# Datensicherheit in intelligenten Infrastrukturen

Sebastian Bretthauer, Ass. iur.; Thomas Bräuchle, Ref. iur.

Zentrum für Angewandte Rechtswissenschaft (ZAR)
Karlsruher Institut für Technologie (KIT)
Vincenz-Prießnitz-Straße 3
Geb. 07.08 (3. OG)
76131 Karlsruhe
(sebastian.bretthauer | thomas.braeuchle)@kit.edu

**Abstract:** Intelligente Infrastrukturen, wie etwa Smart Metering Systeme oder intelligente Videoüberwachung öffentlicher Räume, stellen große Herausforderungen an die IT-Sicherheit der Zukunft. Diese Systeme können einerseits klassischen manipulativen Eingriffen von Außen ausgesetzt sein, andererseits müssen mögliche Bedrohungen von Innen verhindert werden können. Zudem genügt eine isolierte Sicherheitsbetrachtung von Teilsystemen heutigen Anforderungen nicht mehr, da hierdurch die Funktionsfähigkeit des Gesamtsystems nicht gewährleistet ist. Technischer Datenschutz erfordert eine disziplinübergreifende Zusammenarbeit, um von sicheren Systemen sprechen zu können. Die so entstehenden Wechselwirkungen zwischen der juristischen und technischen Perspektive ermöglichen ein fachübergreifendes Verständnis von Sicherheit. Der Beitrag nimmt sich dieser Herausforderung an und beleuchtet dabei aus juristischer Sicht den Aspekt der Datensicherheit in intelligenten Infrastrukturen.

## 1 Einleitung

Am Karlsruher Institut für Technologie (KIT) existiert seit 2011 das Kompetenzzentrum für Angewandte Sicherheitstechnologie (KASTEL), ein vom Bundesministerium für Bildung und Forschung (BMBF) gefördertes Projekt, das deutschlandweit eines von drei Forschungszentren[1] für Cybersicherheit ist.[2] Um eine ganzheitliche Betrachtung intelligenter Infrastrukturen zu realisieren, ist ein disziplinübergreifender Konsens über den Sicherheitsbegriff nötig. Im Rahmen dieses interdisziplinären Vorhabens beschäftigt sich deshalb ein Teilprojekt[3] mit der Frage, wie sichere Systeme auszugestalten sind und

[1] Weitere Forschungszentren sind das „European Center for Security and Privacy by Design – EC-SPRIDE“ der Technischen Universität Darmstadt und das „Kompetenzzentrum für die IT-Sicherheitsforschung Sicherheit, Vertraulichkeit, und der Schutz der Privatsphäre in der digitalen Gesellschaft“ der Universität des Saarlandes.
[2] Siehe hierzu: http://www.kastel.kit.edu [abgerufen am 26.6.2013].
[3] Beteiligt sind unter anderem das Institut für Kryptographie und Sicherheit (IKS), Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB), Institut für Programmstrukturen und

welche Sicherheitsgarantien diese gewährleisten müssen. Dabei muss technischer und juristischer Sachverstand frühzeitig bei der Entwicklung sicherer Systeme Berücksichtigung finden. Gegenwärtig ist zu beobachten, dass informationstechnische Kommunikationsinfrastrukturen immer mehr personenbezogene Daten aufnehmen und verarbeiten.[4] Die juristische Perspektive antwortet dabei auf Normabweichungen bei der Entwicklung, der Bereitstellung und der Nutzung von Informations- und Kommunikationstechnologien.[5] Dem Recht kommen hierbei drei Funktionen zu: Es bildet die Maßstäbe, regelt die Sanktionen bei Normverstößen und stellt Verfahren sowie Organisationen zur Normdurchsetzung zur Verfügung.[6] Aus diesen facettenreichen Funktionen greift der Aufsatz den Aspekt der Datensicherheit heraus, der beispielhaft an Smart Metering Systemen und intelligenter Videoüberwachung illustriert wird. Zunächst werden die verfassungsrechtlichen Grundlagen untersucht (2). Anschließend wird § 9 BDSG als zentrale Datensicherheitsvorschrift[7] analysiert und technischer Datenschutz näher betrachtet (3). Schließlich werden Lösungsansätze für eine Modernisierung der Datensicherheit aus anderen datenschutzrechtlichen Regelungen untersucht (4) und sodann ein Fazit gezogen (5).

