeit für Anti-Doping-Kontrollen über das in Kanada beheimatete Internetsystem „ADAMS“ jeweils drei Monate im Voraus als sog. „Whereabouts“ sicherzustellen, ist unverhältnismäßig und verletzt grundlegende Datenschutzprinzipien. Die Sicherheit und Vertraulichkeit dieser sensiblen Daten sowie die Verantwortlichkeit hierfür ist nicht gewährleistet. Die Art und Weise der konkret praktizierten Anti-Doping-Kontrollen ist zu weitgehend und schießt teilweise über das berechtigte Ziel, Doping zu verhindern, hinaus. Die geforderten Unterwerfungserklärungen der Sportlerinnen und Sportler unter diese Kontrollmaßnahmen sind rechtlich nicht akzeptabel.

Die beiden Datenschutzbeauftragten schlugen daher vor, das Doping-Bekämpfungsverfahren gesetzlich zu regeln und hierbei sicherzustellen, dass dem Datenschutz und den Belangen der Betroffenen durch eine konsequente Anwendung des Verhältnismäßigkeitsgrundsatzes Rechnung getragen wird, auch durch die Einbeziehung von Sportlervertretungen bei der Erarbeitung der Bekämpfungskonzepte.

Die Datenschutzbeauftragten Thilo Weichert und Edgar Wagner erläuterten ihren Vorstoß wie folgt:

> „Die Sportler stehen vor einem durch sie nicht lösbaren Dilemma: Entweder sie verzichten auf die Wahrung ihrer grundrechtlich gewährleisteten Privatsphäre und können an internationalen Wettkämpfen teilnehmen oder sie pochen auf ihre Rechte und werden ausgeschlossen. Mit einem Gesetz zum Anti-Doping-System kann und muss der Zielkonflikt zwischen sauberem Sport und Schutz der Privatsphäre zu einem gerechten Ausgleich gebracht werden. Bisher entziehen sich die Sportfunktionäre und die Politik ihrer Fürsorgepflicht. Nur über ein Gesetzgebungsverfahren kann zudem der politische Druck gegenüber den internationalen Sportverbänden und der Welt-Anti-Doping-Agentur aufgebaut werden, dass auch dort ein vertretbarer Mindeststandard beim Datenschutz eingehalten wird.“

In der Folgezeit geriet das Doping-Kontrollsystem immer stärker unter Druck. So kommt ein von der deutschen Basketballspielervereinigung SP.IN beim Frankfurter Arbeits- und Datenschutzrechtler Prof. Wedde eingeholtes Gutachten (http://www.spinbb.net/uploads/media/Wedde_-_Gutachten_fu__r_SP.IN_per_5.9.2011.pdf) ebenfalls zum Ergebnis, dass das bestehende Anti-Doping-System die Rechte der Sportlerinnen und Sportler als Arbeitnehmerinnen und Arbeitnehmer gravierend verletzt.

In einer Anhörung des Sportausschusses des Deutschen Bundestages im Oktober 2011 konnte der LfD seine bisherige Kritik am Doping-Kontrollsystem der NADA erläutern. Er verwies dabei auf die besondere Problematik, dass es sich beim Doping-Kontrollsystem wegen des bestimmenden finanziellen und strukturellen Einflusses des Bundesinnenministeriums auf die NADA um ein quasi „staatliches Überwachungssystem“ handele. Von Seiten der NADA wurde eingeräumt, dass auch sie datenschutzrechtliche Probleme sehe, etwa bei der Speicherung von Sportlerdaten über acht Jahre hinweg. Der vom Bundesinnenministerium favorisierte Lösungsansatz, das Doping-Kontrollsystem zukünftig dadurch rechtmäßig zu gestalten, dass man sich auf internationaler Ebene um die Änderung der Doping-Kontrollregeln bemühe, reicht jedoch aus Sicht des Datenschutzes nicht aus.

Hierzu führte der LfD vor dem Bundestag aus:

> „Die Grundrechte und das deutsche Datenschutzrecht gelten nicht nach Belieben internationaler Organisationen wie der Welt-Anti-Doping-Agentur, sondern unbedingt. Auch Sportler sind daher keine Grundrechtsträger zweiter Klasse. So wichtig die internationale Koordinierung des Anti-Doping-Kampfes auch ist, sie findet ihre Grenzen an unserer Verfassung.“

Auch wenn sich das Innenministerium großen Einfluss auf die Welt-Anti-Doping-Agentur zuschreibe, bliebe doch fraglich, ob sich international der hohe deutsche Datenschutzstandard durchsetzen lasse.

Daher begrüßt der LfD die von der Bundestagsfraktion Bündnis 90/Die Grünen angekündigte Gesetzesinitiative zur Sicherung der Persönlichkeitsrechte von Sportlerinnen und Sportlern im Doping-Kontrollsystem. Gleichzeitig müsse unter Beteiligung der Betroffenen intensiv an der Suche nach Alternativen zum vorgeblich „alternativlosen“ Anti-Doping-System gearbeitet werden.

# 3. Verbraucherschutz und Beschäftigtendatenschutz

## 3.1 Verbraucherschutz

### 3.1.1 RFID – Datenschutz darf nicht verpasst werden

Die RFID-Technnologie stellt wie der Barcode eine Möglichkeit zur automatischen Identifikation dar. Hierbei werden Daten auf einem Chip (auch „tag“ genannt) mittels Funkwellen von einem Lesegerät kontaktlos ausgelesen. Die Chips sind mittlerweile so unscheinbar, dass sie an den Produkten nicht mehr auffallen. Mit Hilfe des auf dem Chip gespeicherten einzigartigen Produktcodes kann das Produkt auf der ganzen Welt individuell erkannt werden.

Wurde RFID-Technik zunächst nur im Logistikbereich eingesetzt, sind Verbraucherinnen und Verbraucher heute oft unmittelbar davon betroffen. So wird die Technik z.B. in elektronischen Schlössern, Zutrittskontrollen, elektronischen Wegfahrsperren, Skipässen, in Bibliotheken, dem Reisepass oder Personalausweis, in der Gesundheitsversorgung und in der Textilindustrie eingesetzt. RFID bietet Vorteile. So kann ihr Einsatz z.B. Produktionskosten senken und Bezahlsysteme beschleunigen. Außerdem sind Waren eindeutig identifizierbar und damit rückverfolgbar.

Wie bereits im letzten Datenschutzbericht dargestellt, birgt die unbemerkte Identifikation aber auch Gefahren – insbesondere bei Produkten (z.B. Kleidungsstücken), die ohne klare Kennzeichnung mit RFID ausgestattet sind (vgl. 22. Tb., Tz. 6.1.1). Wie sollen Betroffene feststellen, was erhoben wird, wer die Daten speichert, wozu sie verwandt werden und ob auch andere Personen sie erhalten? Die unbemerkt erhobenen Daten könnten einzelnen Verbraucherinnen und Verbrauchern zugeordnet oder mit ihren sonstigen Daten verknüpft werden. Hierdurch würden Verbraucherinnen und Verbraucher zu gläsernen Menschen. Jedes Mal, wenn sie mit einem Chip in den Bereich eines Lesegerätes treten, würden sie erkannt. So ergäben sich wie bei einer Kameraüberwachung Profile über ihre Bewegungen und ihr Konsum- und Nutzungsverhalten.

Diese Problematik ist auf Bundes- und europäischer Ebene seit Jahren genauso bekannt wie der daraus folgende Handlungsbedarf. Dementsprechend hat die Kommission der Europäischen Union bereits am 12. Mai 2009 den Mitgliedsstaaten einen Maßnahmenkatalog für den datenschutzkonformen Einsatz der RFID-Technologie empfohlen (Empfehlung 2009/387/EG). Diese Empfehlung wurde vom LfD in den bereits am 25. August 2008 gemeinsam mit dem Ministerium für Verbraucherschutz und Vertreterinnen und Vertretern aus Wirtschaft und Verwaltung begonnenen Verbraucherdialog als Diskussionsgrundlage übernommen.

Einigkeit wurde dabei erzielt, dass die Forderungen der Kommission nach einem Datenschutzkonzept, nach mehr Informationen für Verbraucherinnen und Verbraucher sowie nach einer Kennzeichnung der Produkte und Deaktivierung der Chips umzusetzen seien. Bei den ergänzenden Forderungen im Sinne des Datenschutzes dagegen konnte mit den Vertreterinnen und Vertretern der Wirtschaft keine Einigung erzielt werden.

Nach dem Maßnahmenkatalog der EU-Kommission haben Unternehmen im Wege der Selbstverpflichtungen beim Einsatz von RFID für ein ausreichendes Schutzniveau zu sorgen. Nach Vorstellung der Kommission sollte hierzu von Unternehmerseite bis Mai 2010 zunächst ein Konzept entwickelt werden, nach dem Unternehmen vor Markteinführung eines mit RFID-Technologien versehenen Produkts zunächst eine Datenschutzfolgeabschätzung erstellen und den Aufssichtsbehörden zur Prüfung vorlegen können. Es dauerte beinahe ein Jahr länger, bis ein für die Kommission akzeptables Rahmenkonzept (PIA – Privacy Impact Assessment) vorlag. Ob Unternehmen diesen Rahmen kennen, beachten und Datenschutzfolgeabschätzungen hiernach erstellen, ist nicht bekannt. Dem LfD wurde bislang noch keine Datenschutzfolgeabschätzung eines Unternehmens vorgelegt.

Der Erfolg des Selbstverpflichtungsversuchs ist nicht nur aus diesem Grund zu bezweifeln. Die Selbstverpflichtung der Unternehmen ist nicht kontrollierbar. Es bestehen keine verbindlichen und sanktionierbaren Vereinbarungen. Die Aufsichtsbehörden haben den Einsatz von RFID weiterhin losgelöst von einer Selbstverpflichtung des Unternehmens anhand der Regelungen des Bundesdatenschutzgesetzes zu prüfen und ggf. zu sanktionieren.

Daher wurde die Bundesregierung auf Initiative der rheinland-pfälzischen Landesregierung durch den Bundesrat am 18. März 2011 (BR-Drs. 48/11) zu Recht aufgefordert, die Empfehlungen der EU-Kommision auf nationaler Ebene umzusetzen und zu konkretisieren. Allerdings hat die Bundesregierung sich hierzu nicht geäußert.

Für den Schutz der Persönlichkeitsrechte betroffener Verbraucherinnen und Verbraucher, aber auch zur Sicherheit der Unternehmen bedarf es daher nach Auffassung des LfD gesetzlicher Regelungen, welche die Empfehlungen der Kommission der Europäischen Union

vom 12. Mai 2009 beachten und dabei zumindest folgende Anforderungen erfüllen:

1. Der Einsatz von RFID-Anwendungen in verbraucherrelevanten Bereichen muss mit einem Datenschutzkonzept verbunden sein, um die Sicherheit der persönlichen Daten zu gewährleisten. Die Einhaltung dieser Vorgabe soll durch die datenschutzrechtlichen Aufsichtsbehörden kontrollierbar und sanktionierbar sein.
2. Mit RFID-Technologie versehene Produkte sind mit einem einheitlichen, für Verbraucherinnen und Verbraucher gut erkennbaren Logo zu kennzeichnen. Die Kennzeichnung hat grundsätzlich am Produkt zu erfolgen. Die Verantwortlichkeit für die Kennzeichnung trägt der Betreiber.
3. Die Betreiber haben eine kurze und leicht verständliche Information auszuarbeiten und zu veröffentlichen, in der mindestens Name und Anschrift des Anbieters, Zweck der Anwendung, die Art der verarbeiteten Daten, eine Zusammenfassung der Datenschutzfolgeabschätzung sowie die wahrscheinlichen Risiken aus der Anwendung der RFID-Technologie sowie Maßnahmen zur Risikominderung enthalten sind. Auf diese Information ist hinzuweisen; sie ist leicht zugänglich bereit zu halten.
4. Mit einem einheitlichen und gut sichtbaren Zeichen sind Verbraucherinnen und Verbraucher auf das Vorhandensein und den Standort von Lesegeräten aufmerksam zu machen.
5. Vorgänge, die eine Verarbeitung der Daten auf den RFID-Chips auslösen, müssen optisch oder akustisch erkennbar gemacht werden.
6. Durch technische Schutzvorkehrungen ist zu verhindern, dass die auf den RFID-Chips gespeicherten Daten von Unbefugten ausgelesen werden können.
7. Die Verknüpfung der auf den RFID-Chips gespeicherten Daten mit anderen personenbezogenen Daten ohne Einwilligung ist durch technische Schutzvorkehrungen zu verhindern.

### 3.1.2 Umsetzung der Scoringnovelle

Mit der sog. Scoringnovelle des Bundesdatenschutzgesetzes wurden die Rechte der Verbraucherinnen und Verbraucher erheblich gestärkt. Auch der LfD und die Verbraucherschutzorganisationen haben einiges getan, um die Neuerungen bekannt zu machen und die Verbraucherinnen und Verbraucher aufzufordern, von ihren neuen Rechten Gebrauch zu machen und so aktiv Datenschutzbewusstsein zu zeigen. So hat der LfD zusammen mit der rheinland-pfälzischen Verbraucherzentrale und dem hiesigen Ministerium für Umwelt, Forsten und Verbraucherschutz die Informationsbroschüre „Scoring – Sind Sie kreditwürdig?“ aufgelegt (abrufbar auch unter http://www.datenschutz.rlp.de/de/service.php?submenu=mat). Darüber hinaus haben die Verbraucherzentralen die Adressen der großen deutschen Auskunfteien veröffentlicht und ein Musterschreiben für den Antrag auf Auskunftserteilung bereit gestellt, um den Zugang zu den Informationen zu erleichtern.

In diesem Zusammenhang hatte sich eine genannte Stelle gegen die Einordnung als Auskunftei durch die Verbraucherzentrale gewehrt. Es handelte sich bei dieser Stelle um einen Verein mit Sitz in Rheinland-Pfalz, so dass der LfD auf Bitte der Verbrauchzentrale überprüfte, ob es sich hierbei um eine Auskunftei handelte.

Zweck dieses Vereins ist es, Vermieterinnen und Vermieter zu beraten. Als eine Leistung wird angeboten, wirtschaftliche Informationen über potentielle Mieterinnen und Mieter einzuholen, also sog. Bonitätsabfragen durchzuführen, die in der Regel auch mit einem Scoringwert verknüpft sind. Dabei stellte sich heraus, dass der Verein selbst keine Daten über mögliche Mieterinnen und Mieter vorhält, sondern die Anfrage lediglich an eine bekannte Auskunftei weiterleitet, die dann die gewünschten Auskünfte erteilt.

Aber auch dieses Angebot ist an den Voraussetzungen des § 29 BDSG, der die Datenverarbeitung durch Auskunfteien regelt, zu messen. Denn letztlich hat die „Vermittlertätigkeit“ des Vereins dieselben Auswirkungen auf die Betroffenen, wie sie direkte Vermieterabfragen bei der Auskunftei hätten. Maßstab der datenschutzrechtlichen Bewertung ist dabei, dass die datenschutzrechtlichen Belange der abgefragten Mietinteressentinnen und -interessenten, also der Betroffenen, auch bei diesem Geschäftsmodell gewahrt bleiben. Dies bedeutet konkret:

- Durch den Verein muss sichergestellt sein, dass seine Kundinnen und Kunden, also die Vermieterinnen und Vermieter wissen, in welchen Fällen sie berechtigt sind, Bonitätsauskünfte einzuholen. Der Verein kann sich hierbei am Beschluss („Bonitätsauskünfte über Mietinteressenten nur eingeschränkt zulässig“) des Düsseldorfer Kreises vom 22. Oktober 2009 orientieren (vgl. 22. Tb., Tz. 6.1.3).
- Kundinnen und Kunde des Vereins müssen ihre datenschutzrechtlichen Verpflichtungen gegenüber den Betroffenen kennen, z.B. die Informationspflichten im Vorfeld der Abfrage nach § 4 Abs. 3 BDSG. Da es sich bei den Kundinnen und Kunden des Vereins wohl vorwiegend um private Vermieterinnen und Vermieter handeln dürfte, die mit den Vorgaben des Bundesdatenschutzgesetzes nicht vertraut sind, muss der Verein sie auf diese Verpflichtungen hinweisen.
- Weiterhin müssen die Datenflüsse transparent sein, sowohl gegenüber den Kundinnen und Kunden des Vereins (Vermieterinnen und Vermieter) als auch

gegenüber den Betroffenen (Mietinteressentinnen und -interessenten).
- Da die Auskunftserteilung gem. § 29 Abs. 2 BDSG die Darlegung eines berechtigen Interesses voraussetzt, muss dieses von den Kundinnen und Kunden des Vereins diesem gegenüber dargelegt werden, so dass es der Verein an die Auskunftei weitergeben kann. Zudem müssen Kundinnen und Kunden des Vereins darlegen, dass Mitinteressentinnen und -interessenten zuvor über die geplante Abfrage informiert wurden.
- Wenn Betroffene eine Selbstauskunft beim Verein verlangen, muss dieser ihnen die über sie bei seiner Vertragsauskunftei gespeicherten Daten mitteilen oder mitteilen lassen und die Auskunftei als „Hintergrundauskunftei“ benennen. Dadurch wird den schutzwürdigen Belangen der Betroffenen hinreichend Rechnung getragen.

Zusammenfassend lässt sich sagen, dass auch sog. „Durchleiteauskunfteien“, wie der in Rheinland-Pfalz ansässige Verein, sicher stellen müssen, dass die Rechte der Betroffenen gewahrt werden. Der Verein hat sich dieser Rechtsauffassung angeschlossen und sorgt nunmehr auch durch Änderung seines Internetangebots für die nötige Transparenz.

### 3.1.3 Inkasso und Datenschutz

Viele Eingaben an den LfD betreffen den Geschäftsbereich Inkasso. Wer tatsächlich oder auch nur vermeintlich einen Vertrag abschließt und dafür eine Zahlung erbringen soll, muss damit rechnen, von einem Inkassobüro Post zu kriegen, wenn er – aus welchen Gründen auch immer – nicht zahlt. Viele sehen bereits dann einen datenschutzrechtlichen Verstoß, wenn die vermeintlichen Gläubigerinnen bzw. Gläubiger ein Inkassobüro mit dem Einzug der Forderung beauftragen und bei dieser Gelegenheit auch Informationen über die vermeintlichen Schuldnerinnen bzw. Schuldner übermitteln. Hier kann der LfD aber meistens nicht weiterhelfen. Zum einen kann er nicht beurteilen, ob tatsächlich ein wirksamer Vertrag zustande gekommen und eine Zahlung fällig ist. Diese Frage kann die Verbraucherzentrale beantworten. Zum anderen ist die Übergabe einer (vermeintlich) offenen Forderung an ein Inkassobüro zum Einzug mit den dazu notwendigen Informationen kein Vorgang, der datenschutzrechtlich zu beanstanden wäre.

Denn die Zulässigkeit der Übermittlung personenbezogener Daten an ein Inkassobüro richtet sich nach § 28 BDSG. Danach ist das Übermitteln personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Das berechtigte Interesse des übermittelnden Unternehmens besteht darin, dass die offene Forderung von der Schuldnerin bzw. dem Schuldner beglichen wird. Hierzu kann es sich der Hilfe Dritter, nämlich eines Inkassobüros bedienen. Dann ist es aber auch erforderlich, dass das Inkassobüro die Informationen erhält, die die Forderung begründen und die einen Einzug durch das Inkassobüro ermöglichen.

Da die Datenübermittlung der Forderungsbegleichung dienen soll, ist grundsätzlich nicht davon auszugehen, dass schutzwürdige Interessen der Betroffenen, hier der Schuldnerinnen und Schuldner, die Datenverarbeitung überwiegen. Etwas anderes kann dann gelten, wenn das Unternehmen bereits vor der Übermittlung wusste, dass die Forderung gar nicht besteht.

Datenschutzrechtlich erheblich wird die Angelegenheit aber dann, wenn das Inkassobüro Daten an eine Wirtschaftsauskunftei weitergibt, ohne dass hierfür die erforderlichen Voraussetzungen vorliegen. Denn das kann erheblichen Einfluss auf die Beurteilung der Bonität haben. Diese Voraussetzungen sind nun seit dem 1. April 2010 ausdrücklich in § 28a BDSG geregelt. Die Übermittlung personenbezogener Daten über eine Forderung an Auskunfteien ist danach nur zulässig, soweit

- die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist und
- die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder Dritter erforderlich ist und
  - die Forderung rechtskräftig festgestellt worden ist oder
  - die Forderung von den Betroffenen ausdrücklich anerkannt worden ist oder
  - eine fristlose Kündigung des zugrunde liegenden Vertragsverhältnisses aufgrund von Zahlungsrückständen möglich ist nach Unterrichtung über die bevorstehende Übermittlung oder
  - die Betroffenen die Forderung nach zweimaliger schriftlicher Mahnung nicht bestritten haben. Zwischen der ersten und der zweiten Mahnung müssen vier Wochen liegen. Zudem müssen die Betroffenen über die bevorstehende Übermittlung rechtzeitig (frühestens jedoch bei der ersten Mahnung) informiert worden sein.

Sobald also eine Forderung bestritten wird, darf der Sachverhalt nicht an eine Auskunftei übermittelt werden und

somit auch keinen Eingang in eine Bonitätsbewertung finden.

Viele Inkassobüros versuchen auch mit dem Hinweis auf mögliche negative Folgen bei der Bonität, die Betroffenen zur Zahlung zu bewegen. Hier konnte der LfD zumindest erreichen, dass eine gesetzeskonforme Formulierung im Mahnschreiben gewählt wurde. Den Betroffenen muss klar sein, dass das Gesetz die Anforderungen an eine Datenübermittlung bestimmt und nicht das Inkassobüro nach eigenem Gutdünken.

## 3.2 Beschäftigtendatenschutz

Der Schutz personenbezogener Daten in privaten wie öffentlichen Arbeitsverhältnissen bildet aus verschiedenen Gründen seit jeher einen besonderen Schwerpunkt in der Tätigkeit des LfD: Zum einen sind die betroffenen Beschäftigten in besonderer Weise darauf angewiesen, dass ihre personenbezogenen Daten im Beschäftigungsverhältnis sorgsam behandelt werden. Zum anderen belegt die Vielzahl von Eingaben gerade in diesem Bereich, dass sich viele Beschäftigte an ihrem Arbeitsplatz überwacht und kontrolliert fühlen und daher den LfD besonders häufig um Unterstützung bitten.

Dies ist auch der Grund dafür, dass der LfD die Bemühungen um eine Neufassung des Bundesdatenschutzgesetzes zur „Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses“ (vgl. Tz. I-3.1) so intensiv begleitet.

### 3.2.1 Beschäftigtendatenschutz im privaten Bereich

Ein knappes Drittel aller Eingaben an die Datenschutzaufsichtsbehörde betrifft den Bereich Beschäftigtendatenschutz. Zu den zahlreichen Problemfeldern zählen insbesondere die Videoüberwachung von Beschäftigten, der Einsatz von Ortungssystemen im Arbeitsverhältnis sowie die Kontrolle der E-Mail- und Internetnutzung am Arbeitsplatz.

#### ■ Videoüberwachung von Beschäftigten

Aufgrund der mittlerweile relativ billigen Videotechnik kommen offenbar viele Arbeitgeberinnen und Arbeitgebern auf die Idee, ihre Arbeitnehmerinnen und Arbeitnehmer am Arbeitsplatz bzw. während ihrer Tätigkeit mit oder ohne Aufzeichnung der Videobilder zu überwachen, z.B. in Bäckereien, Pflegeeinrichtungen, in der Systemgastronomie und in Einzelhandelsgeschäften. Immer häufiger werden Kameras zur gezielten Personalüberwachung eingesetzt, wobei auch Pausen- oder Umkleidebereiche ins Visier kommen. Teilweise werden Minikameras in Rauchmeldern oder in der Deckenverkleidung von Geschäften installiert. Anders als bei der Überwachung eines unbestimmten Personenkreises in öffentlich zugänglichen Räumen sind die Arbeitnehmerinnen und Arbeitnehmer im Betrieb der Arbeitgeberin bzw. dem Arbeitgeber persönlich bekannt; jede Verhaltensweise und Kommunikation unterliegt so der Kontrolle. Wer sich aber nicht sicher ist, zu welchem Zweck und wann er überwacht wird, wird versuchen, sich angepasst zu verhalten. Dieser Anpassungsdruck wird durch die wirtschaftliche Abhängigkeit der Beschäftigten von Arbeitgeberinnen und Arbeitgebern verstärkt. Für die Beschäftigten gibt es oft keine Möglichkeit, sich der Erfassung durch Kameras zu entziehen.

Arbeitgeberinnen und Arbeitgeber führen in erster Linie den Schutz ihres Personals vor Übergriffen und den Diebstahlschutz als Gründe für diese Überwachungsmaßnahmen an. Der eigentliche Grund ist aber häufig die Leistungs- und Verhaltenskontrolle der Beschäftigten durch die Geschäftsführung. Dabei kontrolliert sie auch das Verhalten ihrer Angestellten gegenüber den Kundinnen und Kunden, die korrekte Abrechnung bei Bezahlvorgängen oder die Einhaltung von Pausenzeiten. Viele solcher Kameras werden zudem heimlich installiert. Eine heimliche Kamerainstallation ist jedoch ohne ein konkretes Verdachtsmoment stets rechtswidrig (vgl. § 32 Abs. 1 Satz 2 BDSG). Darüber hinaus sind stets arbeitsrechtliche Vorgaben zu beachten. Insbesondere ist die Zulässigkeit der Überwachung am Arbeitsplatz mittels Videobeobachtung am Persönlichkeitsrecht der Beschäftigten zu messen. Bereits die Möglichkeit der jederzeitigen Überwachung erzeugt einen Überwachungsdruck, der mit dem Anspruch der Beschäftigten auf Wahrung ihrer Persönlichkeitsrechte nicht zu vereinbaren ist. Insoweit ist eine Videoüberwachung am Arbeitsplatz nur durch besondere Sicherheitsinteressen der Arbeitgeberinnen und Arbeitgeber ausnahmsweise gerechtfertigt.