## 2 Verfassungsrechtliche Entwicklung

Für die verfassungsrechtliche Untersuchung sind das Volkszählungsurteil[8], das Urteil zur Online-Durchsuchung[9] und das Urteil zur Vorratsdatenspeicherung[10] des Bundesverfassungsgerichts (BVerfG) von zentraler Bedeutung.

### 2.1 Das Volkszählungsurteil

Das BVerfG entwickelte hier das Recht auf informationelle Selbstbestimmung als Ausprägung des durch Art. 2 Abs. 1 S. 1 GG in Verbindung mit Art. 1 Abs. 1 GG geschützten allgemeinen Persönlichkeitsrechts.[11] Um dieses Recht gleichzeitig zu schützen, verpflichtete es den Gesetzgeber „organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken“.[12] Die rechtliche Absicherung der informationellen Selbstbestimmung ist daher durch technische Sicherungen zu ergänzen.[13] Das BVerfG nennt hierzu konkret eine Verpflichtung zur Abschottung der Daten, zu ihrer Geheimhaltung, zu ihrer

Datenorganisation (IPD), Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) und das Zentrum für Angewandte Rechtswissenschaft (ZAR).

[4] [Ho08], S. 1011.
[5] [He06], S. 280.
[6] [He06], S. 280.
[7] [Er11], § 9 Rn. 1.
[8] [Bu83].
[9] [Bu08].
[10] [Bu10].
[11] [Fa13], Rn. 173.
[12] [Bu83].
[13] [Er03], Kap. 3.2 Rn. 16 und [He03], Kap. 4.5 Rn. 16.

Anonymisierung und zu ihrer Löschung, sobald sie nicht mehr erforderlich sind.[14] Diese Forderungen sind erste Ansätze zu Datensicherheitsstrukturen, wenngleich sie noch sehr kryptisch wirken. Das Volkszählungsurteil kann somit als „Sternstunde“ des Datenschutzes bezeichnet werden.[15] Heute gewinnt die Datensicherheit in technisch hochkomplexen und dynamischen Systemen immer mehr an Bedeutung. Deshalb muss sie sich parallel zur verwendeten Technologie stetig weiterentwickeln und dementsprechend flexibel gehandhabt werden.[16] Bezog sich Datensicherheit Anfang der 1980er Jahre noch auf Großrechner und war an vernetzte Systeme - wie beispielsweise das Internet - nicht zu denken, so stellen sich heutzutage die zentralen Fragen der Datensicherheit auch im Kontext von Smart Metering Systemen oder intelligenter Videoüberwachung öffentlicher Räume. Neuere Projekte wollen beispielsweise Daten aus Überwachungskameras mit Informationen aus sozialen Netzwerken vergleichen und „abnormales“ Verhalten identifizieren.[17] Der Einsatz von Smart Metering Systemen wiederum birgt die Gefahr anhand der Stromverbrauchsdaten das Fernsehprogramm zu bestimmen.[18]

### 2.2 Das Urteil zur Online-Durchsuchung

Das BVerfG hat am 27.2.2008 in der Entscheidung zur Online-Durchsuchung ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[19] als weitere besondere Ausprägung des allgemeinen Persönlichkeitsrechts[20] entwickelt. Die positive Definition des Schutzbereiches setzt bei drei Schlüsselbegriffen an: „informationstechnisches System“, „Vertraulichkeit“ und „Integrität“.[21]

#### 2.2.1 Informationstechnisches System

Das Urteil beschreibt nur vage, was abstrakt unter einem „informationstechnischen System“ zu verstehen ist.[22] Wörtlich heißt es hierzu: „Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ist hingegen anzuwenden, wenn die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu

[14] [Bu83], S. 49.
[15] [Do98], S. 69.
[16] [Sc05], S. 73.
[17] Heise Newsticker v. 28.7.2012, http://www.heise.de/newsticker/meldung/Europaweite-Proteste-gegen-das-Ueberwachungsprojekt-INDECT-1654965.html „Europaweiter Protest gegen das Überwachungsprojekt INDECT“ [abgerufen am 26.6.2013].
[18] Heise Newsticker v. 20.9.2011, http://www.heise.de/newsticker/meldung/Smart-Meter-verraten-Fernsehprogramm-1346166.html „SmartMeter verraten Fernsehprogramm“ [abgerufen am 26.6.2013].
[19] [Bu08].
[20] [Ho08], S. 1014; [Ku08], S. 1043; [Ho08a], S. 300; [Ei12], S. 452; [RS08], S. 3534; [SK08], S. 483; [Lu11], S. 76; aA [Le08], S. 21; [Br08], S. 413; [Bö08], S. 927 Fn. 25.
[21] [Bö08], S. 928.
[22] [Sp13], S. 803 und 815.

gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten.“[23] Hornung legt den Begriff daher extensiv aus und versteht darunter jedes System, das elektronisch Daten verarbeitet.[24] Als Beispiele nennt das BVerfG Personalcomputer[25], Laptops, Person Digital Assistants (PDAs) und Mobiltelefone.[26] Das System kann aber auch ein Rechnernetzwerk selbst oder ein Verbund von Rechnernetzwerken sein.[27] Nicht erfasst werden hingegen beispielsweise „nicht vernetzte elektronische Steuerungsanlagen der Haustechnik“.[28] Diese enthalten lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen, sodass in einem solchen Fall der Schutz durch das Recht auf informationelle Selbstbestimmung ausreicht.[29]

Das BVerfG versucht also eine Abgrenzung zwischen dem „neuen Grundrecht“ und dem Recht auf informationelle Selbstbestimmung zu entwickeln. Diese Abgrenzung ist jedoch nicht trennscharf und wirft neue Fragen auf.[30]

#### 2.2.1.1 Videoüberwachungssysteme als informationstechnisches System?

Die Videoüberwachung wurde bisher immer nur am Recht auf Informationelle Selbstbestimmung gemessen.[31] Dies erscheint nunmehr unter Bezugnahme auf das „neue“ Grundrecht fraglich, da Videoüberwachungssysteme ebenfalls als informationstechnisches System qualifiziert werden können. Intelligente Videoüberwachung zeichnet sich dadurch aus, dass sie zusätzlich zur Bildaufnahmeschaltung anwendungsspezifische Informationen aus Bildern herausfiltern und verarbeiten, sowie darauf basierende Entscheidungen treffen kann. Danach muss differenziert werden, ob lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich anfallen oder aber eine weitergehende Datenerfassung vorliegt. Diese Abgrenzung dürfte in der Praxis nicht einfach zu handhaben sein. Eine Kamera, die nur einen kleinen überschaubaren Bereich überwacht (beispielsweise die Überwachung eines Eingangs), erfasst dann nur Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich. Eine Kamera, die hingegen einen großflächigen Bereich überwacht (beispielsweise einen Kundenparkplatzes oder Bahnsteig) ermöglicht aber ein aussagekräftigeres Bild über die Persönlichkeit zu erstellen. Der Einsatz der gleichen Technik führt somit je nach Szenario zur Anwendung von unterschiedlichen Grundrechtsausprägungen. Welche rechtlichen Folgen sich daraus ergeben bleibt allerdings offen.[32] Das „neue“ Grundrecht soll ferner nur dann zur Anwendung kommen, „soweit der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt

[23] [Bu08], S. 314.
[24] [Ho08a], S. 302.
[25] [Bu08], S. 314.
[26] [Bu08], S. 311.
[27] [Bö08], S. 928.
[28] [Bu08], S. 313.
[29] [Bu08], S. 314.
[30] Kritisch auch [Br08], S. 413.
[31] Vgl. nur [Bu07], S. 330 ff. - Videoüberwachung.
[32] [Sp13], S. 803, 820, 821.

verfügt“[33]. Diese Einschränkung des BVerfG sagt gleichwohl nichts darüber aus, ob ein System als informationstechnisches System zu qualifizieren ist oder nicht. Sie besagt nur, wann eine Vertraulichkeits- und Integritätserwartung nicht besteht. Es handelt sich um eine subjektive Einschränkung. Deshalb können Videoüberwachungssysteme objektiv betrachtet als informationstechnische Systeme qualifiziert werden.