Beschäftigte sollten vor Installation einer Videoüberwachungsanlage in jedem Falle schriftlich von ihrer Geschäftsführung informiert werden. Die Arbeitgeberinnen und Arbeitgeber sollten ihre Beschäftigten über den Überwachungszweck, die Speicherdauer der Bilddaten und die Zugriffsmöglichkeiten auf die Daten in Kenntnis setzen. Dieser Zugriff und damit das Sichten und Auswerten des Bildmaterials darf nur bei begründetem Tatverdacht und nur im Zusammenwirken von Geschäftsführung und Betriebsrat erfolgen.

#### ■ Einsatz von Ortungssystemen

Besonders gravierende Verletzungen des informationellen Selbstbestimmungsrechts von Mitarbeiterinnen und Mitar-

beitern kann der Einsatz von Ortungssystemen im Arbeitsverhältnis hervorrufen. Man mag in engen Grenzen ein berechtigtes Interesse der Arbeitgeberinnen und Arbeitgeber anerkennen, sich etwa über den Standort ihrer Kundendienstfahrzeuge einen Überblick zu verschaffen. Durch den Einsatz von Ortungssystemen lässt sich aber nicht nur der Standort der Fahrzeuge auf einem Monitor in den Betriebsräumen der Firma anzeigen, auch die zurückgelegten Fahrstrecken und die Fahrtunterbrechungen werden nach Ort und Zeit festgehalten, all diese Daten werden gespeichert. Dies schafft die Grundlage für den „gläsernen Mitarbeiter“, den es aus Sicht des Datenschutzes zu verhindern gilt.

### ■ Kontrolle der E-Mail- und Internetnutzung am Arbeitsplatz

Auch die Nutzung moderner Kommunikationstechnologien am Arbeitsplatz ist sehr häufig Gegenstand von Eingaben beim LfD. Bei unsachgemäßer Einrichtung der Kommunikationssysteme und bei unberechtigten Kontrollmaßnahmen der Arbeitgeberinnen und Arbeitgeber machen diese sich im Einzelfall sogar strafbar.

Umgekehrt stellt der LfD bei der Bearbeitung von Eingaben immer wieder fest, dass eine große Anzahl von Beschäftigten sich auch bei der erlaubten Nutzung von Internet oder E-Mail am Arbeitsplatz beobachtet und kontrolliert fühlen und sich – ebenso wie die Arbeitgeberseite – häufig über die Zulässigkeit ihres Verhaltens im Unklaren sind.

Eine Orientierungshilfe der Datenschutzbeauftragten des Bundes und der Länder steht hierfür zum Abruf bereit: http://www.datenschutz.rlp.de/downloads/oh/uld_oh_email_internet.pdf

## 3.2.2 Beschäftigtendatenschutz im öffentlichen Bereich

### ■ Neuerlass des Landesbeamtengesetzes

Im Zuge der Föderalismusreform sind auch im Bereich des öffentlichen Dienstrechts die Gesetzgebungszuständigkeiten zwischen Bund und Ländern neu geordnet worden. Der Bund hat mit dem Beamtenstatusgesetz vom 17. Juni 2008 von seiner Regelungskompetenz im Bereich der konkurrierenden Gesetzgebung Gebrauch gemacht. Dieses Gesetz regelt das Statusrecht für die Beamtinnen und Beamten in den Ländern und legt die beamtenrechtlichen Grundstrukturen für ergänzendes Landesrecht fest. Für das Personalaktenrecht bedeutsam sind insoweit die Regelungen in § 49 BeamtStG – Übermittlung personenbezogener Daten bei Strafverfahren – und in § 50 BeamtStG, der Grundaussagen zur Personalaktenführung trifft und den Begriff des Personalaktendatums definiert. Diese bundesrechtlichen Vorschriften gelten unmittelbar; daneben kommen die beamtenrechtlichen Bestimmungen auf Landesebene zur Anwendung.

Mit dem Landesbeamtengesetz vom 20. Oktober 2010 hat der Gesetzgeber zwischenzeitlich von seiner o.g. Regelungskompetenzen Gebrauch gemacht. Gegenüber dem Landesbeamtengesetz von 1970 sind für das Personalaktenrecht folgende Änderungen bedeutsam: Künftig kann die Personalakte ausschließlich automatisiert geführt werden; bislang war die automatisierte Datenverarbeitung auf Hilfs- und Unterstützungsfunktionen beschränkt. Das Landesbeamtengesetz regelt nur die Verarbeitung von Personalaktendaten; für sonstige personenbezogene Daten (also z.B. Sachakten, Geschäftsverteilungspläne, Telefonlisten oder personenbezogener Daten, die für Personalplanungszwecke oder Organisationsuntersuchungen verarbeitet werden) gilt § 31 LDSG. Dies gilt auch für die Daten von Bewerberinnen und Bewerbern sowie Ehemaligen. Im Bereich der Beihilfe ist die Verpflichtung, die eingereichten Unterlagen an den Beihilfeberechtigten zurückzusenden, weggefallen. Hintergrund ist die Einführung der Software „RHESCABA“ bei der Oberfinanzdirektion, mit der die eingereichten Belege eingescannt und sodann vernichtet werden. Die Aufbewahrungsfrist von Unterlagen über Beihilfe wurde verdoppelt und beträgt jetzt zehn Jahre. Grund hierfür ist der Übergang von Ersatzansprüchen Beihilfeberechtigter auf den Dienstherrn bei unrichtiger Abrechnung von Leistungserbringern. Die Möglichkeit, Ersatzansprüche geltend zu machen, soll dem Dienstherrn nicht durch eine frühzeitige Löschung der Beihilfedaten genommen werden.

Der LfD wurde im Gesetzgebungsverfahren frühzeitig beteiligt. Seiner grundlegenden Forderung, nämlich den Beschäftigtendatenschutz weitgehend in § 31 LDSG zu regeln, wurde Rechnung getragen. Die beamtenrechtlichen Bestimmungen helfen nämlich in den Fällen, in denen es nicht unmittelbar um die Personalakte geht, oftmals nicht weiter. Dies betrifft insbesondere neu aufkommende Fragen zum Personaldatenschutz, die mit dem Einsatz von Informationstechnik am Arbeitsplatz zusammenhängen. Die Verwendung der Terminologie des allgemeines Datenschutzrechts in § 31 LDSG erleichtert demgegenüber in der Datenschutzpraxis die Beurteilung von Rechtsfragen zum Personal- und Arbeitnehmerdatenschutz. Bewährt haben sich hier insbesondere die expliziten Bestimmungen zur Übermittlung von Beschäftigtendaten sowie zur Verarbeitung von Bewerberdaten (vgl. § 31 Abs. 2, 3, 5, 6 und 7 LDSG). Durch die gegenseitigen Verweise im Landesbeamtengesetz einerseits

und in § 31 LDSG andererseits ist sichergestellt, dass für alle öffentlich Bediensteten in Rheinland-Pfalz ein einheitliches Datenschutzniveau gilt.

Das neue Landesbeamtengesetz tritt als Ganzes zum 1. Juli 2012 in Kraft; das Inkrafttreten der Bestimmungen zum Gendiagnostikgesetz (§ 11 Abs. 3 LBG), zur Beihilfeakte (§ 95 LBG) und deren Aufbewahrungsfristen (§ 96 Abs. 2 Satz 2 und Abs. 3 LBG) wurde aus rechtssystematischen Gründen vorgezogen. Diese Vorschriften gelten bereits seit der Verkündung des Gesetzes am 20. Oktober 2010 (vgl. § 145 LBG).

## ■ Datenschutz im Bewerbungsverfahren

Durch die Beantwortung parlamentarischer Anfragen im Landtag (LT-Drs. 15/4176 und 15/4249) wurde deutlich, dass die Landesregierung bei Personaleinstellungen in einem beachtlichen Umfang unbeschränkte Auskünfte nach dem Bundeszentralregistergesetz (§ 41 BZRG) eingeholt hatte. Für den LfD bestand Veranlassung, sich über die Praxis bei Bewerbungen und Einstellungen im Bereich der Ressorts genauer zu informieren. In einer Besprechung mit den Zentralabteilungsleitungen wurde deutlich, dass die neuen Kräfte oft schon unmittelbar nach ihrer Einstellung in ganz unterschiedlichen Bereichen, die teilweise auch sicherheitsrelevant sein können, zum Einsatz kommen können und dass die neuen laufbahnrechtlichen Bestimmungen eine Rotation der Kräfte sogar ausdrücklich vorsehen. Der LfD wies darauf hin, dass die Erhebung personenbezogener Daten über Bewerberinnen und Bewerber an den Grundsatz der Erforderlichkeit geknüpft ist (§ 102 Abs 4 LBG; § 31 Abs. 6 LDSG). Im Regelfall reiche die Vorlage des polizeilichen Führungszeugnisses aus; der Ausnahmecharakter einer unbeschränkten Auskunft aus dem Bundeszentralregister müsse daher stärker betont werden.

Da die Verwaltungsvorschrift des Innenministeriums „Vorlage von Führungszeugnissen und Einholung von unbeschränkten Auskünften aus dem Zentralregister bei der Einstellung in den Landesdienst“ seit 2004 außer Kraft getreten ist, fasste die Zentralabteilungsleiterkonferenz auf Vorschlag des LfD einen Beschluss mit folgender Regelung:

„Den obersten Landesbehörden steht ein Auskunftsrecht aus dem Bundeszentralregister nach § 41 Abs. 1 Nr. 2 BZRG zu. Diese Auskunft kann im Rahmen von Einstellungsverfahren eingeholt werden, wenn wegen der zu übertragenden Aufgaben erhöhte Anforderungen an die persönliche Eignung der einzustellenden Person gestellt werden und ein Führungszeugnis nach § 30 BZRG nicht ausreichend ist. Dies kann insbesondere bei einer herausgehobenen Bewertung des Arbeitsplatzes oder dann der Fall sein, wenn eine erhöhte Vertrauenswürdigkeit verlangt wird. Der Zweck der Auskunft ist anzugeben; sie darf nur für diesen Zweck verwendet werden.“

# 4. Polizei

## 4.1 Novellierung des Polizei- und Ordnungsbehördengesetzes

Mit Datum vom 18. August 2010 brachte die Landesregierung den Entwurf eines Landesgesetzes zur Änderung des Polizei- und Ordnungsbehördengesetzes in den Landtag ein (LT-Drs. 15/4879). Es trat am 23. Februar 2011 in Kraft. Die Landesregierung verfolgte mit dem Gesetzentwurf ein doppeltes Ziel: Zum einen wollte sie der Polizei zum Zweck der Gefahrenabwehr neue Instrumente an die Hand geben, die im Zeitalter der extensiven Internetkommunikation notwendig erschienen. Dazu gehören insbesondere die sog. „Quellen-Telekommunikationsüberwachung“ (Quellen-TKÜ, vgl. Tz. II-8.2.5) und die Online-Durchsuchung. Zum anderen musste das Polizei- und Ordnungsbehördengesetz an die aktuelle Verfassungsrechtsprechung angepasst werden. Dies betraf in erster Linie Maßnahmen zum Schutz des unantastbaren Kernbereichs privater Lebensgestaltung bei allen in die persönliche Lebenssphäre heimlich eingreifenden Ermittlungshandlungen, Änderungen beim automatisierten Kfz-Kennzeichenabgleich und bei der Rasterfahndung.

Der LfD war intensiv in die Formulierung des Gesetzentwurfs einbezogen. Im Gesetzgebungsverfahren selbst hat er im Rahmen der vom Innenausschuss des Landtags durchgeführten Anhörung schriftlich und mündlich Stellung genommen. Seine Anliegen sind weitgehend akzeptiert worden. So wurde die bisher im Gesetz enthaltene Ermächtigung zum automatisierten Kfz-Kennzeichenabgleich aufgehoben, es wurden zahlreiche Schranken für die neu geschaffenen Maßnahmen der Quellen-TKÜ und der Online-Durchsuchung eingeführt. Besonders bedeutsam ist, dass diese Maßnahmen von einer Anordnung des Oberverwaltungsgerichts abhängig sind und dass auch ihre ordnungsgemäße Durchführung durch das Gericht zu prüfen ist.

Bis zum Schluss hat er allerdings Vorbehalte gegenüber der Regelung der Online-Durchsuchung von Computern durch die Polizei aufrecht erhalten, auch wenn die gesetzlichen Schutzvorkehrungen gegen einen missbräuchlichen bzw. extensiven Einsatz dieses Mittels ausgesprochen zahlreich und wirksam sind. So enthält das Gesetz auch keine Ermächtigung zum Betreten und Durchsuchen einer Wohnung, um eine Online-Durchsuchung vorzubereiten. Der Bedarf für ein solches Mittel schien und scheint dem LfD allerdings dennoch nach wie vor zweifelhaft zu sein; es stößt in weiten Kreisen der Bevölkerung auf Ablehnung und steigert das Misstrauen gegenüber dem Staat. In Anbetracht der Tatsache, dass bislang noch kein Fall eingetreten ist, in dem die Polizei des Landes selbst eine konkrete Notwendigkeit für eine solche Maßnahme gesehen hat, ist ernsthaft über eine Streichung dieser Befugnis nachzudenken.

Die Polizei verarbeitet sensible Daten; häufig handelt es sich um bloße Verdachtsdaten, nicht selten sind auch Daten aus der Telekommunikation betroffen. Um sicherzustellen, dass hierbei ein angemessener Sicherheitsstandard beachtet wird, wurden im Rahmen der Novellierung des Polizei- und Ordnungsbehördengesetzes auf Initiative des LfD eigene technisch-organisatorische Datenschutzregelungen in das Polizei- und Ordnungsbehördengesetz aufgenommen (§ 41a POG). Ziel ist die Sicherstellung eines adäquaten Datenschutzniveaus polizeilicher Verfahren sowie die Erhöhung der Akzeptanz und des Vertrauens der Bürgerinnen und Bürger in die Datenschutzkonformität bei der polizeilichen Verarbeitung personenbezogener Daten.

Im Zusammenhang mit der Speicherung von Telekommunikationsdaten hat das Bundesverfassungsgericht (in seiner Entscheidung zur Vorratsdatenspeicherung vom. 2. März 2010, Az. 1BvR 256/08, 1BvR 263/08, 1BvR 586/08; vgl. Tz. II-8.2.4) grundsätzlich eine getrennte Speicherung von Telekommunikationsdaten und sonstigen Daten, eine anspruchsvolle Verschlüsselung, ein gesichertes Zugriffsregime sowie eine revisionssichere Protokollierung gefordert. Ferner ist zu berücksichtigen, dass die Überlegungen der Sicherheitsbehörden dahin gehen, die Telekommunikationsüberwachung in gewissem Umfang zu zentralisieren, so dass mittelfristig von Datenbeständen bei der Polizei auszugehen ist, die vom Umfang her mit den bei einer Speicherung von Verbindungsdaten durch die Anbieter von Telekommunikationsleistungen anfallenden Datenbeständen vergleichbar sind. Um ein Auseinanderlaufen technischer Sicherheitsanforderungen zu vermeiden, verweist der neu geschaffene § 41a POG zunächst auf die allgemeinen technisch-organisatorischen Datenschutzanforderungen des Landesdatenschutzgesetzes, greift darüber hinaus jedoch die im Urteil des Bundesverfassungsgerichts und der Diskussion um die Novellierung der Technikregelungen der Datenschutzgesetze (vgl. 22. Tb., Tz. 13.3) enthaltenen Sicherheitsziele Vertraulichkeit und Integrität auf. Auf der Grundlage einer Schutzbedarfsfeststellung und einer Risikoanalyse sind die technisch-organisatorischen Maßnahmen in einem IT-Sicherheits- und Datenschutzkonzept festzulegen und in angemessenen Abständen bzw. bei Verfahrensänderung auf ihre Eignung zu überprüfen und zu dokumentieren.

Abweichend von § 9 Abs. 5 LDSG unterliegen zudem künftig alle Verfahren der Polizeibehörden und –

einrichtungen zur automatisierten Verarbeitung personenbezogener Daten einer Vorabkontrolle. Damit soll sichergestellt werden, dass Datenschutzaspekte frühzeitig berücksichtigt werden.

Ergänzend hierzu ist ein IT-Sicherheits- und Datenschutzaudit vorgeschrieben. Zwar fehlt es wie unter Tz. I-2.2 dargestellt bislang weiterhin an einer inhaltlichen gesetzlichen Regelung zum Datenschutzaudit, dies schließt jedoch nicht aus, landesintern für den Datenschutz im Polizeibereich ein Auditierungsverfahren einzuführen und dabei auf vorhandene Kriterien und Anforderungskataloge wie den Baustein 1.5 der IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik zurückzugreifen. Die Polizeibehörden und -einrichtungen sollen nunmehr die von ihnen eingesetzten Verfahren zur automatisierten Verarbeitung personenbezogener Daten sowie die dabei genutzten technischen Einrichtungen durch unabhängiges und fachkundiges Personal prüfen und bewerten lassen. Die Regelung sieht weiterhin vor, dass vorrangig auditierte Verfahren und technische Einrichtungen eingesetzt werden sollen. Als erstes polizeiliches Verfahren wurde im Auftrag des Innenministeriums das Polizeiliche Informationssystem POLIS einem Datenschutzaudit durch eine unabhängige Stelle unterzogen. Die Ergebnisse lagen bei Drucklegung noch nicht vor.

Die mit der Novellierung des Polizei- und Ordnungsbehördengesetzes neu geschaffenen Eingriffsmaßnahmen sollen durch eine unabhängig durchgeführte wissenschaftliche Untersuchung auf den Prüfstand gestellt, „evaluiert“ werden. Aufgrund der Koalitionsvereinbarung des Jahres 2011 soll die ursprünglich für 2016 vorgesehene Evaluation bereits 2013 durchgeführt werden. Der LfD hofft auf sachdienliche Erkenntnisse aus dieser Untersuchung, um allen Beteiligten eine fundierte Entscheidung dieser Frage zu ermöglichen. Insgesamt wird aus der Sicht des LfD mit dem Gesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes eine ausgewogene Balance zwischen Sicherheitsbelangen einerseits und den berechtigten Interessen und persönlichen Rechten des Einzelnen gewahrt.

## 4.2 Protokollierung im Polizeilichen Informationssystem POLIS

POLIS, das Polizeiliche Informationssystem des Landes, ist das tägliche Arbeitsmittel der Polizei, das zur Sachbearbeitung nahezu aller polizeilichen Vorgänge genutzt wird. Der LfD hatte im letzten Tätigkeitsbericht die missbräuchliche Nutzung dieses Informationssystems durch zwei Abgeordnete des rheinland-pfälzischen Landtags im Jahr 2009 dargestellt und angekündigt, das Verfahren der POLIS-Abfragen zu überprüfen und die Notwendigkeit eines verbesserten Datenschutzes zu untersuchen (vgl. 22. Tb., Tz. 7.10). Diese Prüfung hat im Berichtszeitraum stattgefunden. Hierzu wurden die Protokolldaten von insgesamt 222.000 Abfragen herangezogen. Die durchschnittliche Abfragehäufigkeit lag bei täglich ca. 7.400 Abfragen. Insgesamt spricht dies für eine eher moderate Nutzungsintensität des Verfahrens. Das Einwohnerinformationssystem EWOIS verzeichnet im Vergleich hierzu pro Monat ca. 900.000 Zugriffe, davon 60 Prozent durch die Polizei (vgl. 21. Tb., Tz. 4.2).

Bei der Auswertung wurde untersucht, inwieweit die Protokolldaten geeignet sind, Hinweise auf nicht dienstlich bedingte Zugriffe zu liefern. Da angesichts der Vielzahl polizeilicher Sachverhalte keine direkt erkennbaren „typisch missbräuchlichen“ Abfragen existieren, bestand der bei der Kontrolle verfolgte Ansatz deshalb darin, die Protokolldaten im Rahmen strukturierter Auswertungen auf Auffälligkeiten hin zu untersuchen. Folgende Prüfansätze wurden dabei verfolgt:

- Nutzerinnen und Nutzer bzw. Arbeitsplätze mit auffällig hohen Abfragezahlen,
- die Auswertung des jeweiligen Abfragegrundes,
- Abfragen nur mit Namen, jedoch ohne Geburtsdatum,
- Abfragen auf im Licht der Öffentlichkeit stehende Personen,
- Abfragen mit Platzhalterzeichen,
- Abfragen nur mit Vornamen, jedoch ohne Familienname,
- „Verwandtenabfragen“,
- „Kollegenabfragen“,
- Abfragehäufungen außerhalb der üblichen Bürozeiten.

Etwa 200 Fälle wiesen in diesem Zusammenhang Auffälligkeiten auf. Diese wurden dem Innenministerium zur weiteren Klärung übermittelt. Auch wenn in einer Reihe von Fällen kein sicherer Nachweis über den Anlass und die Erforderlichkeit der Abfragen geführt werden konnte, haben sich dabei letztlich keine Hinweise auf eine systematisch missbräuchliche Nutzung des Verfahrens ergeben. In einigen wenigen Fällen wurde allerdings festgestellt, dass Abfragen aus Neugier vorgenommen wurden. In diesen Fällen wurden förmliche Disziplinarverfahren eingeleitet.

Durch die Kontrolle des LfD hat sich weiterhin ergeben, dass die in bestimmten Fällen vorgesehene Protokollierung des Abfragegrundes und der die Abfrage veranlassenden Person seit geraumer Zeit nicht mehr aktiviert war; des Weiteren wurden Vorgaben über die Angabe des Abfragegrundes bei sog. Vertreterabfragen, d.h. Abfragen, die für Dritte vorgenommen werden, nicht beachtet.

Als Konsequenz wurde seitens des Innenministeriums für das Verfahren die vollständige und automatische Protokollierung des Abfragegrundes veranlasst, so dass dieser nunmehr für jede Abfrage erhoben wird. Zur Minimierung des Eingabeaufwands wird in den Fällen, in denen eine POLIS-Abfrage aus dem polizeilichen Vorgangsbearbeitungssystem POLADIS heraus erfolgt, automatisch das Aktenzeichen des jeweiligen Vorgangs übernommen. Damit wurde einer Empfehlung des LfD zur generellen Erfassung des Abfragegrundes und zur Erfassung von Angaben, die es erlauben, den dienstlichen Hintergrund einer Abfrage zu klären, entsprochen.

Auch mit den nunmehr getroffenen Maßnahmen können missbräuchliche Abfragen letztlich nicht verhindert werden. Angesichts der Bandbreite dienstlich begründeter Abfragen und der vielfach nur mit Teilinformationen möglichen Suche lassen sich befugte und unbefugte Abfragen nur bedingt voneinander unterscheiden. Die vollständige Protokollierung aller Abfragen sowie die Erfassung des anzugeben Abfragegrundes eröffnen im Missbrauchsfall eine bessere Aufklärungsmöglichkeit und entfalten aus Sicht des LfD präventive Wirkung. Um diese noch zu verstärken, hat der LfD empfohlen, die Protokollierung durch eine regelmäßige Stichprobenprüfung von Abfragen und strukturierte Auswertungen hinsichtlich statistisch auffälliger Abfragen zu ergänzen. Das Innenministerium ist dem gefolgt.

## 4.3 Anti-Terror-Datei

Seit 2007 wird die Anti-Terror-Datei als gemeinsame Datei der Verfassungsschutzbehörden des Bundes und der Länder einerseits und der Polizeibehörden von Bund und Ländern andererseits geführt (vgl. 21. Tb., Tz. 5.4). Über die dagegen gerichtete Verfassungsbeschwerde hat das Bundesverfassungsgericht bislang noch nicht entschieden.

Alle statistischen Aussagen über die praktische Nutzung und die konkrete Eignung dieser Datei im Land unterliegen zur Zeit der Geheimhaltung; die insoweit von der Landesregierung dem LfD mitgeteilten Informationen können deshalb hier nicht dargestellt werden. Die Wirksamkeit der Datei wird von der Bundesregierung (und mit gleicher Tendenz auch von der Landesregierung) wie folgt beurteilt: Die Erfahrungen mit der analog aufgebauten Antiterrordatei (Art. 1, Gemeinsame-Dateien-Gesetz), die bereits seit 2007 in Wirkbetrieb ist, würden eindrücklich belegen, dass eine gemeinsame elektronische Plattform ein sehr wirkungsvolles Instrument bei der Verbesserung der Zusammenarbeit zwischen verschiedenen, an der Bekämpfung eines Kriminalitätsphänomens beteiligten Behörden sei. Über die punktuelle Kontaktaufnahme bei der Beantwortung einer Suchanfrage hinaus habe sich um die Antiterrordatei ein Netzwerk von „Terrorismusbekämpfern“ in Polizeien und Nachrichtendiensten gebildet. Dies sei ein Befund aus der zur Zeit laufenden Evaluierung der Anti-Terror-Datei nach Art. 5 Abs. 2 Gemeinsame-Dateien-Gesetz. Die Analyse der vorliegenden Nutzungsdaten habe darüber hinaus ergeben, dass der Datenbestand von den teilnehmenden Behörden kontinuierlich gepflegt und angereichert werde (so die Bundesregierung in der Begründung zum Entwurf eines Gesetzes zur Verbesserung der Bekämpfung des Rechtsextremismus, vgl. Tz. II-4.4).

## 4.4 Entwurf eines Bundesgesetzes zur Verbesserung der Bekämpfung des Rechtsextremismus

Die Mordtaten Rechtsextremer, die im November 2011 bekannt geworden sind, haben zu einer Diskussion darüber geführt, ob nicht eine neue gemeinsame Datei von Polizei- und Verfassungsschutzbehörden geeignet wäre, solche Taten effizienter aufzuklären. Als Modell für eine entsprechende Datei erschien die Anti-Terror-Datei, die seit 2007 in Funktion ist.

Kurz vor dem Ende des Berichtszeitraums ist ein Gesetzentwurf der Bundesregierung bekannt geworden, der dieses Ziel verfolgt. Es sollen die gesetzlichen Grundlagen für die Errichtung einer gemeinsamen Datei von Polizeien und Nachrichtendiensten geschaffen sowie die Vorschriften zur Datenübermittlung zwischen Polizeien und Nachrichtendiensten entsprechend angepasst werden. Eine Erweiterung der Antiterrordatei um den Rechtsextremismus wurde geprüft und als unzweckmäßig abgelehnt. Die Erfahrungen mit der Antiterrordatei (Art. 1, Gemeinsame-Dateien-Gesetz), würden die Effizienz einer solchen gemeinsamen Datei belegen. Stichworte sind „Intensivierung“, „Beschleunigung“, „Vereinfachung“ und „Optimierung“ des Informationsaustauschs.

Aus der Sicht des Datenschutzes ist zu prüfen, ob ein solch enger Informationsverbund zwischen Polizei und Verfassungsschutz grundsätzlich zulässig ist. Das Trennungsgebot zwischen Polizei und Nachrichtendiensten wird dadurch zumindest relativiert. Erkenntnisse auch zu dieser Frage werden sich sicherlich der Entscheidung der oben erwähnten Verfassungsbeschwerde (vgl. Tz. II-4.3) entnehmen lassen. Zweifel bestehen auch an der Geeignetheit und der Validität der Daten aus einer solchen bundesweiten Datei: Die Erkenntnisse der Verfassungsschutzbehörden und der Polizei sind häufig bloße Verdachtsinformationen, die ohne Kenntnis des

konkreten Entstehungszusammenhangs nicht zutreffend bewertet werden können. Eine schematische überregionale und überbehördliche Dateispeicherung kann diese Informationen nicht zureichend abbilden. Es besteht damit die Gefahr, dass auf der Basis ungesicherter Informationen schwerwiegende belastende Folgerungen durch andere Behörden gezogen werden. Diese Problematik ist bei sog. „Kontaktpersonen“ noch deutlicher.

Unabhängig davon sollte vor der Einrichtung einer solchen neuen Datei abgewartet werden, welche Ergebnisse die Evaluierung der Anti-Terror-Datei zeigt, deren Ergebnis 2012 aufgrund einer gesetzlichen Regelung vorgelegt werden muss. Erst dann kann fundierter beurteilt werden, ob eine solche Dateiführung wirklich angemessen sein kann. Eine Bewertung des Gesetzentwurfs im Einzelnen bedarf einer eingehenden Prüfung, die im Berichtszeitraum nicht abgeschlossen werden konnte.

## 4.5 Weiterentwicklung der polizeilichen Datenverarbeitung auf der Ebene des Bundes

Ein wesentlicher Teil der polizeilichen Datenverarbeitung erfolgt auf der Ebene des Bundes in sog. „Verbunddateien“, durch die ein bundesweiter polizeilicher Informationsverbund geschaffen wird. Der bislang bedeutsamste Teil dieses Systems ist „Inpol“, das polizeiliche Informationssystem, das vom Bundeskriminalamt betreut und entwickelt wird. Die Weiterentwicklungen dieses Systems und die Überlegungen zu seiner Ergänzung haben sämtlich Auswirkung auf den Datenschutz. Der LfD hat seit vielen Jahren Wert darauf gelegt, hier zeitnah unterrichtet zu werden, um ggf. auch frühzeitig Einfluss nehmen zu können. Er arbeitet deshalb in der Arbeitsgruppe Inpol der Datenschutzbeauftragten des Bundes und der Länder mit. In dieser Arbeitsgruppe wird derzeit besonders das Konzept des „Polizeilichen Informations- und Analyseverbundes – PIAV-“ thematisiert. Dabei handelt es sich um eine technische Neukonzeption zur Verbesserung des polizeilichen Informationsaustausches, in die erhebliche Mittel investiert werden sollen. Welche Auswirkungen dieses Verfahren unter datenschutzrechtlichen Aspekten haben wird, ist derzeit – in der Phase der Konzeptionierung – noch nicht absehbar. Die Arbeitsgruppe wird sich damit intensiv befassen.

Ein anderes bedeutsames Thema der Arbeitsgruppe war die Frage, welche „personengebundenen Hinweise (PHW)“ unter welchen Voraussetzungen im Verfahren „Inpol“ gespeichert werden dürfen. Hierzu sollten klare zentrale Vorgaben getroffen werden, die dem Datenschutz entsprechen müssen. Dies ist nur zum Teil gelungen. Die Länder müssen die verbleibenden Unklarheiten durch eigene Festlegungen ausfüllen. Dies betrifft etwa Definitionen im Bereich des PHW „Waffenbesitz“ oder auch die Frage, welche Nachweise der Polizei vorliegen müssen, bevor das Merkmal „geisteskrank“ gespeichert werden darf. Auf der Ebene des Landes sind diese Konkretisierungen erfolgt.

## 4.6 Vorbeugendes Informationsaustauschsystem zum Schutz vor inhaftierten und entlassenen Rückfalltätern (VISIER.rlp)

Im Dezember 2008 ist eine Vereinbarung zwischen Justiz-, Innen- und Sozialministerium über die Einrichtung eines Verfahrens „Vorbeugendes Informationsaustauschsystem zum Schutz vor inhaftierten und entlassenen Rückfalltätern“, abgekürzt VISIER.rlp, geschlossen worden (vgl. 22. Tb., Tz. 7.6).

Dieses Verfahren soll den Schutz der Allgemeinheit vor gefährlichen Rückfalltäterinnen und -tätern verbessern. Ein wesentlicher Teil dieses Verfahrens ist ein strukturierter Informationsfluss zwischen Justiz, Polizei und Maßregelvollzug. Außerdem wurde eine polizeiliche Datei für eine analytische Risiko- oder Gefährdungsbewertung sowie die im Einzelfall zu treffenden präventiven Maßnahmen zur Verhinderung erheblicher Straftaten geschaffen.

Die von diesem Informationsfluss und der Datenspeicherung Betroffenen wurden wie folgt definiert: „Vom Konzept VISIER.rlp erfasste Personen sind bestimmte gefährliche Strafgefangene oder Maßregelvollzugspatientinnen bzw. -patienten, deren Entlassung aus dem Vollzug bevorsteht. Eine weitere Zielgruppe stellen gefährliche Inhaftierte oder Untergebrachte dar, bei denen die Beantragung einer nachträglichen oder bislang lediglich vorbehaltenen Sicherungsverwahrung in Betracht kommt. Unter Bewährung stehende Personen werden nur dann erfasst, wenn sich ihre Gefährlichkeit im Sinne des Konzepts erst nachträglich im Rahmen der Bewährungs- bzw. Führungsaufsichtszeit ergibt. Erfasst werden unter bestimmten Voraussetzungen Personen, die kraft Gesetzes oder aufgrund gerichtlicher Entscheidung der Führungsaufsicht und bestimmten Risiko mindernden Weisungen unterworfen sind“ (Gemeinsames Rundschreiben des Ministeriums des Innern und für Sport, des Ministeriums der Justiz und des Ministeriums für Arbeit, Soziales, Gesundheit, Familie und Frauen vom 17. Dezember 2008, Justizblatt 4/2009, S. 16).

Dem gemeinsamen Rundschreiben ist weiter zu entnehmen, dass Art und Weise der Umsetzung des Konzeptes und der Datei VISIER.rlp von der

Arbeitsgruppe „Gefährliche Entlassene“ ein Jahr nach Inkrafttreten zu evaluieren sind. Da das Konzept in Rheinland-Pfalz nun seit deutlich längerer Zeit als ein Jahr praktiziert wird, ist es für den LfD von Bedeutung zu überprüfen, ob die mit dem Konzept einhergehenden Eingriffe in das Datenschutzrecht der Betroffenen erforderlich und angemessen sind. Maßstab ist dabei die Frage, ob die angestrebten Ziele des Konzepts durch die eingesetzten Mittel der Datenverarbeitung auch erreicht worden sind. Ein entsprechender schriftlicher Bericht der verantwortlichen Ressorts liegt leider noch nicht vor. In einem Gespräch mit den Verantwortlichen der beteiligten Ressorts wurde allerdings deutlich, dass das Konzept grundsätzlich den Erwartungen entspricht und deutliche Erfolge zu verzeichnen sind. Ein Dissens besteht zwischen den Beteiligten offensichtlich in der Frage, ob durch das Konzept nur Sexualstraftäterinnen und -täter erfasst werden oder ob auch sonstige Gewalttäterinnen und -täter betroffen sein sollen. Der LfD geht davon aus, dass eine entsprechende Entscheidung, orientiert am Erforderlichkeitsgrundsatz, zeitnah erfolgen wird. Auch eine schriftliche Darstellung des Evaluationsergebnisses sollte in absehbarer Zeit vorgelegt werden. Dem LfD ist eine nachvollziehbare Evaluation von Datenverarbeitungen der vorliegenden Art, durch die sehr sensible Daten von entlassenen Personen betroffen sind, wichtig.

## 4.7 Datei „Gewalt im öffentlichen Raum und bei Veranstaltungen (GöRuV)“ beim Polizeipräsidium Trier

Beim Polizeipräsidium Trier wurde im August 2008 eine Datei eingerichtet, in der durch Gewalttaten bei Volksfesten und Veranstaltungen auffällige Personen gespeichert werden sollten. Ziel war es, überregional auftretende Personen zu erkennen, um rechtzeitig auf diese einwirken zu können und um ggf. auch Ermittlungen zu befördern.

Grundlage dafür war § 33 i.V.m. § 41 POG. Die Datei sollte dienen

- der Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung sowie
- der Verhütung von Straftaten und Ordnungswidrigkeiten, insbesondere gewalttätiger Auseinandersetzungen,

die im Zusammenhang mit besonders kriminalitätsbelasteten Örtlichkeiten und Veranstaltungen standen, wie z.B. Volksfeste, Jahrmärkte, Musikevents, Diskotheken und Szenekneipen.

Aufnahme in die Datei fanden

- Tatverdächtige, Beschuldigte, Verurteilte insbesondere in den Fällen von Straftaten unter Anwendung von Gewalt gegen Leib und Leben, Straftaten unter Anwendung von Gewalt gegen fremde Sachen mit der Folge eines erheblichen Schadens, sowie Sexualstraftaten unter Anwendung von Gewalt und Bezug zum öffentlichen Raum bzw. Veranstaltungen.
- Kontakt- und Begleitpersonen der o.a. Personen,
- Betroffene von Ordnungswidrigkeiten von erheblicher Bedeutung, soweit durch Tatsachen begründete Anhaltspunkte die Annahme rechtfertigen, dass sie zukünftig anlassbezogene Straftaten begehen, sowie
- verantwortliche Personen gemäß §§ 4, 5 POG, bei denen durch Tatsachen begründete Anhaltspunkte die Annahme rechtfertigen, dass sie künftig anlassbezogene Gefahren durch ihr Verhalten oder den Zustand von Sachen verursachen.

Unabhängig von einer Prüfung der Erforderlichkeit aus aktuellem Anlass erfolgte die Aussonderungsprüfung spätestens nach zwei Jahren. Bei weiterer (zu dokumentierender) Erforderlichkeit der Informationen war die Verlängerung um ein Jahr zulässig. Bei der Einrichtung der Datei war der LfD beteiligt worden. Er hat deshalb auch die Praxis der Dateinutzung kritisch verfolgt. Nach einem zwei Jahre dauernden Pilotbetrieb teilte ihm das Ministerium des Innern auf seine Anfrage hin mit, dass der Pilotbetrieb der Datei zum 31. Dezember 2010 eingestellt wurde. Die gespeicherten Daten seien gelöscht worden.

Wesentlich für die Entscheidung war der Umstand, dass im Erprobungszeitraum die in der Datei gespeicherten Personen nahezu ausschließlich örtlich auftraten. Insoweit sind die von der Behörde erwarteten Erkenntnisse und Nutzungsmöglichkeiten ausgeblieben.

Dieses Beispiel zeigt, dass die Polizei durchaus selbstkritisch die Notwendigkeit von Dateien und Datenspeicherungen überprüft und ggf. auch Korrekturen im Sinne des Datenschutzes vornimmt.

## 4.8 Reality-TV-Sendungen zur polizeilichen Tätigkeit

Mit dem Innenministerium wurde die Frage erörtert, ob es datenschutzrechtlich möglich ist, im Fernsehen polizeiliche Arbeit „live“ zu dokumentieren. Als Beispiel wurde ein Film des SWR präsentiert, der bereits in der Vergangenheit ausgestrahlt worden ist und der als Vorbild für eine Serie dienen sollte, in der die praktische Polizeiarbeit im Land konkret dargestellt werden soll. Ein wesentlicher Teil des

gezeigten Beitrags war, dass die Fernsehjournalistinnen bzw. -journalisten an der täglichen Arbeit der Polizei teilnahmen, dass sie in den Büros Gespräche zwischen den Beamtinnen und Beamten miterlebten und teilweise auch aufzeichneten und dass sie die Beamtinnen und Beamten bei Außenterminen begleiteten, in deren Verlauf auch Bürgerinnen und Bürger als Zeuginnen bzw. Zeugen oder sonst Betroffene von der Polizei angesprochen worden sind.

Bei einer solchen Einbettung von Journalistinnen und Journalisten in die tägliche Arbeit stellt sich ein Grundsatzproblem: Bereits die Information außenstehender Dritter (auch Journalistinnen bzw. Journalisten) darüber, welche Person aus welchem Anlass Kontakt zur Polizei hat, ist – unabhängig von gefertigten Bild- bzw. Tonaufnahmen – eine dem Datenschutz unterliegende Information, für deren Übermittlung an die Journalistinnen bzw. Journalisten eine Rechtsgrundlage vorliegen muss. Der Datenübermittlung steht in diesem Zusammenhang gleich, wenn den Journalistinnen und Journalisten durch die Polizei bewusst die Möglichkeit zur Datenerhebung verschafft wird.

Als Rechtsgrundlage für solche Datenübermittlungen kommt nur die vorherige informierte Einwilligung der Betroffenen in Betracht. Wenn keine vorherige Einwilligung der betroffenen Bürgerinnen und Bürger vorliegt, ist auszuschließen, dass Journalistinnen und Journalisten im polizeilichen Umfeld entsprechende Informationen zur Kenntnis nehmen können. Die Beachtung dieser Anforderungen kann möglicherweise Sendeformate, wie sie hier vorgestellt worden sind, erschweren und die Aufzeichnung spontaner Aktionen verhindern. Auch bei strikter Beachtung der datenschutzrechtlichen Vorgaben wäre allerdings die Erstellung realitätsnaher Dokumentationen über behördliche Tätigkeiten nicht ausgeschlossen. Unbestritten ist, dass vor der Fertigung von Ton- und Bildaufnahmen eine Einwilligung der Betroffenen vorliegen muss, die vorab über die beabsichtigte Aufzeichnung und deren Verwendung zu informieren sind.

Diese rechtliche Beurteilung entspricht der vom LfD herausgegebenen Information vom 21. Juni 2000 mit dem Titel „Fernsehreportagen über behördliches Handeln und Datenschutz“ sowie der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder „„Reality-TV‘ – keine Mitwirkung staatlicher Stellen bei der Bloßstellung von Menschen“ vom 9. Oktober 2009 (vgl. http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=dsb&ber=078_realitytv).

# 5. Soziales und Gesundheit

## 5.1 Soziales

### 5.1.1 Evaluation des Landeskinderschutzgesetzes

Auf Anregung des LfD wurde in das im Jahre 2008 in Kraft getretene Landesgesetz zum Schutz von Kindeswohl und Kindergesundheit eine Pflicht zur Evaluation aufgenommen (vgl. 22. Tb., Tz. 2.3.3). Nach der in § 11 Abs. 1 LKindSchuG enthaltenen Regelung hat die Landesregierung gegenüber dem Landtag alle zwei Jahre einen Bericht über die in dem Gesetz implementierten Maßnahmen zu erstatten. An dem Bericht, der zum ersten Mal Ende 2010 zu erstatten war, ist der LfD regelmäßig zu beteiligen.

Angesichts der insbesondere mit dem gesetzlichen Einladungs- und Erinnerungsverfahren verbundenen vielfältigen Eingriffe in das informationelle Selbstbestimmungsrecht kommt dem vorzulegenden Bericht eine besondere Bedeutung zu. Nach der Gesetzesbegründung sollen dabei v.a. die Wirksamkeit der lückenlosen Erfassung der Inanspruchnahme der Früherkennungsuntersuchungen und die zeitnahe und gezielte Kontaktaufnahme mit den Familien, für die keine Untersuchungsbestätigung eingegangen ist, untersucht werden. Der Verfassungsgerichtshof unterstrich in seiner Entscheidung vom 28. Mai 2009 (Az. B 45/08) die grundlegende Bedeutung der Evaluation und stellte sogar die verfassungsrechtliche Rechtfertigung der mit dem Einladungs- und Erinnerungsverfahren verbundenen Eingriffe in das informationelle Selbstbestimmungsrecht unter den Vorbehalt der Evaluationsergebnisse.

„Die dazu in den §§ 5 bis 10 LKindSchuG vorgesehenen Einschränkungen des Grundrechts der Eltern auf Selbstbestimmung über personenbezogene Daten sowie des Rechts der Eltern zur Erziehung ihrer Kinder (Art. 4a und 25 LV) sind bei Beachtung vorgegebener verfahrensmäßiger Sicherungen und vorbehaltlich des Ergebnisses der erstmals im Jahr 2010 vorgesehenen Evaluation gerechtfertigt."

(Auszug aus dem Urteil des Verfassungsgerichtshofs vom 28. Mai 2009, Az. B 45/08, 3. Leitsatz)

Zugleich gab der Verfassungsgerichtshof in dem Urteil einige Aufgabenstellungen des von der Landesregierung zu erstattenden Berichts dezidiert vor:

„Insoweit wird der (…) zu erstattende Bericht über die Auswirkungen der im Gesetz vorgesehenen Maßnahmen eindeutigere Feststellungen zu treffen haben. Gegebenenfalls müsste der Gesetzgeber eine Neubewertung der Eignung der Maßnahmen vornehmen.

(…)

Allerdings wird die praktische Umsetzung des auch aus Gründen des Datenschutzes gesetzlich vorgesehenen Verfahrensablaufs im Rahmen der (…) wissenschaftlichen Evaluation überprüft werden müssen. Hierzu hat in der mündlichen Verhandlung der Landesbeauftragte für den Datenschutz nicht unerhebliche Defizite geschildert, die von der Landesregierung eingeräumt wurden. Sie können als Anlaufschwierigkeiten bei der Einführung eines mehrstufigen Verfahrens nur übergangsweise hingenommen werden."

(Auszug aus dem Urteil des Verfassungsgerichtshofs vom 28. Mai 2009, Az. B 45/08, S. 20 und S. 25)

Im Rahmen der Evaluation nahm der LfD gegenüber der Landesregierung zu dem wissenschaftlichen Abschlussbericht des Universitätsklinikums Ulm und des Deutschen Instituts für Jugendhilfe und Familienrecht sowie zu dem Monitoringbericht des Instituts für Sozialpädagogische Forschung Mainz Stellung. Aufgrund der überwiegend auf das Einladungs- und Erinnerungsverfahren zurückzuführenden Eingriffe in das informationelle Selbstbestimmungsrecht behandelten die Äußerungen des LfD in erster Linie die hierzu in diesen Berichten getroffenen Aussagen. Die Bewertung hatte folgende Schwerpunkte:

- Im Ergebnis teilte der LfD die in den Berichten geäußerten Zweifel an der Notwendigkeit aller der Zentralen Stelle zur Verfügung gestellten Meldedaten. Hiernach ist der von den Meldebehörden übermittelte Meldedatensatz im bundesweiten Vergleich am höchsten, ohne dass es hierfür tragfähige Gründe gäbe. Der LfD forderte daher eine Reduzierung der zu übermittelnden Meldedaten.
- Die in den Berichten enthaltene Kritik an der gesetzlich vorgesehenen uneingeschränkten Verpflichtung der Gesundheitsämter zur Datenübermittlung an die Jugendämter entsprach den bereits zuvor seitens des LfD hierzu geäußerten Bedenken. Eine starre Unterrichtungspflicht der Gesundheitsämter steht nach Ansicht des LfD im Widerspruch zum Verhältnismäßigkeitsgrundsatz. Denn eine Nichtteilnahme an der primär dem Gesundheitsschutz dienenden Früherkennungsuntersuchung stellt für sich genommen noch kein Indiz einer Kindeswohlgefährdung dar. Die Gesundheitsämter als Gesundheitsfachbehörden sollten daher eigenverantwortlich über eine im Einzelfall gebotene Unterrichtung des Jugendamtes entscheiden können. Der LfD forderte aus diesem Grund die Landesre-

gierung auf, die zugrunde liegende Regelung des § 9 Abs. 1 Satz 1 LKindSchuG entsprechend anzupassen.

- Dem für das Jahr 2009 in Höhe von 76,7 Prozent festgestellten Anteil falsch-positiver Fälle kam nach übereinstimmender Bewertung der Berichte und des LfD eine zentrale Bedeutung zu. Konkret geht es um Fälle, in denen trotz erfolgter Untersuchung keine Untersuchungsbestätigung bei der Zentralen Stelle einging und aufgrund dessen die Gesundheitsämter die Sorgeberechtigten gezielt und unter Hinweis auf eine mögliche Einschaltung der Jugendämter zur Teilnahme an den tatsächlich bereits wahrgenommenen Untersuchungen auffordern. Der LfD stellte in seiner Stellungnahme klar, dass die Erforderlichkeit und Angemessenheit und damit die verfassungsrechtliche Vereinbarkeit des Verfahrens in Frage gestellt ist, sofern nicht in einem absehbaren Zeitraum der außerordentlich hohe Anteil falsch-positiver Fälle wesentlich verringert werden kann. Ähnliches hatte bereits der Verfassungsgerichtshof in der Entscheidung vom 28. Mai 2009 angedeutet.
  Darüber hinaus wirft auch der weitere Umgang mit den bislang aufgetretenen falsch-positiven Fällen datenschutzrechtliche Fragen auf. Denn Prüfungen des LfD bei den Gesundheitsämtern in den Jahren 2008 und 2009 hatten ergeben, dass in den Verwaltungen auch nach Aufdeckung der falsch-positiven Fälle gleichwohl die dazu gespeicherten Daten der Betroffenen nicht unverzüglich gelöscht wurden. Vielmehr schöpften die Gesundheitsämter die in § 10 LKindSchuG enthaltene Maximalspeicherfrist von drei Jahren aus, obwohl die Daten zur Erfüllung der Aufgaben nach dem Landeskinderschutzgesetz nicht benötigt werden und eine zeitnahe Löschung folglich datenschutzrechtlich geboten wäre. Der LfD forderte die Landesregierung auf, die Maßnahmen zur Reduzierung der falsch-positiven Fälle und die dabei zu beachtenden Löschfristen in der nach dem Landeskinderschutzgesetz vorgesehenen Rechtsverordnung festzulegen.
- Schließlich schloss sich der LfD den in den Berichten geäußerten grundsätzlichen Vorbehalten gegen die Tauglichkeit des Einladungsverfahrens an und unterstützte die von den Wissenschaftlerinnen und Wissenschaftlern ausgesprochene Empfehlung zur Durchführung einer zusätzlichen Kosten-Nutzen-Analyse. Dabei sollen nach den Vorstellungen des LfD mögliche Alternativmodelle zu dem bestehenden Verfahren wie z.B. ein Verzicht auf das bestehende Erinnerungswesen oder eine Verschlankung der Organisationsstruktur des Verfahrens einbezogen werden.

Die Landesregierung legte im Januar 2011 dem rheinland-pfälzischen Landtag den Bericht über die Umsetzung und die Auswirkungen sowie den Weiterentwicklungsbedarf der im Landeskinderschutzgesetz festgelegten Maßnahmen vor. Die Stellungnahme des LfD war dem Bericht als Anlage beigefügt. Nach dem Bericht beabsichtigt die Landesregierung, im Wesentlichen auf die Forderungen des LfD einzugehen. So soll die in dem Gesetz enthaltene Übermittlungspflicht der Gesundheitsämter an die Jugendämter bei Nichtvorliegen einer Untersuchungsbestätigung durch eine Übermittlungsbefugnis im Falle von Anhaltspunkten für eine Kindeswohlgefährdung oder einen weitergehenden Hilfebedarf ersetzt werden. Weiterhin wird angekündigt, den Umfang der der Zentralen Stelle bereit gestellten Meldedaten unter Berücksichtigung der Erfahrungen in anderen Ländern zeitnah zu reduzieren. Im Hinblick auf eine Verringerung des Anteils der falsch-positiven Fälle kündigt die Landesregierung den Erlass einer Rechtsverordnung an, in der geeignete Maßnahmen sowie konkrete Löschungsvorgaben verbindlich festgelegt werden sollen. Schließlich soll das zuständige Fachministerium jährlich über die Umsetzung des zentralen Einladungs- und Erinnerungsverfahrens bei den Gesundheits- und Jugendämtern berichten und dabei eine umfassende Analyse des Kosten-Nutzen-Verhältnisses des bestehenden Verfahrens zugrunde legen.

Zum Jahresende 2011 hat der LfD die mittlerweile zuständigen Ministerien gebeten, den Sachstand zur Umsetzung der angekündigten Maßnahmen mitzuteilen. Eine Antwort lag bis zum Ende des Berichtszeitraums noch nicht vor.