#### 2.2.1.2 Smart Metering Systeme als informationstechnisches System?

Ebenso wurden Smart Metering Systeme[34] bisher immer nur am Recht auf informationelle Selbstbestimmung gemessen.[35] Sie können aber ebenfalls ein informationstechnisches System darstellen, da durch die Erfassung von elektrischer Energie ein aussagekräftiges Bild der Persönlichkeit erstellt werden kann.[36] Entscheidend ist, dass eine Messeinrichtung - also die herkömmliche Messsensorik - nunmehr in ein Kommunikationsnetz eingebunden ist. Danach werden neben abrechnungsrelevanten Messdaten auch Netzzustandsdaten[37] erhoben und weiterverarbeitet, sodass keine ausschließlich punktuelle Datenerhebung vorliegt. Zudem können über den Stromverbrauch weitergehende Rückschlüsse über persönlichkeitsrelevante Verhaltensmuster (Bestimmung des Fernsehprogramms, Dauer und Zeitraum der Nutzung des Computers) gezogen werden.[38]

### 2.2.2 Vertraulichkeit und Integrität

Der zweite Schlüsselbegriff „Vertraulichkeit“ meint das Vertrauen hinsichtlich des Schutzes des „im“ System gespeicherten von ihm erzeugten Datenbestandes vor Ausspähung und Überwachung.[39] Hier sind aus technischer Sicht Maßnahmen entscheidend, die Vertraulichkeit sicherstellen oder wenigstens unterstützen können[40], wie etwa kryptographische Verschlüsselungsverfahren. Aufgrund der rasanten technischen Entwicklung in diesem Bereich, müssen allerdings bei diesen Verfahren Schutzniveau und Risiken immer wieder neu bewertet werden, Schlüssellängen müssen angepasst und Verfahren einer Kontrolle unterzogen werden.[41] Aus juristischer Sicht werden die Erwartungen an die Gewährleistung der Sicherheit des Systems durch technischen Selbstschutz zurückgedrängt, Erwartungen an den Staat, sich um die Sicherheit der Informationstechnologie zu bemühen, gleichsam hochgeschraubt.[42] In welchem Maße der Staat tatsächlich imstande ist die Vertraulichkeit von informationstechnischen Systemen zu sichern und zu schützen, müssen die künftigen Entwicklungen erst zeigen.

---

[33] [Bu08], S. 315.
[34] Siehe Legaldefinition des Messsystems in § 21d Abs. 1 EnWG.
[35] BR-Drs. 343/11, S. 195; [JRV11], S. 101.
[36] [HF12], S. 23.
[37] Beispielsweise Frequenz, Phasenwinkel, Spannung.
[38] [Gu12], S. 619 m.w.N.
[39] [Bö08], S. 928.
[40] [Ha12], S. 409.
[41] [Ha12], S. 409.
[42] [Bö08], S. 938.

Mit dem dritten Schlüsselbegriff „Integrität“ wird die Unversehrtheit des Systems vor Ausspähung, Überwachung und Manipulation durch Dritte verstanden.[43] Aus technischer Sicht kommen für den Schutz vor Manipulation kryptographische Verfahren, revisionssichere Protokollierung oder die Verwendung von Trusted Computing[44] in Betracht.[45] Aus rechtlicher Sicht liegt der Akzent nicht auf dem Schutz subjektiver Abwehrrechte, sondern der Begründung eines objektiv-rechtlichen Schutzes informationstechnischer Systeme.[46] Der Staat ist folglich verpflichtet, die Integrität informationstechnischer Systeme zu schützen. Um dies zu gewährleisten, sind beispielsweise Vorschriften nötig, die sich mit dem Thema der Datensicherheit auseinandersetzen. Diese Schutzpflicht des Staates findet u.a. einfachgesetzlichen Ausdruck in § 9 BDSG, da dieser als die Datensicherheitsvorschrift im BDSG gilt und den technischen Datenschutz symbolisiert.[47]