### 5.1.2 Neuordnung der Aufsichtszuständigkeit über die Jobcenter

Mit dem Gesetz zur Weiterentwicklung der Organisation der Grundsicherung für Arbeitsuchende vom 3. August 2010 hat der Gesetzgeber gerade noch fristgerecht den Vorgaben des Bundesverfassungsgerichts aus dem Urteil vom 20. Dezember 2007 (Az. 2 BvR 2433/04 und 2 BvR 2434/04) Rechnung getragen und die Grundsicherung für Arbeitsuchende organisatorisch neu geordnet. Das Gesetz lässt auf der Grundlage einer Verfassungsänderung die Aufgabenwahrnehmung der bisherigen Arbeitsgemeinschaften auch weiterhin in Form gemeinsamer Einrichtungen zu. Die als Jobcenter bezeichneten Verwaltungen, die von der Bundesagentur für Arbeit und den kommunalen Trägern gebildet werden, stellen nun aber eine verfassungsrechtlich zulässige Ausnahme vom Verbot der Mischverwaltung im Bereich der Grundsicherung für Arbeitsuchende dar. In seiner damaligen Entscheidung hatte das Bundesverfassungsgericht noch die Konstruktion der Arbeitsgemeinschaften nach § 44b SGB II als vom Grundgesetz nicht zugelassene Form der Mischverwaltung für verfassungswidrig erklärt und für eine

Neuregelung eine Übergangsfrist bis zum 31. Dezember 2010 eingeräumt (vgl. 22. Tb., Tz. 8.1).

Durch die Gesetzesänderung brachte der Gesetzgeber letztendlich auch Klarheit in die Frage der datenschutzrechtlichen Aufsichtszuständigkeit über die gemeinsamen Einrichtungen. Nach § 50 Abs. 4 Satz 3 SGB II obliegt die Datenschutzkontrolle bei den gemeinsamen Einrichtungen als auch für die zentralen Verfahren dem BfDI. Dies bedeutet, dass seit dem 1. Januar 2011 der LfD nicht mehr die Zulässigkeit der Datenverarbeitung bei den Jobcentern im Lande überprüfen darf, es sei denn, es handelt es sich um einen zugelassenen kommunalen Träger im Sinne von § 6a SGB II (Optionskommune). Hierbei handelt es sich um Kommunen, die ausdrücklich per Rechtsverordnung als alleiniger Träger der Leistungen nach dem Sozialgesetzbuch II zugelassen wurden. Die Zahl dieser Optionskommunen, die als kommunale Gebietskörperschaft automatisch der datenschutzrechtlichen Aufsichtszuständigkeit der jeweiligen Landesdatenschutzbeauftragten unterliegen, wird sich in Rheinland-Pfalz von zwei (Landkreis Südwestpfalz, Landkreis Vulkaneifel) zum 1. Januar 2012 um weitere drei (Landkreis Kusel, Landkreis Mainz-Bingen, Landkreis Mayen-Koblenz) auf insgesamt fünf erhöhen. Insoweit wird der LfD auch weiterhin Ansprechpartner für datenschutzrechtliche Fragen im Zusammenhang mit der Gewährung von Leistungen zur Grundsicherung für Arbeitsuchende bleiben.

### 5.1.3 Informationsaustausch zwischen Jobcentern und Schuldnerberatungsstellen

Noch vor der organisatorischen Neuordnung der Grundsicherung für Arbeitsuchende hatte der LfD eine vertragliche Vereinbarung zwischen einem Landkreis als Grundsicherungsträger und einem Anbieter von Schuldnerberatungsstellen zu bewerten. Darin war ein regelmäßiger Informationsaustausch zwischen der örtlichen Arbeitsgemeinschaft (ARGE) und der Schuldnerberatungsstelle über Klienten- bzw. Kundenbelange, die mit der Integration in Arbeit zusammenhängen, vorgesehen. Das Vorgehen sollte auf einer zuvor bei den Betroffenen routinemäßig einzuholenden Schweigepflichtentbindungserklärung basieren. Die Vertragspartner legten in der Vereinbarung ein Verfahren zur Rückkopplung zwischen Schuldnerberatung und ARGE sowie konkrete Mitteilungsverpflichtungen fest, wobei allerdings der Umfang des beabsichtigten Informationsaustauschs nur allgemein umschrieben war. Die Übereinkunft sah zudem vor, auf Anregung der Schuldnerberaterinnen und -berater bzw. der ARGE-Vermittlerinnen und -vermittler Fallbesprechungen durchzuführen.

Im Rahmen seiner datenschutzrechtlichen Bewertung nahm der LfD zur Rechtsgrundlage und zum Umfang für einen derartigen Informationsaustausch Stellung.

Hiernach bleibt die Einwilligung der Betroffenen die einzig zulässige Legitimationsmöglichkeit für eine Weitergabe von Informationen zwischen Schuldnerberatung und ARGE bzw. Jobcenter. Denn nach übereinstimmender Einschätzung der Bundesagentur für Arbeit und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, die vom LfD geteilt wird, erfasst die bereichsspezifisch in § 61 Abs. 1 SGB II geregelte Auskunftsverpflichtung gerade nicht die kommunalen Eingliederungsleistungen aus § 16a SGB II, zu denen u.a. auch die Schuldnerberatung gehört. Da keine gesetzliche Übermittlungsbefugnis besteht, ist es notwendig und im Hinblick auf den Schutzbedarf der betroffenen Informationen auch sachgerecht, eine ausdrückliche Legitimation bei den Betroffenen einzuholen. Denn Angaben im Zusammenhang mit einer Schuldnerberatung unterliegen regelmäßig einer gesetzlichen Schweigepflicht im Sinne von § 203 Abs. 1 StGB.

Im Hinblick auf den Umfang der von der Schuldnerberatung an die ARGE bzw. die Jobcenter weiterzugebenden Informationen muss der Erforderlichkeitsgrundsatz beachtet werden. Nur die zur Aufgabenerfüllung und insbesondere zur Arbeitsvermittlung erforderlichen Angaben dürfen von den Beratungsstellen an die gemeinsamen Einrichtungen übermittelt werden. Dabei ist zu differenzieren: Rahmeninformationen wie beispielsweise das Teilnahmeverhalten, ein möglicher Beratungsbedarf, die voraussichtliche Dauer und die Erfolgsaussichten einer Beratung sowie ein eventueller Abbruch sind für die weitere Leistungsgewährung durchaus von Bedeutung. Deren Übermittlung an den Grundsicherungsträger wäre daher datenschutzrechtlich auf der Grundlage einer regelmäßig einzuholenden Einwilligungserklärung nicht zu beanstanden. Die Einzelheiten eines Beratungsgesprächs stellen dagegen den Kern einer vertraulichen Beratung dar und dürfen selbst auf der Basis einer Einwilligung nicht an Dritte übermittelt werden. Sofern ausnahmsweise auch die Kenntnis von Beratungsinhalten für die Aufgabenerfüllung der ARGE bzw. des Jobcenters erforderlich sein sollte, wäre deren Offenbarung nur in allgemeiner Form und ohne Details des Gesprächs zulässig, wenn sich die Betroffenen hiermit im Einzelfall ausdrücklich einverstanden erklären.

Vor dem Hintergrund dieser Bewertung wurde die Vereinbarung zwischen dem Landkreis und dem Anbieter der Schuldnerberatungsleistungen an die datenschutzrechtlichen Vorgaben angepasst und der Text der regelmäßig

bei den Betroffenen einzuholenden Schweigepflichtentbindungserklärung entsprechend präzisiert.

Im Rahmen der Betreuung und Unterstützung von Arbeitsuchenden zur Eingliederung in Arbeit ist ein Informationsaustausch zwischen Beratungsstellen im Sinne von § 16a SGB II und Grundsicherungsträgern auf der Basis einer ausdrücklichen Erklärung durch die Betroffenen grundsätzlich denkbar. Übermittelt werden dürfen in diesem Zusammenhang allerdings regelmäßig nur Rahmeninformationen z.B. über den Verlauf und die voraussichtliche Dauer der Beratung sowie das Teilnahmeverhalten. Allgemeine Informationen über die Beratungsinhalte können im Einzelfall nur auf der Grundlage einer zusätzlichen Einwilligung der Betroffenen übermittelt werden, wenn sie für die Aufgabenerfüllung der ARGE bzw. des Jobcenters erforderlich sind. Einzelheiten der Beratungsgespräche einschließlich der Gesprächsprotokolle stellen den Kern einer vertraulichen Beratung dar, deren Weitergabe an Dritte ausgeschlossen ist.

### 5.1.4 Modellprojekt von MDK und AOK zur Fallsteuerung bei Arbeitsunfähigkeit

Durch eine Eingabe erhielt der LfD Kenntnis von einem Erhebungsbogen, mit dem sich die AOK Rheinland-Pfalz im Falle häufig auftretender Arbeitsunfähigkeit von Versicherten an deren behandelnde Ärztinnen oder Ärzte wandte und um weiterführende Informationen bat. In dem Vordruck, der von den auf Bundesebene vereinbarten Formularen abwich, wurden u.a. den Intimbereich der Befragten tangierende Angaben erbeten.

In einem Gespräch mit der betroffenen Krankenkasse und dem MDK Rheinland-Pfalz stellte sich heraus, dass der Fragebogen datenschutzrechtlich nicht von der AOK Rheinland-Pfalz oder einer anderen Krankenkasse, sondern vielmehr dem MDK im Zusammenhang mit der von diesem nach § 275 Abs. 1 Nr. 3a SGB V zu erbringenden gutachtlichen Stellungnahme eingesetzt wurde. Im Falle länger andauernder Arbeitsunfähigkeiten, bei denen sonstige ärztliche oder therapeutische Maßnahmen sowie der Einsatz der auf Bundesebene abgestimmten Mustervordrucke keine nachhaltige Klärung der Gründe der Arbeitsunfähigkeit brachten und die chronisch zu werden drohten, sollten im Rahmen der sozialmedizinischen Fallberatung durch den MDK ggf. verantwortliche psycho-soziale Ursachen und ein daraus resultierender möglicher Rehabilitationsbedarf erkannt werden. Vor diesem Hintergrund hatte der MDK zusammen mit der AOK Rheinland-Pfalz regional begrenzt ein entsprechendes Projekt aufgelegt und den o.g. Vordruck entwickelt. Das Ausfüllen des Fragebogens sei dabei für die Versicherten freiwillig.

Datenschutzrechtlich hielt der LfD die mit dem Einsatz des Vordrucks in dem Projekt verbundene Datenerhebung durch den MDK Rheinland-Pfalz auf der Basis einer Einwilligung der Versicherten für zulässig. Allerdings bestand der LfD auf einer umfassenden Überarbeitung des Fragebogens. Dabei sollte auf dem Formular die für die Datenerhebung verantwortliche Stelle – der MDK Rheinland-Pfalz – deutlich hervorgehoben und der Fragebogen um eine gesonderte schriftliche Einwilligungserklärung der Betroffenen ergänzt werden. Weiterhin bat der LfD, den konkreten Fragenkatalog zu überarbeiten und insbesondere auf den Intimbereich betreffende Fragen zu verzichten. Der LfD regte an, ein separates Informationsblatt zu entwickeln, in dem den Betroffenen neben der Freiwilligkeit der Teilnahme und den Folgen einer Nichtteilnahme auch der Zweck und die Hintergründe der Befragung erläutert werden. Schließlich war aus Sicht des LfD das Rücklaufverfahren zu überprüfen. Dabei sollte sichergestellt werden, dass die Krankenkassen die ausgefüllten Fragebögen nicht zur Kenntnis nehmen können.

Den Forderungen des LfD Rheinland-Pfalz wurde zeitnah entsprochen.

### 5.1.5 Errichtung von Pflegestützpunkten

Durch das Pflegeweiterentwicklungsgesetz wurde in § 92c SGB XI die gesetzliche Grundlage für die bundesweite Errichtung von Pflegestützpunkten geschaffen. Die in der gemeinsamen Trägerschaft von Pflege- und Krankenkassen sowie der nach Landesrecht zu bestimmenden Stellen befindlichen Einrichtungen sollen die Versicherten auf deren Wunsch zu den pflegerischen, sozialen und gesundheitlichen Versorgungs-, Betreuungs- und Unterstützungsangeboten beraten, alle für die wohnortnahe Versorgung und Betreuung in Betracht kommenden Maßnahmen koordinieren und ggf. fallbegleitend bei deren Inanspruchnahme helfen. In Rheinland-Pfalz werden die bereits vorhandenen vernetzten Strukturen der 135 Beratungs- und Koordinierungsstellen genutzt und bis Ende 2011 zu Pflegestützpunkten weiterentwickelt.

Der LfD war im Berichtszeitraum wiederholt in den Umwandlungsprozess eingebunden. Ausgehend von der notwendigen Neuausrichtung und Umstrukturierung der bislang bestehenden Beratungs- und Koordinierungsstellen wurde der datenschutzrechtliche Rahmen der künftigen Pflegestützpunkte gegenüber dem Landesamt für Soziales, Jugend und Versorgung als koordinierender Behörde deutlich gemacht. Dabei wurde u.a. gefordert, das Tätigkeitsspektrum der Pflegestützpunkte an die in § 92c SGB XI enthaltenen Aufgaben anzupassen und bisherige Leistungen wie z.B. die Schuldnerberatung künftig nicht mehr selbst anzubieten. Im Hinblick auf die

Datenverarbeitung in den Stützpunkten wurde klar gestellt, dass es angesichts der eindeutigen Verarbeitungsbefugnis aus § 92c Abs. 7 SGB XI unterbleiben sollte, eine Einwilligung bei den Betroffenen einzuholen. Gleichwohl wurde angeregt, den Betroffenen durch Bereitstellung eines Merkblattes die Aufgaben der Pflegestützpunkte und die in diesem Zusammenhang bestehenden Datenverarbeitungsbefugnisse transparent zu machen. Dies wurde zugesichert.

Hinsichtlich der in den Pflegestützpunkten zum Einsatz kommenden IT-Verfahren wies der LfD auf die sich nach § 78a SGB X ergebenden Vorgaben hin. Dabei wurde mit Blick auf das zentral vom Landesbetrieb Daten und Information betriebene Dokumentationsverfahren u.a. die Vorlage eines Berechtigungskonzepts, die Abschottung des Verfahrens gegenüber externen Stellen wie z.B. den Pflegekassen oder den Trägern, die Festlegung eines Löschkonzepts sowie der Einsatz eines geeigneten Protokollierungsverfahrens gefordert. Der LfD beabsichtigt, die Einhaltung dieser Forderungen durch Besuche bei einzelnen Pflegestützpunkten vor Ort zu überprüfen.

### 5.1.6 Hausarztzentrierte Versorgung

Das Krankenversicherungsrecht verpflichtet die gesetzlichen Krankenkassen, ihren Versicherten eine besondere Form der hausärztlichen Versorgung, die sog. hausarztzentrierte Versorgung (hzV), anzubieten. Diese unterliegt bestimmten gesetzlich festgelegten fachlichen Anforderungen und kann von den Versicherten auf freiwilliger Basis in Anspruch genommen werden. Um diese besondere Versorgungsform flächendeckend sicherzustellen, hat der Gesetzgeber eine vertragliche Vereinbarung vorrangig zwischen Krankenkassen und Gemeinschaften der Leistungserbringer vorgesehen. Nur in Ausnahmefällen ist ein direkter Vertragsschluss mit einzelnen Ärztinnen und Ärzten zulässig.

Bundesweit schlug im Berichtszeitraum die Frage der Abrechnung von im Rahmen der hzV erbrachter Leistungen hohe Wellen. Denn in den hierzu geschlossenen Vereinbarungen zwischen einzelnen Krankenkassen und den jeweiligen Hausärzteverbänden wurde festgelegt, dass zur Abrechnung der Leistungen gegenüber den Kostenträgern automatisch eine bestimmte von dem Verband ausgewählte Stelle beauftragt wird. Dies hatte zur Folge, dass die betroffenen Ärztinnen und Ärzte, die an der hzV teilnehmen wollten, die für die Abrechnung erforderlichen Patientendaten an den vertraglich vorgesehenen Dritten übermitteln mussten, ohne noch selbst auf dessen Auswahl oder die von ihm eingesetzte Software Einfluss nehmen zu können.

Datenschutzrechtlich sehen zwar die zugrunde liegenden Regelungen (§ 295 Abs. 1b Satz 5 SGB V in der bis zum 30. Juni 2011 geltenden Fassung bzw. aktuell § 295a Abs. 1 SGB V) die Möglichkeit einer Beauftragung Dritter mit der Verarbeitung der für die Abrechnung erforderlichen Daten vor. Dies stellt allerdings gesetzessystematisch eine Ausnahme dar. Nach der Festlegung des Gesetzgebers bleibt vielmehr die in § 295 Abs. 1b Satz 1 SGB V beschriebene Direktabrechnung zwischen Leistungserbringer und Krankenkasse auch nach Einfügen des § 295a SGB V weiterhin das Grundmodell einer Leistungsabrechnung bei besonderen Versorgungsformen. Die Entscheidung, ob und ggf. welche externe Stelle einzelne Ärztinnen und Ärzte möglicherweise in den Abrechnungsprozess einbinden möchten und wem gegenüber von der Schweigepflicht umfasste Patientendaten offenbart werden, obliegt somit im Bereich der hzV auch weiterhin allein ihnen. Hierfür tragen sie auch zu Recht die datenschutzrechtliche Verantwortung.

Verträge, die eine Teilnahme von Leistungserbringern an der hzV zwangsläufig und alternativlos mit einer externen Datenverarbeitung koppeln, stehen im Widerspruch zu diesen sozialrechtlichen Vorgaben und sind bereits aus diesem Grund datenschutzrechtlich bedenklich. Dies gilt umso mehr, wenn den Leistungserbringern darüber hinaus auch noch der umfassende Zugang zu den IT-Verfahren, die Auftragnehmerinnen und Auftragnehmer einsetzen, verwehrt wird und er dadurch nicht die mit einer Beauftragung verbundenen Risiken für den Schutz und die Sicherheit der Patientendaten verlässlich einschätzen kann.

Der LfD hat seine Rechtsauffassung frühzeitig gegenüber dem zuständigen Ministerium und dem Hausärzteverband Rheinland-Pfalz dargelegt. Es bleibt abzuwarten, ob die Verträge, die rheinland-pfälzische Leistungserbringer betreffen, zumindest zukünftig die dargestellten datenschutzrechtlichen Maßstäbe beachten.

### 5.1.7 Verarbeitung von Sozialdaten im Rahmen eines bundesweiten Projekts der Kassenärztlichen Bundesvereinigung

In Genehmigungsverfahren zur Übermittlung von Sozialdaten für die Forschung und Planung (§ 75 Abs. 2 S. 1 SGB X) wird der LfD teilweise vom Sozialministerium eingebunden. In anderen Bereichen, z.B. §§ 9, 9a LKRG, ist die Anhörung des LfD im Rahmen des Verfahrens sogar gesetzlich geregelt. Im Hinblick auf die meist hohe Sensibilität der verwendeten Daten ist eine (zeit)intensive Prüfung der regelmäßig komplexen Studien erforderlich. Als Beispiel für die bei wissenschaftlichen Studien auftretenden Probleme oder Fragestellungen wird das Projekt

„Prognose der demografisch bedingten Veränderungen des Versorgungs- und Arztbedarfs“ vorgestellt.

Ziel des Projekts ist die Ermittlung von Praxisstandorten nach Arztgruppen, welche bis zum Jahr 2025 vorrangig zu besetzen sind und deshalb durch die Kassenärztliche Vereinigung gefördert werden sollen. Das Forschungsvorhaben dient dazu, die Voraussetzungen sowie den Handlungsbedarf für eine dauerhafte Sicherstellung der wohnortnahen, flächendeckenden vertragsärztlichen Versorgung zu erkennen.

Zu diesem Zweck beantragte die Kassenärtzliche Vereinigung beim zuständigen Ministerium die Genehmigung, um Patientendaten (Patienten-ID, Alter, Geschlecht, ambulante Leistungsdaten, Postleitzahl, Ort, Straße) und Daten behandelnder Ärztinnen und Ärzte (Arztnummer, Alter, Geschlecht, Fachgruppe, Postleitzahl, Ort, Straße) an das Zentralinstitut für die kassenärztliche Versorgung in der Bundesrepublik Deutschland (Zentralinstitut) übermitteln zu dürfen.

Aufgrund der gewünschten Daten wäre die Übermittlung sowohl im Hinblick auf die Ärztinnen und Ärzte als auch die Patientinnen und Patienten personenbeziehbar erfolgt, weshalb der Antrag der Kassenärztlichen Vereinigung anhand § 75 SGB X zu bewerten war. Diese Vorschrift setzt u.a. voraus, dass das öffentliche Interesse an der Forschung oder Planung das Geheimhaltungsinteresse der Ärztinnen und Ärzte sowie der Patientinnen und Patienten als Betroffene erheblich überwiegt (§ 75 Abs. 1 S. 1 SGB X). Diese Voraussetzung war im Hinblick auf die eher geringe Empfindlichkeit der Daten der Ärztinnen und Ärzte noch gegeben, nicht jedoch hinsichtlich der sensiblen Leistungsdaten der Patientinnen und Patienten.

Der LfD schlug daher vor, auf das Datum „Straße“ zu verzichten und das Patientenalter in Kategorien anzugeben, um die Datenverarbeitung aus der Sicht des Zentralinstituts als faktisch anonym und daher aus datenschutzrechtlicher Sicht als zulässig bewerten zu können.

Das Zentralinstitut hielt dem entgegen, dass bei einer Umsetzung des Vorschlags des LfD mit einem hohen Informationsverlust zu rechnen sei, weshalb die Zwischenschaltung eines Datentreuhänders vorgezogen wurde. Diese Stelle erhielt von der Kassenärztlichen Vereinigung nur die Adressdaten der Patientinnen und Patienten, um sie in Geokoordinaten mit einem Aggregationsniveau umzuwandeln, die die Indentifizierung von Einzelpersonen durch das Zentralinstitut unmöglich mache. Diese Geokoordinaten würden beim Zentralinstitut dann über einen Code mit den ambulanten Leistungsdaten zusammengeführt.

Im weiteren Verlauf stellte sich dann aber heraus, dass das Zentralinstitut unter Verwendung einer kommerziellen Software in der Lage war, die Geokoordinaten auf Ort und Straße und ggf. sogar die Hausnummer zurückzuführen. Zu diesem Zeitpunkt wurden auch verschiedene Datenschutzbeauftragte anderer Bundesländer auf dieses Projekt aufmerksam und machten in dieselbe Richtung gehende Einwände geltend.

Mit einer nochmaligen Änderung im Geschäftsprozess wurde laut Zusicherung des Zentralinstituts dann sichergestellt, dass die dorthin übermittelten Geokoordinaten nicht mehr straßenbeziehbar seien. Die ursprünglich geäußerten datenschutzrechtlichen Bedenken wurden damit als ausgeräumt angesehen.

## 5.2 Gesundheit

### 5.2.1 Datenschutz im Krankenhaus

Mit der Erarbeitung einer Orientierungshilfe zur datenschutzgerechten Ausgestaltung und Betrieb von Krankenhausinformationssystemen (KIS) bildete der Datenschutz im Krankenhaus einen der Arbeitsschwerpunkte des LfD im Berichtszeitraum. Neben der sehr konstruktiven Mitarbeit in der dafür von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eingesetzten Arbeitsgruppe gehörten hierzu insbesondere vielfältige Aktivitäten auf Landesebene, die einen dialogorientierten und einvernehmlichen Umsetzungsprozess in Gang bringen sollten (ausführliche Informationen hierzu finden sich in Tz. I-3.6).

### 5.2.2 Einsatz von Standardvordrucken im öffentlichen Gesundheitsdienst

Aufgrund einer Eingabe hatte der LfD den Umgang eines Gesundheitsamtes mit einem standardmäßig vor Untersuchungsbeginn eingesetzten Vordruck über die Befreiung von der ärztlichen Schweigepflicht zu bewerten. In dem mit „Beurteilungsgrundlage“ überschriebenen Formular werden die zu Untersuchenden aufgefordert, ihr Einverständnis mit der Beiziehung der für die Beurteilung erforderlichen ärztlichen Befunde und Unterlagen von konkret zu bezeichnenden Ärztinnen und Ärzten durch das betreffende Gesundheitsamt zu erklären. Die Erklärung bezieht sich nach dem Vordrucktext auch auf die Weitergabe des zu erstellenden Gesundheitszeugnisses an die für die dienst- und arbeitsrechtliche Entscheidung zuständige Stelle sowie die Verwendung der für das

Gutachten maßgeblichen Beurteilungsgrundlage innerhalb der Gesundheitsverwaltung.

Im konkreten Fall hatte die Behörde den Betroffenen vor Beginn der amtsärztlichen Untersuchung zur Abklärung der Dienstfähigkeit um Unterzeichnung des Vordrucks gebeten, obwohl die in dem Formular einzutragenden Angaben zum Untersuchungszweck und zur Identität der Ärztinnen und Ärzte, bei denen Unterlagen beigezogen werden sollen, nicht eingetragen waren. Nachdem sich die zu untersuchende Person unter Hinweis auf von ihr vorgelegte ärztliche Befunde wiederholt weigerte, die in dem Vordruck vorgesehene Erklärung abzugeben, lehnte das Gesundheitsamt die Durchführung der Untersuchung ab und teilte dem Dienstherrn des Betroffenen mit, dass eine amtsärztliche Begutachtung aufgrund dessen Weigerung nicht möglich sei.

Gegen das Vorgehen des Gesundheitsamtes äußerte der LfD grundsätzliche Bedenken. Nach den zugrunde liegenden Bestimmungen der §§ 9 ÖGdG, 56 ff., 61a LBG sind Beschäftigte der Landes- bzw. Kommunalverwaltung verpflichtet, sich in den gesetzlich bestimmten Fällen einer amtsärztlichen Untersuchung zu unterziehen. Zugleich sind Amtsärztinnnen und Amtsärzte zur Anfertigung medizinischer Gutachten oder Gesundheitszeugnisse und der in diesem Zusammenhang erforderlichen Verarbeitung medizinischer Daten befugt. Dies gilt auch für die Anforderung von Fremdbefunden oder sonstigen medizinischen Unterlagen bei anderen Ärztinnen und Ärzten. In diesen Fällen ist allerdings für die damit verbundene Offenbarung von Patientendaten eine vorherige Entbindung von der ärztlichen Schweigepflicht notwendig, es sei denn, die Betroffenen bringen die angeforderten Unterlagen selbst bei. Soweit darüber hinaus das Gesundheitsamt das Untersuchungsergebnis dem auftraggebenden Dienstherrn übermitteln möchte, besteht bereits auf der Grundlage des § 11 Abs. 3 Nr. 1 ÖGdG i.V.m. § 61a Abs. 2 LBG eine gesetzliche Offenbarungsbefugnis. Für die Einholung einer Schweigepflichtentbindung bei den Betroffenen bleibt somit rechtlich kein Raum.

Im Ergebnis hätte das Gesundheitsamt in dem der Eingabe zugrunde liegenden Fall somit auch ohne Unterzeichnung des Vordrucks die amtsärztliche Untersuchung durchführen und das Ergebnis dem Dienstherrn übermitteln können. Einer Schweigepflichtentbindung durch den Betroffenen hätte es nur dann bedurft, wenn die von ihm zur Verfügung gestellten Befundunterlagen nicht ausreichend und ein direkter Informationsaustausch mit den behandelnden Ärztinnen und Ärzten zur amtsärztlichen Begutachtung erforderlich gewesen wäre. Hierfür gab es jedoch keine Anhaltspunkte.

Der LfD hat anlässlich dieses Falles den Einsatz von Standardvordrucken im öffentlichen Gesundheitsdienst gegenüber dem Landesamt für Soziales, Jugend und Versorgung und dem zuständigen Fachministerium grundsätzlich thematisiert. Nach übereinstimmender Einschätzung soll zukünftig die Einholung von Schweigepflichtentbindungserklärungen, die rechtlich nicht erforderlich ist, unterbleiben. Zu diesem Zweck ist seitens des Landesamtes für Soziales, Jugend und Versorgung beabsichtigt, die Gesundheitsämter in schriftlicher Form allgemein über die Erforderlichkeit von Schweigepflichtentbindungen im Zusammenhang mit amtsärztlichen Untersuchungen und die sich daraus ergebenden Folgen für das Verwaltungshandeln zu informieren. Zugleich sollen geeignete Vordruckvorlagen zur Verfügung gestellt werden, die von den Gesundheitsämtern bereichsspezifisch angepasst und verwendet werden können.

Der Einsatz von Vordrucken im Bereich des Öffentlichen Gesundheitsdienstes und das damit verbundene Einholen von Schweigepflichtentbindungserklärungen muss an die im Einzelfall bestehenden jeweiligen rechtlichen Vorgaben angepasst werden. Verweigern die Betroffenen die Unterzeichnung von routinemäßig eingeholten Erklärungen, ohne dass deren Vorliegen für das weitere Tätigwerden der Gesundheitsbehörde im konkreten Fall rechtlich geboten ist, darf dies nicht zum Abbruch der amtsärztlichen Maßnahmen führen.

### 5.2.3 Neues von der Elektronischen Gesundheitskarte

Mit mehrjähriger Verspätung begann im September 2011 die Auslieferung der Elektronischen Gesundheitskarte. Im Vergleich zu den gesetzlichen Vorgaben verfügt die nun ausgegebene Karte allerdings über ein deutlich eingeschränktes Leistungsspektrum. Zwar enthält die zunächst in Umlauf gebrachte Karte neben dem Lichtbild als weitere Neuerung einen Mikroprozessor-Chip. Dieser verfügt jedoch derzeit noch über keine eigene Funktionalität. Erst ab den Jahren 2012/2013 sollen mit der verpflichtenden Anwendung des Versichertenstammdatenabgleichs die technischen Möglichkeiten des Chips auch aktiv genutzt werden können. Erst danach und nur teilweise noch mit einem konkreten Zeitziel versehen sind dann die in § 291a Abs. 3 SGB V enthaltenen freiwilligen Anwendungen des Notfalldatenmanagements, des elektronischen Arztbriefs, der Arzneimitteltherapiesicherheit und der elektronischen Patientenakte vorgesehen.

Vor diesem Hintergrund muss das einstmals als „Leuchtturmprojekt“ umschriebene Vorhaben mittlerweile auch aus datenschutzrechtlicher Sicht zwiespältig gesehen werden. Es besteht vielmehr die Gefahr, dass die zunächst umfassend berücksichtigten Belange des Daten-

schutzes durch eine Absenkung der Sicherheitsstandards und einen Verzicht auf die sorgfältige Erprobung der vorgesehenen Funktionalitäten zunehmend verwässert werden. So sollen nach dem gegenwärtigen Stand der Planungen der zunächst umfassende Zugangsschutz auf die mit der Karte verarbeiteten Daten über eine PIN gelockert werden. Auch die mit dem Projekt verfolgte zunehmende Anbindung der IT-Systeme von Arztpraxen an das Internet ohne obligatorische Absicherungen verfolgen die Datenschützerinnen und Datenschützer mit Sorge. Sofern mit der Elektronischen Gesundheitskarte zumindest mittelfristig auch Befund- und Diagnosedaten aus den Arztdokumentationen verarbeitet werden sollen, ist schließlich immer noch unklar, in welcher Weise die Betroffenen ihre gesetzlich vorgesehenen Rechte auf Auskunft und Löschung wahrnehmen können.

Aufgrund dessen werden die Datenschutzbeauftragten des Bundes und der Länder die weitere Entwicklung des Projekts intensiv begleiten und auf damit zusammenhängende Gefahren deutlich hinweisen.

### 5.2.4 Datenschutz in der Arztpraxis

Seit Übernahme der Aufsichtszuständigkeit über private datenverarbeitende Stellen durch den LfD im Herbst 2008 nehmen Eingaben und Anfragen aus dem Bereich der niedergelassenen Ärzteschaft kontinuierlich zu. Dies überrascht nicht. Das für eine erfolgreiche Behandlung zwingend notwendige Vertrauensverhältnis zwischen Ärztinnen bzw. Ärzten und Patientinnen bzw. Patienten setzt den umfassenden Schutz der in einer Arztpraxis verarbeiteten Patientendaten voraus. Hierzu gehören z.B. die datenschutzgerechte Gestaltung von Handlungsabläufen oder der sichere Einsatz von Informationstechnologie einschließlich der Nutzung des Internets. Gleichwohl deutet die hohe Zahl der im Berichtszeitraum eingegangenen Anfragen darauf hin, dass hier noch ein beachtliches Verbesserungspotential vorhanden sein dürfte.

Vor diesem Hintergrund versuchte der LfD im Berichtszeitraum, die niedergelassenen Ärztinnen und Ärzte bei der Sicherstellung eines angemessenen Datenschutzniveaus so weit wie möglich zu unterstützen. Von übergeordneter Bedeutung waren dabei folgende Fragestellungen:

#### ■ Bestellung von Datenschutzbeauftragten

Wiederholt wurde der LfD im Berichtszeitraum gefragt, ob Arztpraxen, die weniger als zehn Mitarbeiterinnen oder Mitarbeiter beschäftigen, verpflichtet sind, Datenschutzbeauftragte zu bestellen. Dies wurde letztlich verneint. Datenschutzrechtlich legt § 4f Abs. 1 BDSG die Anforderungen für die Bestellung von Datenschutzbeauftragten bei nicht-öffentlichen Stellen und damit auch bei niedergelassenen Arztpraxen fest. Maßgeblich ist grundsätzlich die Beschäftigtenzahl, es sei denn, die Stelle nimmt automatisierte Datenverarbeitungen vor, die nach § 4d Abs. 5 BDSG einer Vorabkontrolle unterliegen. Dies ist bei niedergelassenen Ärztinnen und Ärzten im Ergebnis jedoch nicht der Fall (§ 4d Abs. 5 S. 2 2. Halbsatz BDSG).

Auch wenn Arztpraxen, die Patientendaten automatisiert verarbeiten und weniger als zehn Personen damit beschäftigen, nicht verpflichtet sind, eigene Datenschutzbeauftragte zu bestellen, bedeutet dies nicht, dass dadurch die Einhaltung der datenschutzrechtlichen Vorgaben gefährdet ist. Bereits die berufs-, datenschutz- und strafrechtlichen Vorgaben verpflichten die Ärzteschaft, ihre Schweigepflicht sicherzustellen und somit zwangsläufig auch die hierzu erforderlichen technischen und organisatorischen Maßnahmen vorzunehmen (§ 9 BDSG).

#### ■ Einsichtsrecht für Patientinnen und Patienten in ärztliche Unterlagen

Auf dem 114. Deutschen Ärztetag 2011 in Kiel stand eine Änderung der Musterberufsordnung auf der Tagesordnung, die das Einsichtsrecht der Patientinnen und Patienten in die sie betreffenden Behandlungsakten betraf. Hintergrund war die Tatsache, dass die hierzu in der Musterberufsordnung enthaltene Regelung immer noch die ehemals vom Bundesgerichtshof vorgesehene Ausnahme bzgl. der subjektiven Eindrücke und Wahrnehmungen enthält, obwohl die Rechtsprechung des Bundesverfassungsgerichts (vgl. Entscheidung vom 9. Januar 2006, Az. 2 BvR 443/02) mittlerweile den Patientinnen und Patienten ein umfassendes Akteneinsichtsrecht zubilligt und Einschränkungen dieses Rechts nicht pauschal, sondern nur im Einzelfall zulässt. Die beabsichtigte Änderung kam lediglich aus Zeitgründen nicht mehr zustande.

Zur Herstellung von Rechtsklarheit hat der LfD die Landesärztekammer gebeten, schon jetzt die Regelung in § 10 Abs. 2 der Berufsordnung für die Ärztinnen und Ärzte in Rheinland-Pfalz an die verfassungsrechtliche Rechtsprechung anzupassen. Die bisherige Bestimmung entspricht der Musterberufsordnung und nimmt von dem Einsichtsrecht der Patientinnen und Patienten die Teile aus, die subjektive Eindrücke oder Wahrnehmungen der Ärztinnen oder Ärzte enthalten. Die Landesärztekammer erklärte sich bereit, die Sache im Interesse einer bundeseinheitlichen Lösung nach der bevorstehenden Beratung in den Berufsordnungsgremien der Bundesärztekammer voranzubringen.

### Auslagerung des eingehenden Telefonverkehrs einschließlich der Terminvergabe

Aufgrund einer Eingabe hatte der LfD zu überprüfen, ob die Beauftragung eines externen Callcenters durch eine Arztpraxis datenschutzrechtlich zulässig war. Im konkreten Fall hatte die Arztpraxis ihren Telefonverkehr auf einen privaten, nicht am Praxisstandort ansässigen Dienstleister ausgelagert. Dieser hatte eine Hotline eingerichtet, auf der alle für die Praxis eingehenden Telefonate von ihm betreut wurden. Daneben sollte das Callcenter allen Anrufern selbständig und patientenbezogen verbindliche Arzttermine vergeben. Zu diesem Zweck stand der Firma an Wochentagen von 8 bis 18 Uhr ein unbeschränkter lesender und schreibender Zugriff auf den elektronischen Terminkalender der Arztpraxis zur Verfügung. Die anrufenden Patientinnen oder Patienten wurden weder durch die Praxis oder das Callcenter auf die konkrete Verfahrensweise aufmerksam gemacht noch um Einwilligung in die damit zusammenhängende Datenverarbeitung gebeten. Der Auslagerung lag eine Vereinbarung zugrunde, die von der Arztpraxis nicht unterzeichnet war und in der zwar die Betreuung des Telefonverkehrs, nicht aber die Terminvergabe als Aufgabe aufgeführt war. Zudem fehlten in der Vereinbarung Festlegungen zum Umfang der dem Callcenter zu gewährenden Zugriffsrechte auf die Praxissoftware und zu den in diesem Zusammenhang von dem Auftragnehmer zu ergreifende technisch-organisatorischen Maßnahmen zum Schutz der Patientendaten.

Übereinstimmend mit der Landesärztekammer hielt der LfD die Beauftragung für unvereinbar mit den heranzuziehenden berufsrechtlichen und datenschutzrechtlichen Vorgaben. Der LfD qualifizierte sowohl die Bereitstellung einer Hotline als auch die Betreuung des eingehenden Telefonverkehrs durch das Callcenter als Auftragsdatenverarbeitung, die jedoch nicht die in § 11 Abs. 2 BDSG enthaltenen Anforderungen einhielt. Hiernach ist der Auftrag schriftlich und unter Festlegung der in der Bestimmung genannten Inhalte zu erteilen. Dies war in dem zugrunde liegenden Sachverhalt nicht der Fall. Neben der Unterschrift des Auftraggebers und damit der eigentlichen Auftragserteilung fehlten auch die vollständige Festlegung des Auftragsgegenstands sowie der nach § 9 BDSG von dem Dienstleister zu treffenden technischen und organisatorischen Maßnahmen. Mangels Dokumentation blieb auch offen, ob sich die Arztpraxis überhaupt vor Beginn der Datenverarbeitung von der Einhaltung der datenschutzrechtlichen Anforderungen beim Callcenter überzeugt hatte.

Darüber hinaus verstieß nach Einschätzung des LfD die mit der Auslagerung der telefonischen Terminvergabe verbundene Preisgabe von Patientendaten gegen die Vorgaben der ärztlichen Schweigepflicht. Hiernach dürfen schweigepflichtige Informationen wie die Tatsache, Patientin oder Patient einer bestimmten Arztpraxis zu sein, nur dann gegenüber Dritten offenbart werden, wenn die Berufsgeheimnisträgerinnen oder der Berufsgeheimnisträger hierzu befugt ist. Auch dies war aber nicht der Fall. Denn die Patientinnen oder Patienten hatten die Praxis nicht von der ärztlichen Schweigepflicht entbunden, da die Tatsache der externen Betreuung der telefonischen Kommunikation überhaupt nicht bekannt war.

Nach der datenschutzrechtlichen Bewertung der Angelegenheit teilte die betroffene Arztpraxis mit, dass die Beauftragung des Callcenters eingestellt worden sei.

### Entsorgung von Patientenunterlagen im Müll

Ein nicht alltäglicher Sachverhalt beschäftigte den LfD zu Beginn des Berichtszeitraums. Ein Arzt hatte Unterlagen, die er im Rahmen einer früheren ärztlichen Tätigkeit angefertigt und genutzt hatte, in Müllsäcken in einem öffentlich zugänglichen Abfallcontainer abgelegt. Zu den entsorgten Dokumenten gehörten u.a. in Diajournalen zusammengefasste Dias von Gesichtsfeldern einzelner ehemaliger Patientinnen und Patienten, auf denen teilweise deren Name, Geburtsdatum und der Befund enthalten waren. Die im Müll befindlichen Aufnahmen wurden von einem Anwohner entdeckt.

Der LfD qualifizierte das Verhalten des Arztes als Verstoß gegen die Vorgabe des § 28 Abs. 6 BDSG und sah im konkreten Fall den Tatbestand einer Ordnungswidrigkeit im Sinne von § 43 Abs. 2 Nr. 1 BDSG erfüllt. Das Ablegen der Diaaufnahmen in einem öffentlich zugänglichen Bereich und die Kenntnisnahme der Daten durch Dritte stellten eine Übermittlung von Gesundheitsdaten gemäß §§ 28 Abs. 6, 3 Abs. 4 Nr. 3a BDSG dar, die mangels Einwilligung der Betroffenen unzulässig war. Für die rechtliche Bewertung als Datenweitergabe und damit als Übermittlung reichte es nach Einschätzung des LfD bereits aus, dass die Informationen aufgrund des bewussten Handelns des Arztes in einen öffentlich zugänglichen Bereich gelangten. Da damit Dritte nach der Ablage der Unterlagen in dem Container zumindest die Möglichkeit hatten, ungehindert die konkreten Informationen zur Kenntnis zu nehmen, war die Weitergabe im Sinne von § 3 Abs. 4 Nr. 3a BDSG erfolgt. Aufgrund der besonderen Bedeutung der Angelegenheit verhängte der LfD ein Bußgeld.

# 6. Bildung und Wissenschaft

## 6.1 Bildung

### 6.1.1 Schultrojaner

Der Inhalt eines Gesamtvertrages, den die Länder am 21. Dezember 2010 mit den Schulbuchverlagen abgeschlossen hatten, wurde in der Öffentlichkeit unter dem Begriff des „Schultrojaners“ lebhaft diskutiert. In dem Vertrag verpflichten sich die Länder, in den Schulen eine (noch zu entwickelnde) Plagiatssoftware zum Einsatz zu bringen, welche sog. Digitalisate, also Kopien von urheberrechtlich geschützten Werken, aufspüren soll.

Unabhängig davon, dass die technische Realisierbarkeit einer solchen Software bei rund 40.000 Verlagsprodukten zweifelhaft erscheint, können aus Sicht des LfD bereits jetzt gewisse rechtliche Grundaussagen zum Einsatz einer solchen Software in Schulen getroffen werden, die die im Gesamtvertrag vorausgesetzte „datenschutzrechtliche Unbedenklichkeit“ in Frage stellen.

Auch wenn die Plagiatssoftware selbst keine personenbezogenen Daten verarbeiten sollte, ist davon auszugehen, dass zumindest im Trefferfall von einer gewissen Personenbeziehbarkeit auszugehen ist. Wird z.B. ein bestimmtes Arbeitsblatt von der Software aufgespürt, dürfte der Rückschluss darauf, welche Lehrkraft das fragliche Arbeitsblatt eingestellt hat, in aller Regel möglich sein. In diesem Zusammenhang ist auch eine weitere Vereinbarung des Gesamtvertrages zu sehen, wonach sich die Länder verpflichten, bei Bekanntwerden von Verstößen gegen die im Gesamtvertrag festgelegten Vorgaben für das Vervielfältigen von urheberrechtlich geschützten Werken disziplinarische Maßnahmen gegen die betreffenden staatlichen Schulleitungen und Lehrkräfte einzuleiten. Dies gilt auch für Verstöße, die mittels Plagiatssoftware aufgedeckt werden; zumindest ist diese Variante im Vertrag nicht ausdrücklich ausgeschlossen worden.

Es ist daher davon auszugehen, dass die Plagiatssoftware allein aufgrund ihrer Zweckbestimmung zumindest eine personenbeziehbare Datenverarbeitung unterstützt, so dass der Anwendungsbereich des § 67 Abs. 1 SchulG eröffnet ist. Hiernach dürfen personenbezogene Daten von Lehrkräften durch die Schulen verarbeitet werden, soweit dies zur Erfüllung der ihnen durch Rechtsvorschrift zugewiesenen schulbezogenen Aufgaben erforderlich ist. Eine solche Rechtsvorschrift, welche die Schulen verpflichten würde, Urheberrechtsverstöße aufzudecken, existiert jedoch nicht. Dadurch, dass die Software anlassunabhängig recherchiert, ist darüber hinaus eine Vereinbarkeit mit dem Erforderlichkeitsgrundsatz in Zweifel zu ziehen.

Der LfD wird die weitere Entwicklung in Abstimmung mit dem Bildungsministerium kritisch begleiten. Ob die Software jemals an rheinland-pfälzischen Schulen zum Einsatz kommen wird, darf jedoch bezweifelt werden. Dazu passt die Pressemitteilung der Kultusministerkonferenz vom 13. Dezember 2011 mit folgendem Wortlaut:

> „…Die in § 6 Absatz 4 des Vertrages beschriebene ‚Scansoftware' wird nach Einschätzung der Vertragspartner bis auf Weiteres, jedenfalls nicht im Jahr 2012, zum Einsatz kommen. Die Vertragspartner verabredeten, im ersten Quartal 2012 ein weiteres Gespräch zu führen, um mögliche Alternativen zu diskutieren. Alle Gesprächsteilnehmer waren sich einig, dass das geistige Eigentum zu schützen sei und die Rechte der Verlage und Autoren, v.a. auch der beteiligten Lehrkräfte, gewahrt werden müssen. Die Lehrerverbände werden weiter in die Gespräche einbezogen.“

### 6.1.2 Gut gemeint – schlecht gemacht: Werbemaßnahmen im Schulbereich

Wiederholt musste sich der LfD mit Eingaben auseinandersetzen, die datenschutzrechtlich problematische Kooperationen von Schulen mit privaten Institutionen zum Gegenstand hatten.

So wollte ein Kreditinstitut den Schulanfängerinnen und -anfängern einen Geschenkgutschein in einem persönlichen Anschreiben überreichen und begehrte dafür von der Grundschule die Namen und Adressen der Erstklässlerinnen und Erstklässler. Nach § 60 Abs. 1 Grundschulordnung ist aber die Weitergabe von Unterlagen über Schülerinnen und Schüler sowie Eltern für Werbezwecke ausdrücklich untersagt. Hierauf wurde das Kreditinstitut mit der Bitte um künftige Beachtung hingewiesen.

In einem anderen bundesweiten Projekt sollten die Kinder im Schulsport gelaufene Kilometer sammeln, diese auf einer Karte eintragen und von der Lehrkraft abzeichnen lassen (sog. KIDS-Marathon). Als Belohnung winkten „tolle Preise“ bei der Abschlussveranstaltung. Die Erziehungsberechtigten sollten auf der Karte einwilligen, dass sie künftig über Produkte und Leistungen der Krankenkasse informiert werden. Der LfD bemängelte, dass die Einwilligung in die Verarbeitung von Daten für den Marathon nicht getrennt wurde von der Einwilligung in die Verarbeitung der Daten für Werbezwecke; auch wurde keine echte Wahlmöglichkeit im Sinne einer Ankreuz- oder Streichmöglichkeit offeriert. Die Krankenkasse reagierte

prompt und stellte eine neue datenschutzverträgliche Version des Anmeldeformulars vor.

Um die Mitgliedschaft von Kindern in einem Sportverein zu fördern, wurde im Bereich der Grundschulen mit Unterstützung des Bildungs- und des Innenministeriums ein „Mitmach-Coupon“ ausgeteilt, der – bei Bestätigung der Mitgliedschaft in einem Sportverein – zur Teilnahme an einem Gewinnspiel berechtigte. Die Preise wurden von privaten Firmen gesponsert. Allerdings war in dem Formular eine Mitwirkung der Erziehungsberechtigten nicht vorgesehen; ob und ggf. welche Daten an die Sponsoren übermittelt wurden, blieb offen. Einen Hinweis auf die Freiwilligkeit der Teilnahme suchte man vergebens. Nach Intervention des LfD wurden die erforderlichen Hinweise in dem Pass aufgenommen.

### 6.1.3 Orientierungshilfe „Videoüberwachung an Schulen“

Im Jahr 2009 hatte der LfD eine Umfrage zur Videoüberwachung an Schulen durchgeführt mit dem Ergebnis, dass von den rund 1.600 Schulen in Rheinland-Pfalz 85 Videomaßnahmen betreiben. Dabei kamen rund 200 Kameras zum Einsatz.

Umso wichtiger war es, für die Schulen in Abstimmung mit dem Bildungsministerium eine Orientierungshilfe zur Videoüberwachung bereitzustellen. Dies ist im Berichtszeitraum gelungen: Sie steht im Internetangebot des LfD unter folgendem Link zum Download zur Verfügung: http://www.datenschutz.rlp.de/downloads/oh/oh_vue_schulen.pdf.

Die Schulen, die den gemachten Angaben zufolge offenkundig gegen die Orientierungshilfe verstoßen hatten (Überwachung von Toiletten oder Krankenzimmern; Überwachung während des laufenden Schulbetriebs; Dauer der Speicherung von zwei Wochen oder mehr), wurden angeschrieben und gebeten, dass die schulischen Datenschutzbeauftragten die Verhältnisse vor Ort anhand der Orientierungshilfe überprüfen mögen. Die kritischen Fälle der Videoüberwachung im Schulbereich konnten so vollständig beseitigt werden.

## 6.2 Wissenschaft

### 6.2.1 Projekt „TexTraLog“ – Berührungslos auslesbare textilintegrierte Mikrosysteme und Einsatz eines „Forschungsbusses“ der Mainzer Verkehrsgesellschaft (MVG)

Der Sachverhalt des o.g. Forschungsprojektes, bei dem ein Linienbus der MVG zum Einsatz kam und auf das der LfD von der Ströer DERG Media GmbH angesprochen wurde, gestaltete sich alles andere als alltäglich.

Ziele des vom Bundesministerium für Bildung und Forschung geförderten und vom Fraunhofer-Institut für Zuverlässigkeit und Mikrointegration Berlin e.V. geleiteten Projekts waren u.a. die Entwicklung eines Abrechnungssystems für textile Werbeträger – hier die Fahrzeugsitze – sowie eines Systems für die Kontrolle und Planung der Fahrgastauslastung. Über mit Sensoren ausgestattete sog. „intelligente Fahrgastsitze“ werden automatisch für sich betrachtet anonyme soziodemographische Daten über die Fahrgäste des jeweiligen Fahrzeugs erfasst. Bei Feldversuchen mit dieser Technologie im ÖPNV wurden zusätzlich personenbeziehbare Videodaten in einem Bus der MVG aufgezeichnet. Mit diesen Aufnahmen wurden die von den Sensoren gesendeten Informationen (mathematische Druckkurven für die Kategorien Frau oder Mann, junge oder alte Person) verglichen. Dieser Abgleich fand noch im Verkehrsunternehmen statt und wurde benötigt, um fehlerhafte Angaben erkennen und die zum Einsatz kommende Software verbessern zu können. Von Bedeutung für die datenschutzrechtiche Bewertung war dabei noch, dass für die Mitarbeiterinnen und Mitarbeiter des Forschungsinstituts nur Aufnahmen in direktem Zusammenhang mit einer Druckkurve und somit nur für einen kurzen Moment einsehbar waren.