### 2.3 Das Urteil zur Vorratsdatenspeicherung

Die dritte wichtige Entscheidung fällte das BVerfG im Urteil zur Vorratsdatenspeicherung am 2.3.2010. Dort führte es in Leitsatz 4 aus: „Hinsichtlich der Datensicherheit bedarf es Regelungen, die einen besonders hohen Sicherheitsstandard normenklar und verbindlich vorgeben. Es ist jedenfalls dem Grunde nach gesetzlich sicherzustellen, dass sich dieser an dem Entwicklungsstand der Fachdiskussion orientiert, neue Erkenntnisse und Einsichten fortlaufend aufnimmt und nicht unter dem Vorbehalt einer freien Abwägung mit allgemeinen wirtschaftlichen Gesichtspunkten steht.“[48] Erstmals taucht damit in der verfassungsgerichtlichen Judikatur ausdrücklich der Begriff der Datensicherheit auf. Die Verfassung selbst gibt nicht detailgenau vor, welche Sicherheitsmaßnahmen im Einzelnen geboten sind. Gleichwohl nennt das Gericht beispielhaft Sicherheitsmaßnahmen wie die getrennte Speicherung von Daten, den Einsatz asymmetrischer kryptographischer Verschlüsselung, die Vorgabe des Vier-Augen-Prinzips, die revisionssichere Protokollierung des Zugriffs auf Daten oder den Einsatz von automatisierten Fehlerkorrektur- und Plausibilitätsverfahren.[49] Die Anforderungen haben sich an neuen technischen Entwicklungen zu orientieren, wofür als Anknüpfungspunkt der „Stand der Technik“ in Betracht kommt.[50] Dem „Stand der Technik“ kommt dabei eine dynamisierende Wirkung zu.[51] Ferner steht es dem Gesetzgeber frei, die technische Konkretisierung des vorgegebenen Maßstabs einer Aufsichtsbehörde anzuvertrauen.[52] Die Ausführungen in diesem Urteil zur Datensicherheit stehen allerdings im Kontext zur anlasslosen Speicherung von Telekommunikationsverkehrsdaten durch private Diensteanbieter.

[43] [Bö08], S. 928.
[44] Mit den rechtlichen Problemen von Trusted Computing setzt sich [Be05], S. 393 ff ausführlich auseinander.
[45] [Ha12], S. 409.
[46] So auch [Bö08], S. 928; aA [SK08], S. 486; [Si09], S. 88 und 91.
[47] [Er11], § 9 Rn. 1.
[48] [Bu10].
[49] [Bu10], S. 326; siehe hierzu ausführlich [Sz11], S. 250 ff.
[50] [Bu10], S. 326.
[51] [HS10], S. 829.
[52] [Bu10], S. 327.