Das Projekt hatte datenschutzrechtliche Bedeutung, weil es sich bei den Videoaufnahmen, auf denen einzelne Personen identifiziert werden konnten, um die Verarbeitung personenbezogener Daten handelte. Da die Nutzung von personenbeziehbaren Videodaten zu den dargestellten Forschungszielen gesetzlich nicht geregelt ist, konnte dies nur auf der Grundlage einer Einwilligung der Fahrgäste erfolgen.

Eine Einwilligung ist aber nur dann wirksam, wenn sie auf der freien Entscheidung der betroffenen Fahrgäste beruht. Um dies zu erreichen, wurden seitens des LfD verschiedene Maßnahmen mit der MVG bzw. dem Forschungsinstitut vereinbart:

- An allen Fahrgasttüren wurde darauf hingewiesen, dass der Bus im Rahmen eines vom Bundesministerium für Bildung und Forschung geförderten Forschungsprojekts genutzt wird.
- Nur etwa die Hälfte der Sitzplätze wurde mit Sensoren ausgestattet und von Videokameras erfasst.
- Auf der Sitzfläche der mit Sensoren ausgestatteten Sitze wurde darauf hingewiesen, dass in diesem Bereich Videoaufnahmen zu wissenschaftlichen Zwecken erfolgen.

Der LfD hat unter diesen Voraussetzungen ausnahmsweise auf die Einholung einer schriftlichen Einwilligung verzichtet, da die Beachtung dieser Form den Forschungszweck erheblich beeinträchtigt hätte. Es wurde als ausreichend angesehen, dass ein Fahrgast trotz der dargestellten Informationen auf einem Sitz mit Sensor Platz nimmt und dadurch konkludent seine Einwilligung zur Nutzung der Videodaten erteilt. Aufgrund der o.g. Hinweise am und im Bus obliegt es vielmehr der freien Entscheidung der Fahrgäste, ob sie diesen Bus nehmen oder ob sie im Bus auf einem der von Videokameras erfassten Sitze Platz nehmen oder nicht.

Nachdem diese datenschutzrechtlichen Vorgaben erfüllt wurden, bestanden keine Bedenken des LfD, die Videoaufnahmen zu dem oben geschilderten Zweck zu verwenden.

### 6.2.2 Anforderungen an ärztliche Atteste als Nachweis von Prüfungsunfähigkeit

Schon im 14. Tätigkeitsbericht hatte sich der LfD mit den Anforderungen an ärztliche Atteste als Nachweis von Prüfungsunfähigkeit befasst (vgl. 14. Tb., Tz. 8.2.3). Er hatte keine datenschutzrechtlichen Probleme darin gesehen, dass zu diesem Zweck mindestens Art und Umfang der von der Ärztin oder vom Arzt aufgrund eigener Wahrnehmung getroffenen Tatsachenfeststellungen im Attest enthalten sind. Seitdem geben diese qualifizierten ärztlichen Atteste immer wieder Anlass für Anfragen von Studierenden sowie Ärztinnen und Ärzten nach deren datenschutzrechtlicher Zulässigkeit. Viele Betroffene sehen das Arztgeheimnis verletzt, wenn das Prüfungsamt genauere Angaben zum Krankheitsverlauf fordert und sich nicht lediglich mit der ärztlichen Feststellung „prüfungsunfähig“ zufrieden gibt. Zuletzt hatte der LfD in seinem 20. Tätigkeitsbericht nochmals darauf hingewiesen, dass grundsätzlich ein solches Vorgehen der Hochschulen datenschutzrechtlich nicht zu beanstanden ist (vgl. 20. Tb., Tz. 8.2.3).

Auch nach der hierzu ergangenen Rechtsprechung (u.a. Urteil des Bundesverwaltungsgerichts vom 6. August 1996, Az. 6 B 17/96) kann Prüfungskandidatinnen und -kandidaten auferlegt werden, den Krankheitszeitraum, die Termine der ärztlichen Behandlung, Art und Umfang der Erkrankung (Befundtatsachen) sowie die Auswirkungen der Erkrankung auf die Prüfung durch eine besondere ärztliche Bescheinigung nachzuweisen.

Denn im Prüfungsverfahren muss besonders auf den Grundsatz der Chancengleichheit geachtet werden. Wer im Verhältnis der Kandidatinnen oder Kandidaten untereinander einen rechtlichen Vorteil in dem Sinne für sich in Anspruch nehmen will, dass ein offiziell angemeldeter Prüfungstermin nicht zählen soll, obwohl insoweit ein Prüfungsrechtsverhältnis besteht, das zum Antritt der Prüfung verpflichtet, hat die für die Nichterreichung des Prüfungstermins tragenden Gründe glaubwürdig und nachvollziehbar offenzulegen.

Solche Atteste wurden von Prüfungsordnungen bei Abschlussprüfungen (Diplom/Staatsexamen) regelmäßig bereits bei einer erstmalig vorgetragenen Prüfungsunfähigkeit verlangt. In der fortschreitenden Umstellung der Prüfungsordnungen, weg von Abschlussprüfungen hin zu kontinuierlichen Leistungsbewertungen über den gesamten Zeitraum des Studiums (Bachelor/Master), die in einer Gesamtnote enden, sah der LfD Anlass, die bisherige Verfahrensweise zu ändern und datenschutzfreundlicher zu gestalten:

Während die alten Prüfungsordnungen nur ein oder zwei abschlussrelevante Prüfungszeiträume vorsahen, in denen die Prüflinge ggf. ein entsprechend qualifiziertes ärztliches Attest vorzulegen hatten, sehen die neuen Prüfungsordnungen vor, dass jede Prüfung ab dem ersten Semester in die Abschlussnote mit einfließt. Durch die gestiegene Zahl der abschlussrelevanten Prüfungszeiträume würde die Intensität der Belastung der Kandidatinnen und Kandidaten durch eine unveränderte Beibehaltung der Regelung zur Glaubhaftmachung von Prüfungsunfähigkeit ansteigen, während die Bedeutung des jeweiligen Prüfungszeitraums für den Abschluss deutlich abnimmt.

Hierdurch sah der LfD die Verhältnismäßigkeit der Regelung in ihrer bisherigen Form nicht mehr gewahrt. Um die Belastung der Prüflinge zu reduzieren und so die Verhältnismäßigkeit der Anforderungen an die Glaubhaftmachung der Prüfungsunfähigkeit gegenüber dem informationellen Selbstbestimmungsrecht der Prüflinge wiederherzustellen, wurde gegenüber dem Wissenschaftsministerium angeregt, dass bei einer erstmalig vorgetragenen Prüfungsunfähigkeit ein einfaches ärztliches Attest, welches lediglich die Prüfungsunfähigkeit aus ärztlicher Sicht bescheinigt, aber keine der o.g. weiteren Angaben

enthält, regelmäßig ausreichen soll und erst ab der zweiten von den Kandidatinnen und Kandidaten geltend gemachten Prüfungsunfähigkeit ein qualifiziertes ärztliches Attest nach o.g. Maßstäben erforderlich ist.

Das Wissenschaftsministerium hat dem Vorschlag entsprochen, so dass den Studierenden ab der zweiten „Krankmeldung“ eine Wahlmöglichkeit zwischen einem amtsärztlichen Attest oder einem qualifizierten Attest der behandelnden Ärztinnen oder Ärzte mit den o.g. Maßstäben eingeräumt wurde.

Trotzdem wandten sich während des Berichtszeitraumes nach wie vor Studierende und v.a. behandelnde Ärztinnen und Ärzte an den LfD, weshalb das Wissenschaftsministerium um Stellungnahme gebeten wurde, wie viele Hochschulen die neue Verfahrensweise bereits eingeführt haben.

### 6.2.3 Wissenschaftspreis des LfD

Im Berichtszeitraum wurde zum zweiten und dritten Mal im Landtag Rheinland-Pfalz der Wissenschaftspreis des LfD verliehen. Der Preis zeichnet herausragende wissenschaftliche Arbeiten mit Datenschutzbezug aus, die an rheinland-pfälzischen Hochschulen erstellt wurden, und soll die wissenschaftliche Auseinandersetzung mit datenschutzrechtlichen Fragen fördern.

Der im Kreis der Datenschutzbeauftragten bislang einzige Preis dieser Art wird gemeinsam vom Ministerium für Bildung, Wissenschaft, Jugend und Kultur und dem LfD getragen und ist je Preiskategorie mit 1.000 Euro dotiert.

Für das Jahr 2009 wurde der Datenschutzpreis für eine an der an der Universität Kaiserslautern bzw. am Institut für Experimentelles Software Engineering der Fraunhofer-Gesellschaft erstellte Bachelorarbeit zur Kontrolle von Datenflüssen in heterogenen IT-Systemen verliehen. Im Rahmen der Preisverleihung betonte der Staatssekretär des Wissenschaftsministeriums, dass es für das Datenschutzgrundrecht nicht allein darauf ankomme, wehrhaft zu sein. Angesichts einer sich permanent verändernden Informationstechnik bedürfe es einer wissenschaftlichen Begleitung des Datenschutzes und einer angemessenen Medienkompetenz der Betroffenen.

In seiner Preisrede zum Thema „Modernisierung des Datenschutzes“ stellte Prof. Roßnagel, Datenschutzexperte und Vizepräsident der Universität Kassel dar, dass die technische Entwicklung die bisherigen Regelungskonzepte zunehmend in Frage stelle und eine grundlegende Modernisierung des Datenschutzes erforderlich sei. Um in Zeiten des globalen Internets, allgegenwärtiger Informationstechnik und zunehmend komplexer werdender Datenverarbeitungsprozesse noch selbst über die Verwendung von Daten bestimmen zu können, bedürfe es einer Allianz von Recht und Technik und der Transparenz von Datenverarbeitungsstrukturen und Datenschutzanforderungen, die sich nicht ausschließlich an datenverarbeitende Stellen, sondern auch an Herstellerinnen und Hersteller sowie Anbieterinnen und Anbieter von IT-Lösungen richteten.

Hierfür leistet nach Auffassung des LfD die mit dem Datenschutzpreis ausgezeichnete Arbeit einen wertvollen Beitrag. Ein zeitgemäßer Datenschutz muss mit der technischen Entwicklung Schritt halten und den Herausforderungen auch auf technischer Ebene begegnen. Daneben bedarf es aber auch der Schaffung eines angemessenen Datenschutzbewussteins bei den Betroffenen. Datenschutz ist mehr denn je nicht nur eine Frage von Recht und Technik, sondern auch von Bildung und Erziehung.

Bei der dritten Ausschreibung wurde der Wissenschaftspreis erstmals in allen drei Kategorien vergeben. Gemeinsam mit dem Ministerium für Bildung, Wissenschaft, Jugend und Kultur zeichnete der LfD in der Kategorie „Recht und Sozialwissenschaften“ eine Dissertation zur Zusammenarbeit von Polizei und Nachrichtendiensten im Lichte des Trennungsgebotes aus. Die Arbeit setzt sich mit Blick auf das Trennungsgebot als verfassungsrechtlichem Leitprinzip für die Zusammenarbeit zwischen Polizeien und Nachrichtendiensten kritisch mit den Regelungen des Antiterrordateigesetzes auseinander. Unter verschiedenen Gesichtspunkten werden die Regelungen auf ihre Vereinbarkeit mit dem Recht auf informationelle Selbstbestimmung untersucht, die dabei auftretenden Probleme näher beleuchtet und Reformvorschläge vorgestellt.

In der Kategorie „Technik und Informatik“ wurde eine Dissertation über die Entwicklung einer Architektur zum Schutz der Privatsphäre bei der Nutzung von kontextbezogenen Diensten im mobilen Umfeld ausgezeichnet. Sie beschreibt vor dem Hintergrund einer zunehmend mobilen Internetnutzung am Beispiel standortbasierter Dienste die Gefahren für die Privatsphäre und das Recht auf informationelle Selbstbestimmung der Nutzerinnen und Nutzer und entwickelt eine Architektur, mit der eine datenschutzfreundliche Nutzung mobiler Dienste möglich ist.

Ein Sonderpreis wurde an die Konzeption eines Schülerlabors verliehen, welche die verschiedenen Aspekte der datenschutzrelevanten Punkte zum Thema RFID, wie sie z.B. in Personalausweisen und Reisepässen oder im

Handel bereits vielfach zum Einsatz kommt, beleuchtete. Mit dem Lernprojekt wurde dabei ein Ansatz verfolgt, der bereits in der Schule methodisch und didaktisch Sensibilität für die Technologie und damit verbundene Chancen und Risiken schafft.

In der Preisrede stellte der Datenschutzbeauftragte der Google Germany GmbH die technischen Möglichkeiten vor, mit denen Nutzerinnen und Nutzer sich über die Datenverarbeitung durch Google informieren und diese steuern können.

Der LfD verknüpft den Preis mit der Erwartung, dass sich die Hochschulen in ihren wissenschaftlichen Disziplinen noch stärker als bisher mit Datenschutzfragen befassen. Ein zeitgemäßer Datenschutz ist angesichts der Durchdringung nahezu aller Lebensbereiche mit Informationstechnik und der Veränderungen, die das Internet mit sich bringt, auch auf eine Unterstützung seitens der Hochschulen angewiesen. Die damit verbundenen rechtlichen und technischen Fragen bedürfen einer wissenschaftlichen Begleitung und Evaluation.

Wissenschaftspreis des LfD
Informationen zum Wissenschaftspreis und die bislang ausgezeichneten Arbeiten sind unter folgender Adresse verfügbar:
http://www.datenschutz.rlp.de/wissenschaftspreis/

# 7. Kommunales, Meldewesen und Statistik

## 7.1 Kommunales

### 7.1.1 Veröffentlichungen im Internet: Solarkataster verschiedener Kommunen

In der ersten Jahreshälfte 2010 erhielt der LfD von den Planungen zweier Kommunen Kenntnis, sog. Solarkataster im Internet zu veröffentlichen. Diese Thematik hat den LfD seitdem kontinuierlich über den gesamten Berichtszeitraum hinweg beschäftigt. Nachdem verschiedene Kommunen ihre Kataster nach entsprechenden Hinweisen des LfD datenschutzkonform gestalteten, kam es in einem Fall zu einer Beanstandung gemäß § 25 LDSG, d.h. der förmlichen Missbilligung eines Verstoßes gegen § 5 Abs. 1 LDSG. Da sich die Kommune trotz intensiver Bemühungen nicht der Rechtsauffassung des LfD anschloss, leitete er deren Durchsetzung mit den Mitteln der Kommunalaufsicht ein.

Dazu im Einzelnen: Die Veröffentlichung von Eignungsdaten zur Solarnutzung von Dachflächen im Internet erfolgt regelmäßig, indem auf den entsprechenden Internetseiten Straßennamen und Hausnummern zur Auswahl angeboten werden oder alternativ dazu in einem digitalen Stadtplan und georeferenzierten Luftbildern einzelne Grundstücke ausgewählt werden können. Zu der anschriftenbezogenen Information zum Eignungsgrad der Dachfläche für die Installation einer Fotovoltaikanlage (Solareignung) sind auch Angaben z.B. zur Modulfläche, zum potenziellen Stromertrag, der zu erwartenden $CO_2$ – Einsparung, zu der Höhe der notwendigen Investitionen und zu den zu erwartenden Einnahmen erhältlich.

Datengrundlage sind in der Regel Geobasisinformationen des amtlichen Vermessungswesens, wie georeferenzierte Gebäudeadressen und Luftbilder. Das Potential jedes Einzeldaches wird mit Hilfe von spezieller Datenverarbeitungssoftware ausgewertet.

Den Zweck eines solchen Katasters sieht das Umweltministerium darin, der Bürgerschaft eine Erstinformation über das theoretische Solarpotential der jeweiligen Dachflächen zu geben. In der mangelnden Kenntnis der Solareignung ihres Daches wird für die Betroffenen eine Hürde gesehen, entsprechende Planungen anzugehen.

Bei den Angaben zu Ort, Straße, Hausnummer i.V.m. mit der Solareignung eines Gebäudedaches sowie der oben bereits genannten Daten handelt es sich um personenbeziehbare Daten i.S. des § 3 Abs. 1 LDSG; sie können über allgemein zugängliche Informationsquellen, wie z.B. ein Telefonbuch, unmittelbar auf die Bewohnerinnen und Bewohner bzw. die Eigentümerinnen und Eigentümer bezogen werden. Das Datenschutzrecht ist deshalb anwendbar.

Gemäß § 5 Abs. 1 LDSG ist die Verarbeitung personenbezogener Daten zulässig, soweit die Betroffenen eingewilligt haben oder das Landesdatenschutzgesetz oder eine andere Vorschrift dies erlaubt oder anordnet. Da in diesem Zusammenhang nicht geplant ist, eine Einwilligung einzuholen, und aufgrund der Anzahl der Betroffenen auch nicht praktikabel erscheint, hängt die Zulässigkeit der Internetveröffentlichung davon ab, ob sie gesetzlich gerechtfertigt ist.

Die Bezeichnung einer Dachfläche als für den Bau einer Photovoltaikanlage gut geeignet, geeignet oder nicht geeignet (Solareignung) wurde vom LfD als Umweltinformation im Sinne von § 2 Abs. 3 LUIG bewertet. Als bereichsspezifische Rechtsgrundlage für die Veröffentlichung dieser Information i.V.m. Ort, Straße und Hausnummer sowie Orthofotos (mit Geokoordinaten verknüpfte Luftbilder) im Internet kommt § 10 Abs. 1, Abs. 6 i.V.m. § 9 Abs. 1 LUIG in Betracht.

Das Landesgeodateninfrastrukturgesetz kommt nicht zur Anwendung, da § 2 Abs. 5 Nr. 2 LGDIG regelt, dass besondere Rechtsvorschriften in Bezug auf Geodaten und Geodatendienste, soweit sie Geodatenverarbeitung, Zugangsbeschränkungen oder Verwendungsvorbehalte betreffen, den Bestimmungen des Landesgeodateninfrastrukturgesetzes vorgehen.

Bei der Veröffentlichung von Umweltinformationen sind allerdings insbesondere die in § 9 Abs. 1 LUIG normierten Schranken zu beachten. Diese Schranken gelten auch für Internetveröffentlichungen, wie sich aus dem Verweis in § 10 Abs. 6 LUIG auf § 9 LUIG ergibt. Da der Weg der Einwilligung der Betroffenen nicht gewählt wird, hängt die Zulässigkeit der Veröffentlichung entsprechender Daten gem. § 9 Abs. 1 LUIG davon ab, dass das öffentliche Interesse an der Bekanntgabe die schutzwürdigen Interessen der Betroffenen überwiegt. Damit ist eine Interessenabwägung vorzunehmen.

Mit dem Solarkataster wird ein konkretes öffentliches Interesse verfolgt, nämlich die Förderung einer erneuerbaren Energie, letztlich also die Förderung des Klimaschutzes. Je mehr Personen Informationen aus dem geplanten Solarkataster in Anspruch nehmen und ggf. auch eine Solaranlage errichten, desto größer ist der Beitrag zum Klimaschutz. Zwar könnte der für eine Photovoltaikanlage in Betracht kommende Personenkreis

von den jeweiligen Kommunen auch auf dem Postweg über das Solarenergiepotential ihrer Häuser und deren Dächer unterrichtet werden. Doch wäre dies mit einem erheblichen Aufwand und Kosten verbunden. Durch die Bereitstellung der Daten im Internet wird dieses Ziel dagegen auf deutlich einfachere Art und Weise erreicht.

Allerdings ist mit der Internetveröffentlichung auch ein Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen verbunden. Dies kann nur hingenommen werden, wenn der Eingriff auf das Unabdingbare reduziert wird, wenn sich also die Internetveröffentlichung auf diejenigen Informationen beschränkt, die zur Realisierung der Ziele des Solarkatasters – Information der Betroffenen über die Möglichkeit der Errichtung einer Solaranlage und Werbung dafür – unabdingbar sind.

Dies bedeutet, dass im Internet i.V.m. mit Ort, Straße und Hausnummer sowie Orthofotos nur veröffentlicht werden darf, ob eine Dachfläche für eine Photovoltaikanlage gut geeignet, geeignet oder nicht geeignet ist.

Alle übrigen Informationen, wie z.B. über die Leistung einer Anlage oder deren Ertrag und erst Recht einen eventuell aufzunehmenden Darlehensbetrag, können auch außerhalb des Internets gegeben werden.

Die beteiligten Ministerien haben der grundsätzlichen rechtlichen Bewertung des LfD in dieser Angelegenheit zugestimmt. Auch die Kommunalen Spitzenverbände haben sich der Rechtsauffassung des LfD angeschlossen.

Eine Entschließung der Datenschutzbeauftragten des Bundes und der Länder zur gemeinsamen Handhabung scheiterte an dem Veto zweier Datenschutzbeauftragter, nach deren Auffassung auch die Veröffentlichung der bloßen Solareignung eines Daches im Internet nur mit informierter Einwilligung der Betroffenen erfolgen kann.

### 7.1.2 Verkehrsüberwachung

Ein Urteil des Bundesverfassungsgerichts vom 11. August 2009 (Az. 2 BvR 941/08) hat bei vielen Verkehrsteilnehmerinnen und -teilnehmern die Hoffnung geweckt, sich zukünftig gegen die Ahndung von Verkehrsverstößen erfolgreich wehren zu können.

Auslöser des Verfahrens war die Verhängung eines Bußgeldes in Höhe von 50,00 Euro wegen Überschreitung der Höchstgeschwindigkeit. Dieser Verkehrsverstoß wurde von der Ordnungsbehörde durch Videoaufzeichnung festgestellt. Hierbei wurde der gesamte Verkehr gefilmt, unabhängig davon, ob bei den aufgenommenen Fahrzeugen eine Geschwindigkeitsüberschreitung vorlag oder nicht. Die Maßnahme wurde auf einen Erlass des Wirtschaftsministeriums gestützt. Gegen diese Videoaufzeichnung legte der betroffene Verkehrsteilnehmer Verfassungsbeschwerde ein mit der Begründung, dadurch werde ohne eine hinreichende gesetzliche Grundlage in sein Grundrecht auf informationelle Selbstbestimmung eingegriffen. Das Bundesverfassungsgericht gab ihm Recht. Es sah in der Videoaufzeichnung einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung, der nur aufgrund einer hinreichenden Gesetzesgrundlage zulässig sein könnte. Ein als Verwaltungsvorschrift zu qualifizierender Erlass stelle keine solche Gesetzesgrundlage dar.

Das dargestellte Urteil bezieht sich allein auf anlassunabhängige Verkehrskontrollen. Anlassbedingte Aufzeichnungen, also solche, bei denen die Aufzeichnung erst z.B. nach Überschreiten einer vorab eingestellten Höchstgeschwindigkeit ausgelöst wird, sind von dem Urteil des Bundesverfassungsgerichts nicht betroffen und somit auch aus datenschutzrechtlicher Sicht grundsätzlich nicht als unzulässig zu beurteilen. Als Rechtsgrundlage für solche Aufzeichnungen sieht der LfD in Übereinstimmung mit dem OLG Koblenz und zahlreichen anderen Oberlandesgerichten § 46 Abs. 1 OWiG i.V.m. § 100h Abs. 1 Satz 1 Nr. 1 StPO als Rechtsgrundlage an. Dabei kann es dahin gestellt bleiben, ob die Aufzeichnung maschinell oder durch eine Beamtin oder einen Beamten ausgelöst wird. In beiden Fällen besteht ein Anfangsverdacht, der Voraussetzung für die Fertigung von Bildaufnahmen gem. § 100h Abs. 1 Satz 1 Nr. 1 StPO ist.

In Rheinland-Pfalz hat dieses Urteil eine datenschutzrechtliche Beschwerde über die Ahndung eines Geschwindigkeitsvertoßes aufgrund einer Videoaufzeichnung ausgelöst. Der LfD hat daraufhin das eingesetzte Aufzeichnungsverfahren vor Ort überprüft und konnte feststellen, dass dieses datenschutzrechtlich nicht zu beanstanden war.

### 7.1.3 Videoüberwachung in den Kommunen

Auch nach dem Abschluss des Arbeitsschwerpunktes „Videoüberwachung“ lässt dieses Thema den LfD nicht los. Immer wieder stellen die zusätzlich sensibilisierten Kommunen beabsichtigte Überwachungsmaßnahmen mit der Bitte um Stellungnahme aus datenschutzrechtlicher Sicht vor. Regelmäßig geht es dabei auch um öffentliche Plätze, die Ziel wiederholter Sachbeschädigungen, Verschmutzungen usw. sind.

Zunächst ist an dieser Stelle nochmals festzuhalten, dass jede Videoüberwachung ein Eingriff in das Persönlichkeitsrecht ist, denn alle Menschen haben das Recht, sich

in der Öffentlichkeit grundsätzlich frei zu bewegen, ohne dass ihr Verhalten durch Kameras aufgezeichnet wird. Gerade bei der Überwachung öffentlicher Straßen und Plätze handelt es sich aber um einen Eingriff mit großer Streubreite, weil eine Vielzahl von Personen, die den Eingriff nicht durch ihr Verhalten veranlasst haben, betroffen sind. Deshalb wird eine solche Maßnahme auch vom Bundesverfassungsgericht als Grundrechtsbeeinträchtigung von erheblichem Gewicht bewertet.

Bei solchen Vorhaben werden die Örtlichkeiten regelmäßig durch Mitarbeiterinnen und Mitarbeiter der Dienststelle des LfD in Augenschein genommen. Sofern an dem Vorhaben seitens der Kommune festgehalten und eine Überwachung grundsätzlich zulässig ist, berät der LfD die öffentliche Stelle hinsichtlich der Verhältnismäßigkeit der Maßnahme. Es wird z.B. darauf hingewiesen, wo eine Kamera anzubringen und wie ein Objektiv auszurichten ist, damit lediglich das gefährdete Objekt (Skulptur) bzw. ein definierter Bereich erfasst wird oder nur Übersichtsbilder aufgenommen werden. Teilweise werden entsprechende Vorhaben nach Prüfung der datenschutzrechtlichen Empfehlungen nicht mehr weiter verfolgt.