Damit ist fraglich, ob sich diese Überlegungen auch auf vergleichbare private Bereiche übertragen lassen und ob sie auch für staatliche Überwachungsmaßnahmen oder sonstige staatliche Datensammlungen relevant sein werden.[53] Dies hätte dann sowohl Auswirkungen auf Smart Metering Systeme, wie auch auf intelligente Videoüberwachung. Gegen eine Übertragung lässt sich die starke Betonung der Risiken, die gerade durch die Speicherung von Telekommunikationsverkehrsdaten bei Privaten im Telekommunikationssektor entstehen, einwenden.[54] Andererseits sind die dargestellten Risiken für die Datensicherheit nicht nur im Telekommunikationssektor und im staatlichen Bereich[55] vorhanden. Auch bei eingriffsintensiven Maßnahmen oder dem Umgang mit sensitiven Daten sind vergleichbare Risiken gegeben; sei es durch staatliche Maßnahmen oder durch das Handeln Privater. Insofern lassen sich die Ausführungen auch auf ähnliche (staatliche) Überwachungsmaßnahmen oder sonstige Datensammlungen übertragen. Einfachgesetzlich gilt für staatliche und private Datenverarbeiter § 9 BDSG. Das BVerfG hat die Vorgaben aus § 9 BDSG allerdings immer noch als zu allgemein eingestuft, um die für die Vorratsdatenspeicherung gerade notwendigen besonders hohen Sicherheitsstandards sicherzustellen.[56] Bei Daten mit sehr hohem Schutzniveau (etwa Sozialdaten oder Gesundheitsdaten) wird man deshalb höhere Anforderungen an die Datensicherheit stellen müssen.[57] Sowohl in Smart Metering Systemen, wie auch bei intelligenter Videoüberwachung können solche Daten anfallen. Dann müssen die höheren Anforderungen schon im jeweiligen Fachgesetz geregelt werden.[58] Fehlt eine fachgesetzliche Regelung, ist auf § 9 BDSG zu rekurrieren. Dieser erfüllt die hohen Sicherheitsanforderungen und -standards jedoch nach Ansicht des BVerfG nicht mehr. Zudem ist § 9 BDSG seit seiner Einführung 1990 nur unwesentlich geändert worden, sodass zweifelhaft ist, ob die Norm den aktuellen technischen Entwicklungen überhaupt noch ein entsprechendes Schutzniveau bieten kann.

## 3 Datensicherheit nach § 9 BDSG und der Anlage zu § 9 S. 1 BDSG

§ 9 BDSG symbolisiert in Verbindung mit der Anlage zu § 9 S. 1 BDSG als zentrale Datensicherheitsvorschrift den technischen Datenschutz.[59] Die Norm richtet sich grundsätzlich an jede Stelle, die personenbezogene Daten erhebt, verarbeitet oder nutzt.[60] Sie beinhaltet die Verpflichtung zur Schaffung technischer und organisatorischer Maßnahmen. Diese Maßnahmen müssen geeignet sein die Sicherung der Daten und der zu ihrer Verarbeitung eingesetzten Prozesse zu unterstützen.[61] Insofern wird in § 9 BDSG der allgemeine Schutzzweck nach § 1 Abs. 1 BDSG um den technischen Aspekt der Datensicherheit erweitert.[62] Datensicherheit soll einerseits unzulässigen Umgang mit

[53] So auch [HS10], S. 829.
[54] [HS10], S. 829.
[55] So auch [HS10], S. 829.
[56] [Bu10], S. 350 und 351.
[57] [HS10], S. 829.
[58] So auch [HS10], S. 829.
[59] [Er11], § 9 Rn. 1.
[60] [Sc10], § 9 Rn. 10; [He03], Kap. 4.5 Rn. 21.
[61] [Sc10], § 9 Rn. 16; [He03], Kap. 4.5 Rn. 2.
[62] Zum Verhältnis Datenschutz und Datensicherheit [Er11], § 9 Rn. 2 f.

personenbezogenen Daten verhindern, andererseits die Integrität und Verfügbarkeit der Daten sowie die zu deren Verarbeitung eingesetzten technischen Einrichtungen erhalten.[63] Die Anlage zu § 9 S. 1 BDSG listet eine Reihe von Maßnahmen auf, um Datensicherheit zu erreichen.[64]

Vielfach wird kritisiert, dass die dort geregelten Kontrollen trotz der jeweiligen Modernisierungen des BDSG nicht (mehr) zeitgemäß sind.[65] Den auf Datensicherheit abzielenden Maßnahmen in der Anlage zu § 9 S. 1 BDSG wird zwar zu Gute gehalten, dass die gesetzlichen Anforderungen an die erforderlichen Datensicherungsmaßnahmen nach wie vor sehr flexibel gehalten sind, „weil sie losgelöst von einem bestimmten Stand der Technik oder der Organisationskenntnisse zum Zeitpunkt des Inkrafttretens des Gesetzes beschrieben werden".[66] Die Fortentwicklung der automatisierten Datenverarbeitung, neuere Methoden in der IT-Sicherheit sowie weltweit standardisierte Begriffe wie Verfügbarkeit, Integrität und Vertraulichkeit verlangen jedoch nach einer grundlegenden Änderung der Maßnahmen des Anhangs zu § 9 S. 1 BDSG.[67] Jedoch relativiere sich diese Annahme, wenn man erkennt, dass es sich bei den einzelnen Maßnahmen der Anlage streng genommen (nur) um abstrakte Zielvorgaben für die von der verantwortlichen Stelle zu ergreifenden technischen und organisatorischen Maßnahmen handelt.[68] Der nicht abschließende[69] Anforderungskatalog in der Anlage zu § 9 S. 1 BDSG stelle aufgrund seines Wortlauts („insbesondere") nur ein Mindestmaß der notwendigen Maßnahmen dar, die die verantwortliche Stelle zu berücksichtigen habe.[70] Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder kritisierte im Jahre 2010, dass „Maßnahmen zur Gewährleistung des technischen und organisatorischen Datenschutzes […] noch aus der Zeit der Großrechnertechnologie [stammen] und […] sich nur noch mit Mühe auf die heutige Welt vernetzter und ubiquitärer Systeme übertragen [lassen]."[71]

Außerdem ist mit § 9 BDSG lediglich ein allgemeiner Maßstab für die Datensicherheit im BDSG gesetzt, der jedoch aufgrund der Subsidiaritätsklausel in § 1 Abs. 3 S. 1 BDSG[72] bzw. der möglichen Verdrängung durch Landesrecht nach § 1 Abs. 2 Nr. 2 BDSG[73] modifiziert werden kann. Zudem können Vorgaben des europäischen Rechts Datensicherheit beeinflussen. Daher stellt sich die Frage, welche Normprogramme zur Modernisierung der Vorschrift als Vorbild dienen könnten.

[63] [Er11], § 9 Rn. 2.
[64] [Er11], § 9 Rn. 48.
[65] [Sc11], S. 11; [Sc10], § 9 Rn. 38; so auch [KDB10], S. 18 ff.
[66] [Er11], § 9 Rn. 48.
[67] [Er11], § 9 Rn. 1.
[68] [Sc10], § 9 Rn. 36.
[69] [Er11], § 9 Rn. 17.
[70] [Sc10], § 9 Rn. 36; [Er11], § 9 Rn. 17.
[71] [KDB10], S. 18.
[72] [GS10], § 1 Rn. 24.
[73] [Er11], § 9 Rn. 4; [GS10], § 9 Rn. 6.

# 4 Potentielle Vorbildnormen für neue Datensicherheitsregelungen im BDSG

## 4.1 Landesdatenschutzgesetz Schleswig-Holstein (LDSG-SH)

In § 5 LDSG-SH sind seit Januar 2012 die allgemeinen Maßnahmen zur Datensicherheit neu geregelt. Diese Norm ist deshalb von besonderem Interesse, weil sie standardisierte Begriffe der IT-Sicherheit integriert. Lediglich die Landesdatenschutzgesetze Berlin, Hamburg und Nordrhein-Westfalen haben in Teilen Schutzziele integriert, jedoch im Wesentlichen eine mit § 9 BDSG i.V.m. der Anlage zu § 9 S. 1 BDSG vergleichbare Struktur beibehalten. In anderen Landesdatenschutzgesetzen wiederum sind Verordnungsermächtigungen zu finden, die den Landesregierungen die Regelung weiterer Einzelheiten in datensicherheitsrechtlichen Fragen ermöglichen sollen.[74]

In § 5 Abs. 1 S. 2 Nr. 1 - 3 LDSG-SH werden die klassischen Schutzziele (Verfügbarkeit, Integrität, Vertraulichkeit) der Datensicherheit[75] legaldefiniert. Sie unterscheiden sich von denen des allgemeinen Datenschutzrechts dadurch, dass sie nicht die Umsetzung des Rechts auf informationelle Selbstbestimmung der natürlichen Person, sondern im Konkreten die Umsetzung von Datensicherheit zum Ziel haben.[76] Verkürzt gesagt soll Datenschutz den Menschen, Datensicherheit hingegen die Daten schützen.[77]

In § 5 Abs. 1 S. 2 Nr. 4 - 6 LDSG-SH werden darüber hinaus „neue Schutzziele“[78] genannt, die aus der verfassungsgerichtlichen Rechtsprechung abgeleitet und nachfolgend näher betrachtet werden sollen.