Die vom LfD ausgearbeitete und mit den Kommunalen Spitzenverbänden sowie dem Innenministerium abgestimmte Orientierungshilfe trägt dazu bei, die Anforderungen des Datenschutzes an solche Maßnahmen auf breiter Ebene bekannt zu machen und vielleicht den Plänen, öffentliche Plätze zu überwachen, bereits im Vorfeld entgegenzuwirken. Sie wurde an die Änderungen im Rahmen der Novellierung des Landesdatenschutzgesetzes, die im März 2011 in Kraft getreten sind, angepasst (vgl. Tz. I-2.3.1).

Denn § 34 LDSG differenziert nun zwischen bloßer Videobeobachtung (Monitoring) und Videoaufzeichnung, die tiefer in das informationelle Selbstbestimmungsrecht der Betroffenen eingreift. Weiterhin wurde eine gesetzliche Ermächtigung für den Einsatz von Kameraattrappen eingeführt, da auch er in das allgemeine Persönlichkeitsrecht der Betroffenen eingreift.

Schließlich konnte der im letzten Datenschutzbericht angesprochene Fall einer Kommune, die trotz der vom LfD geäußerten Bedenken eine Videokamera zur Überwachung eines öffentlichen Platzes in Betrieb nahm, im aktuellen Berichtszeitraum abgeschlossen werden (vgl. 22. Tb., Tz. 10.1.1). Nach der förmlichen Beanstandung dieser Vorgehensweise bedurfte es allerdings noch intensiver Bemühungen seitens des LfD sowie der Unterstützung der Kommunalaufsicht, bis die Kommune die streitige Kamera nicht nur deaktivierte, sondern schließlich auch demontierte.

Von Interesse ist noch, dass Beschwerden von Bürgerinnen und Bürgern nur selten die von einer öffentlichen Stelle betriebene Videoüberwachung betreffen. Eine Anfrage aus der Bürgerschaft allerdings betraf die Bundesgartenschau in Koblenz, wobei eine örtliche Feststellung jedoch nur geringen Nachbesserungsbedarf ergab.

Als Fazit kann festgehalten werden, dass dieses Arbeitsfeld auf Dauer im Blickfeld des LfD stehen wird.

### 7.1.4 Datenschutz und aktive Bürgerbeteiligung

Im Rahmen der Kommunal- und Verwaltungsreform sollen Aufgabenzuständigkeiten verändert und die Leistungsfähigkeit, die Wettbewerbsfähigkeit und die Verwaltungskraft der verbandsfreien Gemeinden und der Verbandsgemeinden im Interesse einer bestmöglichen Daseinsvorsorge für die Bürgerinnen und Bürger durch Gebietsänderungen verbessert werden. Gerade im Zusammenhang mit freiwilligen Veränderungen sind verschiedene Kommunen und mehrere Bürgerinnen und Bürger wegen einer datenschutzkonformen Durchführung von Bürgerbefragungen an den LfD herangetreten.

Der LfD geht davon aus, dass eine personenbezogene Datenverarbeitung in dieser Beziehung mangels Rechtsvorschrift nur auf der Grundlage einer Einwilligung der Betroffenen zulässig ist. Die Einwilligung ist nach dem Prinzip der sog. informierten Einwilligung nur wirksam, wenn sie auf der freien Entscheidung der Betroffenen beruht. Sie müssen abschätzen können, in was sie mit der Teilnahme an der Befragung einwilligen. Teilweise war kein Hinweis auf die Freiwilligkeit der Teilnahme vorgesehen. In einigen Fällen wurde die Beantwortung der Fragen fälschlicherweise als anonym bezeichnet, obwohl einzelne Personen durch die Zusammenfassung mehrerer personenbeziehbarer Merkmale, wie z.B. Datum des Zuzugs in die Gemeinde, Vereinszugehörigkeit, Alter und Geschlecht, bestimmbar waren. Die Verarbeitung personenbezogener Daten wurde mehrmals damit begründet, dass Manipulationen des Befragungsergebnisses durch Mehrfachäußerungen von ein und derselben Person mit dieser Vorgehensweise vermieden werden sollten. Dem könnte aber auch z.B. mit einer fortlaufenden Nummerierung der Fragebögen begegnet werden.

Wegen solcher Mängel mussten daher geplante Verfahren teilweise geändert oder zum Einsatz kommende Unterlagen korrigiert werden.

Im Übrigen ist immer der Grundsatz der Datenvermeidung und Datensparsamkeit im Blick zu behalten, wonach grundsätzlich keine oder zumindest so wenig personen-

bezogene Daten wie möglich zu verarbeiten sind. Es ist also vor Beginn eines Projekts zu prüfen, ob der mit einer Befragung verfolgte Zweck mit verhältnismäßigem Aufwand auch mit anonymen Daten erreicht werden kann.

Bei dieser Form der Bürgerbeteiligung ist es nicht geblieben. Wie die Ereignisse der letzten Zeit gezeigt haben, möchte die Öffentlichkeit zunehmend stärker in Entscheidungsprozesse eingebunden werden. Schon jetzt bieten Kommunen ihren Bürgerinnen und Bürgern z.B. an, sich personenbeziehbar über eine Online-Plattform aktiv an der Haushaltsaufstellung – sog. Bürgerhaushalt – mit Einsparvorschlägen usw. zu beteiligen.

Weitere Projekte zur sog. E-Partizipation laufen bereits. Außerdem hat eine interministerielle Arbeitsgruppe als Kernpunkte für mehr Bürgerbeteiligung bei Großprojekten u.a.

- eine offensive Information und aktive Bürgerbeteiligung vor, während und nach Abschluss von Raumordnungsverfahren,
- die dabei verstärkte Nutzung informeller, konsultativer Verfahren der Bürgerbeteiligung (z.B. Bürgerkongresse und -foren) sowie
- den Ausbau von Möglichkeiten der E-Partizipation (Online-Beteiligung)

identifiziert.

Deshalb hat der LfD Kontakt mit der Leitstelle „Ehrenamt und Bürgerbeteiligung“ in der Staatskanzlei aufgenommen, um Möglichkeiten der Zusammenarbeit oder gegenseitigen Unterstützung auszuloten. Denn es stellt sich die Frage, inwiefern der Datenschutz bei diesen Vorhaben Berücksichtigung findet bzw. wie insbesondere die Kommunen in diesem konkreten Zusammenhang für die Belange des Datenschutzes weiter sensibilisiert werden können.

## 7.2 Meldewesen

### 7.2.1 Allgemeines

Im letzten Tätigkeitsbericht wurde bereits über den Sachstand in Sachen Bundesmeldegesetz berichtet (vgl. 22. Tb., Tz 10.2.1). Mittlerweile liegt ein neuer Gesetzentwurf der Bundesregierung zur Fortentwicklung des Meldewesens vor (BR-Drs. 524/11 vom 2. September 2011). Der Entwurf sieht zwar Verbesserungen bei der Weitergabe von Meldedaten für Zwecke der Werbung und des Adresshandels vor, lässt allerdings maßgebliche datenschutzrechtliche Forderungen unberücksichtigt. Dies gilt v.a. für die vom LfD seit langem geforderte Abkehr von der bloßen Widerspruchsmöglichkeit zugunsten einer Einwilligungserklärung der Betroffenen bei der Weitergabe von Meldedaten. So müssen die Betroffenen auch künftig selbst aktiv werden, wenn sie die Übermittlung ihrer Meldedaten an Adressbuchverlage, öffentlich-rechtliche Religionsgesellschaften oder an das Bundesamt für Wehrverwaltung verhindern möchten. Gleiches gilt für die Weitergabe von Meldedaten für Jubiläumszwecke oder bei der Erteilung einer einfachen Melderegisterauskunft über das Internet.

Weiterhin soll nach dem Gesetzesentwurf bei der Weitergabe von Meldedaten innerhalb einer Verwaltungseinheit (also beim Abruf von Meldedaten durch andere Stellen der Verwaltung, z.B. Ordnungsamt oder Sozialamt) der Verweis auf § 7 LDSG wegfallen. § 7 LDSG regelt die Zulässigkeit der Einrichtung automatisierter Abrufverfahren. Durch diesen Verweis wurde insbesondere die Angemessenheitsprüfung bei der Einrichtung automatisierter Abrufverfahren und die vorherige Anhörungspflicht des LfD sichergestellt. Der Entwurf sieht stattdessen vor, dass die Leitung der Verwaltungseinheit über die Zulässigkeit automatisierter Meldedatenabrufe durch andere Stellen der Verwaltung entscheidet. Damit ist unklar geworden, ob bei Datenabrufen innerhalb einer Kommune nach wie vor § 7 LDSG zu beachten ist. Nach Auffassung des Innenministeriums ist dies jedoch der Fall. Der LfD wird sich dafür einsetzen, dass die Meldebehörden in Rheinland-Pfalz entsprechend unterrichtet werden.

Gelegentlich gelingt es dem LfD, sich bei der Bearbeitung von melderechtlichen Eingaben erfolgreich für die Betroffenen einzusetzen. So befürchtete ein Petent, der bei einer Kirche beschäftigt ist, seinen Arbeitsplatz zu verlieren, wenn dort der Umstand seiner eingetragenen Lebenspartnerschaft bekannt würde. Das Melderecht sieht in der Tat vor, dass den Kirchen die Begründung der Lebenspartnerschaft mitgeteilt werden „darf“. Die Übermittlung dieser Information liegt demnach im pflichtgemäßen Ermessen der zuständigen Meldebehörde. Bei dieser Ermessensausübung sind schutzwürdige Belange der Betroffenen zwingend zu beachten. Es liegt auf der Hand, dass der Verlust des Arbeitsplatzes schutzwürdige Interessen der Betroffenen beeinträchtigen würde. Das Innenministerium teilte die Rechtsauffassung des LfD und stellte daraufhin gemeinsam mit der Gesellschaft für Kommunikation und Wissenstransfer mbH (KommWis) sicher, dass im Verfahren „MESO“ die Datenübermittlung an die Kirche unterbunden wurde.

### 7.2.2 Elektronischer Personalausweis

Seit dem 1. November 2010 werden neue Personalausweise ausgegeben. Der neue Ausweis enthält neben der alten Funktionalität des Identitätsnachweises zwei neue Funktionen, die auf Wunsch genutzt werden können:

- die sog. eID-Funktion zum einfachen und verlässlichen Ausweisen im Internet;
- die Aufnahme einer qualifizierten elektronischen Signatur, mit der in elektronischer Form Verträge abgeschlossen werden können, die der Schriftform bedürfen.

Zusätzlich können auf dem Personalausweis auch Fingerabdrücke abgespeichert werden. Dies ist, im Gegensatz zum elektronischen Reisepass, jedoch nicht verpflichtend.

Der LfD weist darauf hin, dass die eID-Funktion bei über 16-jährigen Personen bei Ausgabe des Ausweises automatisch aktiviert ist. Er rät, sich vor Abholung des Ausweises darüber Gedanken zu machen, ob dieser Dienst tatsächlich benötigt wird, ob also beabsichtigt ist, häufig Dienste im Internet in Anspruch zu nehmen, bei denen ein Identitätsnachweis erforderlich ist. Dies können z.B. Einkäufe oder virtuelle Behördengänge sein. Wenn dies nicht der Fall sein sollte, sollte man diese Funktion gleich durch die Personalausweisbehörde deaktivieren lassen, weil diese Funktion (besonders im Verlustfall) auch missbraucht werden kann. Bei Bedarf kann sie jederzeit nachträglich wieder eingerichtet werden.

Das Aufbringen einer elektronischen Signatur erfolgt nur auf Antrag. Hierzu ist ein entsprechendes Zertifikat bei einem Signaturanbieter zu erwerben.

Bei der Nutzung des Ausweises im Internet sollte beachtet werden, dass der eigene PC sicher ausgestattet ist, damit es zu keinen unangenehmen Überraschungen kommt. Aktuelle Sicherheitsprogramme sind unerlässlich. Empfehlenswert ist es auch, nicht nur die einfachste Version eines Kartenlesers zu kaufen, sondern ein sog. Komfortlesegerät zu erwerben, das eine eigene Tastatur zur sicheren PIN-Eigabe besitzt. Dies ist sogar unerlässlich, wenn eine qualifizierte elektronische Signatur mit dem Ausweis genutzt werden soll.

Auf jeden Fall sollte das zum Personalausweis mitgelieferte Sperrkennwort sorgfältig aufbewahrt werden, damit bei Verlust des Ausweises sofort eine Sperrung erfolgen kann und eine unbefugte Nutzung oder Aktivierung der eID ausgeschlossen ist. (Sperrhotline 0 18 01 33 33 33)

Der LfD weist zudem darauf hin, dass als Folge der neuen Funktionalitäten des Personalausweises niemand mehr aufgefordert werden darf, seinen Ausweis zu hinterlegen. Dies hat der Gesetzgeber eindeutig geregelt. Als Erfolg des Datenschutzes ist auch zu nennen, dass es weder eine zentrale Bilddatenbank noch eine zentrale Datei der Fingerabdrücke der Personalausweisbesitzer geben wird.

## 7.3 Statistik: Durchführung der Volkszählung Zensus 2011

Nach umfangreichen Vorbereitungen startete am 9. Mai 2011 mit der Haushaltebefragung die „heiße Phase“ der ersten Volkszählung für die Bundesrepublik Deutschland seit 1981 (Ostdeutschland) bzw. 1987 (Westdeutschland). Damit wird einer Verordnung der Europäischen Union nachgekommen, wobei zwei Ziele verfolgt werden. Zum einen geht es um die Feststellung der amtlichen Einwohnerzahlen. Nach der Expertenansicht leben in Deutschland 1,3 Millionen Bürgerinnen und Bürger weniger als angenommen. Ob Länderfinanzausgleich, die Einteilung der Bundestagswahlkreise, die Stimmenverteilung der Bundesländer im Bundesrat oder die Sitze Deutschlands im Europaparlament – all das und vieles mehr hängt von aktuellen Einwohnerzahlen ab. Ein zweites wesentliches Ziel des Zensus ist es, Informationen u.a. zum Wohnraum, zur Bildung und zum Erwerbsleben zu gewinnen. Diese Informationen sind Grundlage z.B. für die Stadtentwicklungsplanung oder Wirtschaftsplanung.

Anders als bei früheren Volkszählungen wird bei diesem registergestützten Zensus nicht alle Bürgerinnen und Bürger befragt. Es wurden in erster Linie bestehende Register, wie z.B. die der Meldeämter oder der Bundesagentur für Arbeit, ausgewertet und zusammengeführt. Daraus wird der aus datenschutzrechtlicher Sicht gravierende Unterschied zur Volkszählung 1987 ersichtlich – nur etwa ein Drittel der Bevölkerung musste direkt befragt werden. Somit stellt der Zensus 2011 im Vergleich zur 1987 durchgeführten Volkszählung ein schonenderes Verfahren dar.

Der LfD hat die Vorbereitung des Zensus 2011 und alle bisher durchgeführten Phasen intensiv begleitet. Insbesondere wurde gemeinsam mit dem Statistischen Landesamt und dem Innenministerium eine Musterdienstanweisung mit technischem Anhang erarbeitet, auf die die Mitarbeiterinnen und Mitarbeiter der 36 Erhebungsstellen bei Kreis- und Stadtverwaltungen verpflichtet werden konnten. Auf diesem Weg konnte ein durchgängig hohes Datenschutzniveau v.a. bei der technischen Umsetzung mit der heterogenen Ausstattung vor Ort gewährleistet werden. Im Rahmen von stichprobenartigen örtlichen

Feststellungen durch den LfD wurde die Einhaltung dieser Anweisung sowie die Abschottung der Erhebungsstellen von den übrigen Verwaltungsbereichen gemeinsam mit dem Innenministerium und dem Statistischen Landesamt vor Ort geprüft und bewertet. Hierbei kam es insgesamt nur zu wenigen Defiziten, bei deren Beseitigung der LfD beratend zur Seite stand.

Auch bei der Erstellung des generischen Sicherheitskonzeptes des Statistischen Landesamtes gab es eine intensive Kooperation zwischen den Verantwortlichen beim Statistischen Landesamt und dem LfD. Die Umsetzung wurde ebenfalls im Rahmen einer Ortsbesichtigung in Bad Ems bewertet. Hierbei konnte festgestellt werden, dass die beschriebenen Maßnahmen größtenteils vorbildlich umgesetzt wurden. Zudem fand über mehrere Monate hinweg ein regelmäßiger Austausch zu technischen und rechtlichen Fragestellungen durch Telefonkonferenzen mit Vertreterinnen und Vertretern des Innenministeriums bzw. des Statistischen Landesamtes statt.

Als Fazit kann festgehalten werden, dass Maßnahmen des Datenschutzes und der Datensicherheit von den beteiligten Stellen mit der nötigen Konsequenz getroffen wurden und der Zensus 2011 in Rheinland-Pfalz bisher weitgehend reibungslos verlaufen ist. Hierfür spricht auch die überschaubare Zahl der Anfragen und Eingaben seit 1. April 2011 im Zusammenhang mit dem Zensus.

Ein bundesweiter datenschutzrechtlicher Problempunkt war der Umgang mit in den Meldedaten enthaltenen Übermittlungssperren wegen einer Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen. Hier wurde im Arbeitskreis Statistik der Datenschutzbeauftragten des Bundes und der Länder eine Verfahrensweise abgestimmt, mit der der Schutz der Betroffenen gewährleistet wurde. Dieser Punkt wird Bestandteil der Agenda der Datenschutzbeauftragten des Bundes und der Länder im Hinblick auf den nächsten Zensus sein.

Nachdem die Vor-Ort-Befragungen in Rheinland-Pfalz im August 2011 schon zu rund 97 Prozent abgeschlossen waren, wird das Augenmerk v.a. den Daten gelten, mit denen die Befragten identifiziert werden können. Denn eine Volkszählung in anonymisierter Form ist aus statistiktechnischen Gründen nicht möglich, da z.B. wegen der Rücklaufkontrolle für die Fragebögen und der notwendigen Prüfung auf Vollständigkeit und Vollzähligkeit konkrete Angaben benötigt werden. Diese als Hilfsmerkmale bezeichneten Personengrunddaten müssen nach der Datenerhebung so früh wie möglich gelöscht werden, damit der konkrete Bezug auf eine bestimmte Person aufgelöst wird. Für das Jahr 2012 sind daher weitere örtliche Feststellungen geplant.

Erste Ergebnisse des Zensus 2011, etwa die amtlichen Einwohnerzahlen, werden ab November 2012 erwartet.

# 8. Justiz

Der LfD besitzt im Bereich der Justiz nur eine eingeschränkte Prüfungskompetenz. So kann er Gerichte nicht in dem durch die Verfassung garantierten Bereich richterlicher Unabhängigkeit, sondern nur in Verwaltungsangelegenheiten kontrollieren.

Zu den Aufgaben des LfD gehört es andererseits, alle öffentlichen Stellen – also auch die Gerichte – zu beraten. Dieser Aufgabe ist der LfD im Berichtszeitraum als Ansprechpartner von Fragen, durch Fortbildungsangebote sowie durch Stellungnahmen zu Gesetzesvorhaben nachgekommen. Unter anderem hat er sich mit folgenden Themen befasst:

## 8.1 Datenschutz in der elektronischen Justiz

Unter elektronischer Justiz versteht man den Einsatz von Informationstechnologie innerhalb der Justiz und zwischen deren Organen sowie der öffentlichen Verwaltung und Privatpersonen. Sie ist Teil der Umwandlung analoger Verfahrensweisen behördlicher Institutionen in IT-Strukturen (E-Government).

Angefangen beim Mahnverfahren finden sich IT-Strukturen längst in fast allen Bereichen der Justiz – so im Handelsregister, Schuldnerverzeichnis, Grundbuch, aber auch bei der elektronisch geführten Akte oder der elektronischen Kommunikation von Gerichten und Staatsanwaltschaften untereinander.

Mit der Übertragung analoger Verfahren auf IT-Strukturen entstehen auch in der Justiz neue Probleme. Allerdings liegen sie bei Gerichten außerhalb der Kontrollbefugnisse des LfD. Nach Auffassung des Justizministeriums gehört die Einführung von IT-Strukturen bei Gerichten nicht zu den vom LfD zu kontrollierenden Verwaltungsaufgaben. Trotzdem war seine Beratungskompetenz gefragt; so diskutierte er beim 20. Deutschen Richter- und Staatsanwaltstag am 8. April 2011 in Weimar mit führenden Vertreterinnen und Vertretern aus Rechtsprechung und Lehre über Chancen und Risiken des ständig zunehmenden Einflusses moderner Kommunikationsmittel und Datenverarbeitungsprogrammen auf die richterliche Praxis und die Unabhängigkeit von Richterinnen und Richtern.

## 8.2 Strafprozess

### 8.2.1 Zeugenanschriften in Anklageschriften

Durch das Gesetz zur Stärkung der Rechte von Verletzten und Zeugen im Strafverfahren (Zweites Opferrechtsreformgesetz) vom 29. Juli 2009 sollte nicht nur der Schutz von Opfern im Strafverfahren gestärkt, sondern auch eine größere Rücksichtnahme auf das Persönlichkeitsrecht von Zeuginnen und Zeugen erreicht werden. Hierzu wurden die Bestimmungen über die Erstellung der Anklageschrift in der Strafprozessordnung mit Wirkung vom 1. Oktober 2009 geändert. Entgegen der bisherigen Regelung sind danach Zeuginnen und Zeugen grundsätzlich nur noch mit ihrem Wohn- oder Aufenthaltsort, nicht aber mit der vollständigen Anschrift in die den Angeklagten zuzustellende Anklageschrift aufzunehmen.

Die geänderte Gesetzeslage konnte sich zunächst in der Praxis nicht durchsetzen. Auf Initiative des LfD beabsichtigt das Ministerium der Justiz und für Verbraucherschutz nun eine Anpassung im Sinne des Zeugen- und Opferschutzes vorzunehmen. Die auf Anfrage des LfD seitens des Ministeriums veranlasste Länderumfrage hat auch in anderen Bundesländern Änderungsüberlegungen in Gang gesetzt.

### 8.2.2 Elektronische Aufenthaltsüberwachung (Elektronische Fußfessel)

Mit dem Gesetz zur Neuordnung des Rechts der Sicherungsverwahrung und zu begleitenden Regelungen wurde zum 1. Januar 2011 die Möglichkeit geschaffen, gefährliche Straftäterinnen und -täter, die unter Führungsaufsicht stehen, unter elektronische Aufenthaltsüberwachung zu stellen. Im Fokus der Norm stehen insbesondere Straftäterinnen und -täter, die aus der Sicherungsverwahrung entlassen wurden.

Die elektronische Aufenthaltsüberwachung umgangssprachlich als elektronische Fußfessel bezeichnet – wird am Fuß der zu überwachenden Person angebracht. Ein darin befindlicher elektronischer Sender bestimmt den Aufenthaltsort und übermittelt die Daten per Telefon-, Mobilfunknetz oder per GPS an die Überwachungsstelle.

Die ständige Überwachung stellt einen schweren Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen dar und bedarf daher im Einzelfall einer intensiven Abwägung. Neben der potentiellen Gefährlichkeit der überwachten Straftäterinnen und -täter muss dabei auch die Geeignetheit der Maßnahme konkret abgewogen werden.

Durch die Länder wurde eine gemeinsame Überwachungsstelle geschaffen, der aufgrund eines Staatsvertrages Überwachungsaufgaben der Führungsaufsichtsstelle übertragen werden können. Der LfD erhielt im Rahmen der Planung Gelegenheit zur Stellungnahme. Darin hat er darauf hingewiesen, dass neben der Abwägung im Einzelfall v.a. technisch-organisatorische Maßnahmen beachtet werden müssen, um die hochsensiblen Datensammlungen zu schützen. Außerdem hat er sich erfolgreich dafür eingesetzt, dass die gemeinsame Überwachungsstelle als eigenverantwortliche Stelle ausgestaltet wird. Hierdurch ist sie zum einen handlungsfähiger, ist aber auch nur einem Datenschutzgesetz – und zwar aufgrund ihres Sitzes dem hessischen – unterworfen. Andernfalls hätte die gemeinsame Überwachungsstelle je nach Einzelfall unterschiedliche Landesdatenschutzgesetze zu beachten gehabt und hätte der Kontrolle von sechzehn Aufsichtsbehörden unterstanden.

Der LfD wird die weitere Entwicklung und den Einsatz der elektronischen Fußfessel überwachen.

### 8.2.3 Bargeldlose Zeugenentschädigung – ohne Angabe der Bankverbindung

In rheinland-pfälzischen Gerichtsverfahren ist es nur noch in begründeten Ausnahmefällen vorgesehen, Zeugenentschädigung bar zu leisten. Um die Entschädigungsleistungen bargeldlos erbringen zu können, werden regelmäßig die Bankdaten der Zahlungsempfängerinnen und -empfänger als Entschädigungsnachweis sowie zur späteren Berechnung der Gerichtskosten zu den Verfahrensakten genommen. Hierdurch kann es bei Akteneinsichtnahme dazu kommen, dass die Bankdaten der Zeuginnen und Zeugen Dritten bekannt werden. Dies ist insbesondere bei schutzwürdigen Zahlungsempfängerinnen und -empfängern wie z.B. Polizistinnen und Polizisten u.U. problematisch.

Auf Initiative des LfD wurde seitens der Justiz kurzfristig dafür gesorgt, dass an schutzwürdige Zahlungsempfängerinnen und -empfänger eine Barauszahlung ermöglicht wird. Darüber hinaus wurde eine Programmanpassung der eingesetzten Software veranlasst, wodurch Anweisungsbeamtinnen und -beamte Bankdaten schutzwürdiger Zahlungsempfängerinnen und -empfänger in dem für die Verfahrensakten vorgesehenen Aktenausdruck unterdrücken können.

### 8.2.4 Vorratsdatenspeicherung

Bereits im letzten Tätigkeitsbericht hat der LfD ausführlich die Problematik der von der Europäischen Union geforderten und in Deutschland durch Änderungen des Telekommunikationsgesetzes eingeführten Vorratsdatenspeicherung geschildert (vgl. 22. Tb., Tz. 7.2).

Dort hat er auch auf das seinerzeit anhängige Verfahren vor dem Bundesverfassungsgericht hingewiesen. Dieses ist am 2. März 2010 durch eine wegweisende Entscheidung des Bundesverfassungsgerichts beendet worden (Az. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08).

Unmittelbar nach der Verkündigung des Urteils, bei der der LfD persönlich anwesend war, hat er dieses in einer Presseerklärung mit der Überschrift „Bundesverfassungsgericht bleibt Garant des Datenschutzes“ wie folgt gewürdigt:

> „Mit seiner heutigen Entscheidung zur sog. Vorratsdatenspeicherung hat das Bundesverfassungsgericht sich erneut als Garant des Datenschutzes erwiesen. In einer ersten Reaktion begrüßte der Landesbeauftragte für den Datenschutz, Edgar Wagner, die Grundsatzentscheidung des höchsten deutschen Gerichts, welche die gesetzlichen Grundlagen der Speicherung von Telekommunikationsdaten für nichtig erklärte.
>
> Mit nicht zu überbietender Deutlichkeit habe das Bundesverfassungsgericht einmal mehr den Bundesgesetzgeber korrigieren müssen, dem es nach wie vor nicht gelänge, dem Bürgerrecht auf Datenschutz ausreichend Rechnung zu tragen. Wagner hob hervor, dass
> 1. die bisherigen Vorratsdaten ausnahmslos zu löschen sind,
> 2. bis auf weiteres keine Vorratsdatenspeicherung mehr zulässig ist und
> 3. zukünftig eine Datenspeicherung nur unter engsten Voraussetzungen zulässig sein wird.
>
> Da das Bundesverfassungsgericht mit Blick auf die EU-Richtlinie zur Vorratsdatenspeicherung an der grundsätzlichen Speicherung von Telekommunikationsdaten nicht gerüttelt habe, müsse man jetzt auf europäischer Ebene diese Richtlinie korrigieren. Es sei ein ermutigendes Zeichen, dass die dort zuständigen Stellen – insbesondere die neue Vizepräsidentin der EU-Kommission Viviane Reding – angekündigt hätten, die Richtlinie überprüfen und ggf. korrigieren zu wollen.“

In der Folge des Urteils hat der LfD das Justizministerium aufgefordert zu berichten, ob und ggf. in welchem Umfang Informationen aus der für verfassungswidrig erklärten Vorratsdatenspeicherung in Gerichtsverfahren des Landes Eingang gefunden haben und wie gewährleistet werde, dass künftig keine Verwertung entsprechender Informationen erfolge. Im Ergebnis wurde festgestellt, dass die Justiz des Landes diese Fragen verfassungskonform lösen werde.

Die seinerzeit geäußerte Erwartung, die EU-Kommission werde die maßgebliche Richtlinie überprüfen und korrigieren, hat sich bislang nicht erfüllt. Eine Überprüfung wurde zwar durchgeführt, deren Ergebnis inzwischen veröffentlicht worden ist (Bewertungsbericht der Kommission an den Rat und das Europäische Parlament zur Richtlinie über die Vorratsdatenspeicherung – Richtlinie 2006/24/EG – vom 18. April 2011). Daraus hat sich nach Auffassung der EU-Kommission aber kein wesentlicher Änderungsbedarf bezüglich der EU-Richtlinie ergeben.

Der Streit in Deutschland darüber, ob und wie diese Richtlinie umzusetzen sei, ist nach wie vor heftig; ein Ende und auch nur eine Einigung der Regierungsfraktionen auf der Ebene des Bundes ist nicht abzusehen. Die Positionen derjenigen, die die Notwendigkeit jeder Vorratsdatenspeicherung bestreiten und allenfalls eine „Quick Freeze-Lösung“ mit kleinen Erweiterungen akzeptieren wollen, und auf der anderen Seite derjenigen, die Vorratsdaten als unabdingbar für die Strafverfolgung ansehen, stehen sich nach wie vor unversöhnlich gegenüber. Valide wissenschaftlich fundierte Erkenntnisse liegen weder für die eine noch die andere Position vor. Der LfD plädiert angesichts dieser Situation für äußerste Zurückhaltung des Gesetzgebers. Es kann nicht sein, dass ohne den klaren Nachweis der Wirksamkeit von Vorratsspeicherungen – und dieser Nachweis ist bislang weder von der EU-Kommission noch von der Bundesregierung erbracht worden – auf derart massive Weise in die Grundrechte unbescholtener Bürgerinnen und Bürger eingegriffen werde. Angesichts der vielfältigen Bedrohungen für die Privatsphäre ist die staatliche Erhebung und Speicherung höchstpersönlicher Daten „ins Blaue hinein“ das letzte, was wir brauchen (vgl. Tz. I-2.2).

### 8.2.5 Noch einmal: Quellen-TKÜ

An den Diskussionen um den sog. Staatstrojaner (vgl. Tz. I-3.5) wird deutlich, dass Technologien mittlerweile nicht nur unser Leben weitgehend mitbestimmen, sondern auch in die justiziellen Entscheidungsprozesse eingebunden sein müssen. Dies setzt ein zunehmendes Verständnis für technische Fragen bei den mit der Entscheidungsfindung befassten Richerinnen und Richtern sowie Staatsanwältinnen und Staatsanwälten voraus.

Jetzt können aber nicht alle Richterinnen und Richter oder Staatsanwältinnen und Staatsanwälte auch noch gleichzeitig Ingenieurinnen oder Ingenieure bzw. Informatikerinnen oder Informatiker sein. Oftmals wird auch keine Zeit dafür vorhanden sein, zunächst Sachverständige einzuschalten. Erforderlich sind vielmehr kompetente Ansprechpartnerinnen und -partner, die im Einzelfall kurzfristig für Fragen zur Verfügung stehen und technische Sachverhalte in einer für juristische Entscheidungen verwendbaren Weise erklären können. Wie der Direktor am Max-Planck-Institut für ausländisches und internationales Strafrecht, Professor Dr. Dr. h.c. Ulrich Sieber („Frankfurter Allgemeine Zeitung“ vom 3. November 2011), so spricht sich auch der LfD für die Einrichtung eines technischen Kompetenzzentrums bei der Justiz aus. Denn nur informierte Richterinnen und Richter sowie Staatsanwältinnen und Staatsanwälte können sachgerechte Entscheidungen treffen. Dies vertraten so auch der Minister der Justiz und für Verbraucherschutz und der Präsident des Verfassungsgerichtshofs und Oberverwaltungsgerichts Rheinland-Pfalz anlässlich des jährlich veranstalteten Treffens des LfD mit den Datenschutzbeauftragten der Justiz im November 2011.

### 8.2.6 Einsatz von stillen SMS durch Strafverfolgungs- und Gefahrenabwehrbehörden

Aufgrund von Presseveröffentlichungen ist die Frage erneut zum Gegenstand des öffentlichen Interesses geworden, unter welchen Voraussetzungen und in welchem Ausmaß das Instrument der „stillen SMS“ zu Zwecken der Standortfeststellung durch staatliche Stellen der Strafverfolgung und der Gefahrenabwehr eingesetzt wird und ob die bestehenden Rechtsgrundlagen für derartige Maßnahmen ausreichen. Die Problematik ist bereits im Jahr 2003 öffentlich erörtert worden (vgl. 19. Tb., Tz. 7.3.3).

Die Veröffentlichung neuer Statistiken mit hohen Abfragezahlen hat den LfD veranlasst, die zuständigen Ressorts (Innen- und Justizministerium) zu der Situation im Land zu befragen. Zur maßgeblichen Rechtsgrundlage hat er problematisiert, ob die Landesregierung die Auffassung der Bundesregierung teilt, dass eine derartige Maßnahme nur unter den Voraussetzungen erfolgen darf, die auch das Abhören von Telefonaten erlauben (§§ 100a, 100b StPO; vgl. BT-Drs. 15/1448). Er hat auch gefragt, ob es nach Auffassung der Landesregierung nicht angemessen wäre, für Standortfeststellungen mithilfe von „stillen SMS“ im Interesse der Normenklarheit besondere Rechtsgrundlagen zu schaffen. Dafür plädiert der LfD. Eine Antwort liegt noch nicht vor. Die Diskussion hierüber wird aber weitergehen müssen.

### 8.2.7 Massenhafte Funkzellenabfrage

Anfang 2011 war es in einem anderen Bundesland im Zusammenhang mit Ermittlungen wegen besonders schwerem Landfriedensbruch zu sog. Funkzellenabfragen

gekommen, bei denen 896.072 Verkehrsdaten erhoben worden waren, was von dem zuständigen Datenschutzbeauftragten beanstandet wurde.

Funkzellen stellen den Bereich dar, in dem das von einer Sendeeinrichtung eines Mobilfunknetzes gesendete Signal empfangen und fehlerfrei decodiert werden kann. Mit einer Funkzellenabfrage beim Netzbetreiber können Ermittlungsbehörden, wenn die Nummer oder sonstige Kennung einer Zielperson noch nicht bekannt ist, die Verkehrsdaten aller Mobilfunkteilnehmerinnen und -teilnehmer erheben, die sich in einem bestimmten Zeitraum in einer näher bezeichneten Funkzelle aufhalten oder aufgehalten haben. Da durch diese Maßnahme erwartungsgemäß eine große Anzahl an Daten Nichtbeteiligter erhoben wird, kommt der Verhältnismäßigkeitsabwägung eine besondere Bedeutung zu. Gemäß § 100g Abs. 2 i.V.m. § 100b Abs. 1 StPO darf die Anordnung – soweit keine Gefahr im Verzug vorliegt – auf Antrag der Staatsanwaltschaft nur durch die zuständige Ermittlungsrichterin oder den zuständigen Ermittlungsrichter getroffen werden.

Eine Anfrage des LfD an das rheinland-pfälzische Justizministerium ergab lediglich einen Fall, in dem 2009 seitens einer rheinland-pfälzischen Staatsanwaltschaft 23.375 Verbindungsdaten durch eine Funkzellenabfrage erhoben worden waren. Der Umfang der Erhebung lag damit weiter hinter dem Dresdner Verfahren. Außerdem ging es um die Aufklärung eines Tötungsdelikts. Der LfD hat dennoch die Prüfung des Verfahrens aufgenommen, die allerdings noch nicht abgeschlossen ist.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich in der Entschließung „Funkzellenabfrage muss eingeschränkt werden!“ vom 27. Juli 2011 dafür ausgesprochen, gesetzliche Regelungen zu schaffen, um Funkzellenabfragen zu beschränken, dem Grundsatz der Verhältnismäßigkeit zu stärkerer Beachtung zu verhelfen und die in § 101 Abs. 8 StPO vorgesehene Löschungsregelung zu präzisieren.

## 8.3 Strafvollzug

### 8.3.1 Orientierungshilfe zur Videoüberwachung im Justizvollzug

Vollzugsanstalten sind typischerweise ein intensiv überwachter Bereich. Dabei spielt die Videoüberwachung eine große Rolle. Neben Gefangenen werden von Videoüberwachungsanlagen in den Anstalten auch Bedienstete, tätige Firmen oder Besucherinnen bzw. Besucher erfasst. Der Grad der Betroffenheit hängt dabei von der Intensität des jeweiligen Videoüberwachungseinsatzes ab. Zu unterscheiden sind einerseits das bloße Monitoring, bei dem über die Videoanlage nur eine Beobachtung, nicht aber eine Aufzeichnung stattfindet, und andererseits die Videoaufzeichnung, bei der die beobachteten Inhalte aufgezeichnet werden.

Die Strafvollzugsgesetze enthalten Regelungen, nach denen sich jeweils bestimmt, ob eine Videotechnik zur Überwachung eingesetzt werden darf. Nicht geregelt ist hierbei, wie der Einsatz im Einzelfall konkret ausgestaltet werden kann. Die für den Justizvollzugsbereich erarbeitete Orientierungshilfe ist eine Anleitung, um einen datenschutzgerechten Einsatz der Videotechnologie unter Beachtung der Interessen des Vollzugs und der Betroffenen zu ermöglichen. Sie stellt einen weiteren Beitrag des LfD für einen aktiven und verbesserten Datenschutz in der Justiz dar.

### 8.3.2 Hinweis „Blutkontakt vermeiden“ vermeidbar

Die Deutsche Aidshilfe hatte festgestellt, dass es in deutschen Justizvollzugsanstalten teilweise zur Unterrichtung von Bediensteten über HIV-Infektionen von Gefangenen ohne deren Einwilligung gekommen sei. Dabei sei der Hinweis „Blutkontakt vermeiden“ bzw. ein entsprechendes Kürzel in das verwendete EDV-System aufgenommen worden. Diese Bekanntmachung stellt eine Übermittlung äußerst sensibler personenbezogener Gesundheitsdaten dar, die mangels Einwilligung einer gesetzlichen Grundlage bedarf und danach erforderlich sein muss. Zum Schutz der Bediensteten ist der Hinweis jedoch nicht erforderlich. Bedienstete sind bereits durch die geltenden Sicherheits- und Gesundheitsbestimmungen ausreichend geschützt. Durch den Hinweis kann kein höherer Schutz für sie erreicht werden.

Auf Initiative des LfD wurden die Vollzugsanstalten durch das Ministerium der Justiz und für Verbraucherschutz angewiesen, derartige Hinweise zu unterlassen.

### 8.3.3 Justizvollzugsdatenschutzgesetz Rheinland-Pfalz

Zum 1. September 2006 ist die Gesetzgebungskompetenz für den Justizvollzug auf die Länder übergegangen. Mit der Schaffung des Landesjugendstrafvollzugsgesetzes und des Landesuntersuchungshaftsvollzugsgesetzes hat Rheinland-Pfalz hiervon bereits Gebrauch gemacht. Im September 2011 legte das Ministerium für Justiz und für Verbraucherschutz den Musterentwurf für ein einheitliches rheinland-pfälzisches Strafvollzugsgesetz vor. Es wird erwogen, alle drei Gesetze in einem weiteren Schritt zu einem Landesjustizvollzugsgesetzbuch

zusammenzuführen. Dabei könnten Bestimmungen zum Datenschutz im Justizvollzug sowie bei den sozialen Diensten und Führungsaufsichtsstellen der Justiz mitgeregelt werden. Auf Anfrage legte der LfD dem Ministerium der Justiz und für Verbraucherschutz im August 2011 den Entwurf für ein Gesetz zum Schutz personenbezogener Daten im Justizvollzug sowie bei den sozialen Diensten und Führungsaufsichtsstellen der Justiz des Landes Rheinland-Pfalz (Justizvollzugsdatenschutzgesetz) vor. Der Entwurf baut auf den Grundsätzen des Landesdatenschutzgesetzes auf und schafft in ausgewogener Weise einen Ausgleich zwischen einerseits dem Recht der vom Justizvollzug Betroffenen auf informationelle Selbstbestimmung und andererseits den vollzuglichen Interessen sowie den Anforderungen und Bedürfnissen eines modernen, sicherheitsorientierten sowie kostenbewussten Informationsmanagements. Mit seinen bereichsspezifischen Sonderregelungen dient er der gesetzlichen Vereinfachung und erhöht die Praktikabilität. Mit einer Umsetzung der Regelung ist jedoch frühestens ab Mitte 2012 zu rechnen.

# 9. Finanzen

Im Bereich der Steuerverwaltung hat sich der LfD im Berichtszeitraum insbesondere mit – den zugegeben nicht neu klingenden – folgenden drei Fragen befasst:

## ■ Darf ein Steuerpflichtiger wissen, was das Finanzamt über ihn weiß?

Mit dieser Frage hatte sich der LfD in seinem letzten Tätigkeitsbericht (vgl. 22. Tb., Tz. 12.2) ausführlich auseinandergesetzt und dabei der Hoffnung Ausdruck verliehen, dass er an dieser Stelle schon einen Erfolg der Bemühungen der Datenschutzbeauftragten verkünden könnte. Die Hoffnung trügt nicht ganz. Denn es sind tatsächlich Tendenzen zu erkennen, dass das Bundesfinanzministerium von seiner ursprünglichen Linie abrückt und zukünftig nicht mehr die Darlegung eines berechtigten Interesses verlangt, bevor die Finanzverwaltung überhaupt tätig wird und über das Auskunftsbegehren entscheidet. Die Frage wird den LfD daher wahrscheinlich auch noch im nächsten Tätigkeitsbericht beschäftigen.

## ■ Wird die Steueridentifikationsnummer (Steuer-ID) zum Personenkennzeichen?

Bereits vor Einführung der Steuer-ID haben die Datenschutzbeauftragten davor gewarnt, sie nicht zum allgemeinen Personenkennzeichen werden zu lassen (vgl. 22. Tb., Tz. 12.1). Eine entsprechende Absicht wurde vom Gesetzgeber stets verneint. Dennoch wird die Steuer-ID mittlerweile in den verschiedensten Lebensbereichen verwendet. Nicht nur öffentliche Stellen erheben sie, sondern auch immer mehr nicht-öffentliche Stellen wie Kreditinstitute, Bausparkassen, Versicherungen oder Krankenkassen. Selbst wenn man Elterngeld beantragt, muss man seine Steuer-ID angeben. Oft wissen die Betroffenen gar nicht, wer ihre Steuer-ID zu welchem Zweck verwendet und welche weiteren Daten damit verknüpft sind.

Eine Abschaffung zu fordern, wäre illusorisch. Daher werden sich die Datenschutzbeauftragten gemeinsam weiterhin dafür einsetzen, dass bestimmte Anforderungen beachtet werden: Die unter der Steuer-ID erfassten Daten sind auf ein Minimum zu beschränken. Sie dürfen nicht auf Vorrat gespeichert werden. Der strenge Zweckbindungsgrundsatz der Steuer-ID muss auch für die mit ihr verbunden Daten gelten. Die Steuer-ID ist grundsätzlich zunächst bei den Betroffenen selbst zu erheben. Die Sanktionierungsmöglichkeiten bei Missbrauch müssen verschärft werden.

## ■ Dürfen Kreditinstitute wissen, welcher Religion ihre Kundinnen und Kunden angehören?

Zinseinkünfte z.B. aus Sparguthaben müssen versteuert werden. Die Einführung der Abgeltungssteuer auf Zinseinkünfte soll es dem Steuerpflichtigen einfacher machen. Kreditinstitute z.B. führen einen bestimmten Prozentsatz der Einkünfte – anonym – an das Finanzamt ab. Damit ist die Steuerschuld „abgegolten“, Sparerinnen und Sparer müssen für ihre Zinseinkünfte keine Steuererklärung mehr abgeben, und der Staat hat die ihm zustehende Steuer. Bei der ebenfalls fälligen Kirchensteuer ist dies etwas schwieriger. Denn hier ist das Finanzamt nur Verteiler der Gelder, eigentlicher Steuergläubiger ist die Kirche, der die Sparerinnen und Sparer angehören. Also muss das Finanzamt wissen, an welche Religionsgemeinschaft es wie viel Abgeltungssteuer weiterleiten muss. Bisher konnten sich die Sparerinnen und Sparer aussuchen, ob sie gegenüber ihrer Bank angeben, ob und welcher Religionsgemeinschaft sie angehören. Haben sie diese Daten preisgegeben, konnte der entsprechende Steuerbetrag auch wieder anonym, aber mit genauer Empfängerbezeichnung, abgeführt werden.

Sparerinnen und Sparer konnten aber auch darauf verzichten, ihrem Kreditinstitut gegenüber die doch besonders sensible Information über die Religionszugehörigkeit preiszugeben und waren dann verpflichtet, ihre Zinseinkünfte gegenüber dem Finanzamt zu erklären. Diese Wahlmöglichkeit soll zukünftig entfallen. Vielmehr sollen die Banken berechtigt sein, mit der zusätzlich zu erhebenden Steuer-ID beim Bundeszentralamt für Steuern die Religionszugehörigkeit ihrer Kundinnen und Kunden zu erfragen, um die abzuführende Kirchensteuer zuordnen können. Damit werden alle Kreditinstitute und sonstigen Zinsen auszahlenden Institutionen Kenntnis über das besonders sensible Datum der Religionszugehörigkeit erhalten. Gegen diese Massendatenerhebung und –speicherung hoch sensibler Daten haben die Datenschutzbeauftragten im Bund und den Ländern hart gekämpft. Wenigstens konnte erreicht werden, dass die Sparerinnen und Sparer vor Abfrage ihrer Religionszugehörigkeit darüber informiert werden sollen, dass sie der Abfrage widersprechen können und dann eine Steuererklärung abgeben müssen. Diese Widerspruchsmöglichkeit ist natürlich viel weniger als eine ausdrückliche Einwilligung. Denn wollen die Betroffenen den Datenfluss verhindern, müssen sie aktiv werden.

Ein großes Augenmerk wird darauf zu richten sein, dass die Kreditinstitute und andere Zinsen ausschüttende Institutionen das besonders sensible Datum der Religionszugehörigkeit getrennt vom Kundendatensatz

speichern und auch nur für die Zwecke der Besteuerung nutzen.

Die datenschutzrechtlichen Fragen im Bereich der Finanzverwaltung sind komplex und beschäftigen den LfD konstant.

Darüber hinaus zeigen auch Eingaben von Steuerpflichtigen an den LfD, dass der Datenschutz gerade in der Steuerverwaltung von den Betroffenen durchaus sensibel wahrgenommen wird, etwa wenn die Finanzämter Belege in Umschlägen zurücksenden, die nicht fest verschlossen sind.

# III. Aus der Dienststelle

Gemessen an ihren vielfältigen Aufgaben hat die Dienststelle des LfD nur eine schmale personelle Ausstattung. Dies wird auch nicht dadurch erträglicher, dass der LfD nach der Entscheidung des Europäischen Gerichtshofs mit völliger Unabhängigkeit ausgestattet ist. Im Gegenteil: Setzte man diese Entscheidung konsequent um, müsste der LfD auch den die Dienststelle betreffenden Vollzug des Haushalts und der einschlägigen Verwaltungsangelegenheiten übernehmen. Dies wird zur Zeit von der Verwaltung des Landtags übernommen, was außerordentlich sinnvoll ist, weil es den LfD einerseits entlastet und andererseits ein hilfreiches Korrektiv sein kann. Auch wenn dies der vom Europäischen Gerichtshof geforderten völligen Unabhängigkeit des LfD möglicherweise nicht entspricht, möchte der LfD doch darauf nicht verzichten – selbst wenn er die für die Selbstwahrnehmung dieser Aufgaben erforderlichen Planstellen erhielte. Die – lose – Anbindung an den Landtag, die dem LfD auch eine privilegierende Nähe zum Landtagspräsidenten vermittelt, ist letztlich höher zu veranschlagen als eine völlige Unabhängigkeit, die den LfD am Ende alleine stehen lässt. Es besteht deshalb Anlass, sich in diesem Zusammenhang bei der Landtagsverwaltung für die vielfältige Unterstützung und Beratung zu bedanken.

# Abkürzungsverzeichnis

## Gesetze und Verordnungen

| | |
|---|---|
| BDSG | Bundesdatenschutzgesetz |
| BeamtStG | Beamtenstatusgesetz |
| BZRG | Bundeszentralregistergesetz |
| GG | Grundgesetz |
| LBG | Landesbeamtengesetz |
| LDSG | Landesdatenschutzgesetz |
| LGDIG | Landesgeodateninfrastrukturgesetz |
| LKG | Landeskrankenhausgesetz |
| LKindSchuG | Landeskinderschutzgesetz |
| LKRG | Landesgesetz zur Weiterführung des Krebsregisters |
| LUIG | Landesumweltinformationsgesetz |
| LV | Landesverfassung |
| ÖGdG | Landesgesetz über den öffentlichen Gesundheitsdienst |
| OWiG | Ordnungswidrigkeitengesetz |
| POG | Polizei- und Ordnungsbehördengesetz |
| SchulG | Schulgesetz |
| SGB II | Sozialgesetzbuch – Zweites Buch – |
| SGB V | Sozialgesetzbuch – Fünftes Buch – |
| SGB X | Sozialgesetzbuch – Zehntes Buch – |
| SGB XI | Sozialgesetzbuch – Elftes Buch – |
| StGB | Strafgesetzbuch |
| StPO | Strafprozessordnung |
| TKG | Telekommunikationsgesetz |
| TMG | Telemediengesetz |

## sonstige Abkürzungen

| | |
|---|---|
| App | Application |
| Art. | Artikel |
| BITKOM | Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. |
| BR-Drs. | Bundesratsdrucksache |
| BT-Drs. | Bundestagsdrucksache |
| GPS | Global Positioning System |
| HIV | Humanes Immundefizienz-Virus |
| i.S. | im Sinne |
| i.V.m. | in Verbindung mit |
| JIM-Studie | Jugend, Information, (Multi-)Media; Basisuntersuchung zum Medienumgang 12- bis 19-jähriger in Deutschland |
| LfD | Landesbeauftragter für den Datenschutz Rheinland-Pfalz |
| LT-Drs. | Landtagsdrucksache |
| MdB | Mitglied des Deutschen Bundestages |
| MDK | Medizinischer Dienst der Krankenversicherung |
| MinBl. | Ministerialblatt |
| NADC | Nationaler Anti-Doping-Code |
| ÖPNV | Öffentlicher Personennahverkehr |
| RFID | Radio Frequency Identification |
| SWIFT | Society for Worldwide Interbank Financial Telecommunication |
| Tb. | Tätigkeitsbericht |
| TKÜ | Telekommunikationsüberwachung |
| Tz. | Textziffer |
| WLAN | Wireless Local Area Network |