### 4.1.1 Transparenz

Transparenz ist gegeben, wenn „die Verarbeitung von personenbezogenen Daten mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden kann“ (§ 5 Abs. 1 S. 2 Nr. 4 LDSG-SH). Damit wird die Forderung des BVerfG aus dem Volkszählungsurteil bzgl. der Transparenz der Erhebungs- und Verarbeitungszusammenhänge erfüllt, da nicht die Gefahr entstehen darf, dass die Bürger als Betroffene „nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“.[79] Zudem wird mit der nun vorliegenden Legaldefinition gesetzlich fixiert, was in der Literatur bislang als Voraussetzung für die Beobachtbarkeit, Kontrollierbarkeit und Prüfbarkeit von Systemen[80] umschrieben wurde. Weiterhin wird damit die Forderung nach Klarheit, Erkennbarkeit und Nachverfolgbarkeit erfüllt.[81]

### 4.1.2 Nicht-Verkettbarkeit

[74] So etwa in § 9 Abs. 3 LDSG Rheinland-Pfalz, § 9 Abs. 4 LDSG Baden-Württemberg.
[75] [FP03], Kap. 2.2 Rn. 6; [RB11], S. 32.
[76] [BM12], S. 425.
[77] [FP03], Kap. 2.2 Rn. 5; ausgehend vom Schutzzweck nach § 1 Abs. 1 BDSG ähnlich [SH11], S. 64: „Im Datenschutzrecht geht es […] nicht um den Schutz ‚von‘ Daten, sondern um den Schutz ‚vor‘ Daten.“
[78] [RB11], S. 32 f.
[79] [Bu83], S. 43; [BM12], S. 426.
[80] [RP09], S. 355.
[81] [BA10], S. 325.

Nicht-Verkettbarkeit ist dann gewährleistet, wenn „personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können“ (§ 5 Abs. 1 S. 2 Nr. 5 LDSG-SH). Mit dieser Legaldefinition wird ebenfalls Bezug auf das Volkszählungsurteil des BVerfG genommen. Dort heißt es, dass die „Nutzbarkeit und Verwendungsmöglichkeit [personenbezogener Daten] […] von den der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten ab[hängt]. Dadurch kann ein für sich genommen belangloses Datum einen neuen Stellenwert bekommen“.[82] Das aus dieser Aussage des BVerfG abgeleitete Schutzziel hängt damit unmittelbar mit dem Zweckbindungsgrundsatz zusammen.[83] Danach gilt, dass der Zweck der Verarbeitung personenbezogener Daten bereichsspezifisch und präzise bestimmt werden muss und zudem gewährleistet wird, dass die Verwendung der Daten auf den gesetzlich bestimmten Zweck begrenzt ist.[84] Für die Datensicherheit bedeutet dies, dass zumindest angemessene Funktions- und Rollentrennungen zwischen und innerhalb von Organisationen mit Verantwortungszuweisungen an kompetente Belegschaftsangehörige stattfinden sollen.[85] Insbesondere im Hinblick auf die Gefahren der automatischen Datenverarbeitung könnte so der vom BVerfG geforderte „Schutz gegen Zweckentfremdung durch Weitergabeverbote und Verwertungsverbote“ erreicht werden.[86]

### 4.1.3 Intervenierbarkeit

Das Schutzziel der Intervenierbarkeit verlangt, dass „Verfahren so gestaltet werden, dass sie den Betroffenen die Ausübung der ihnen zustehenden Rechte […] wirksam ermöglichen“ (§ 5 Abs. 1 S. 2 Nr. 6 LDSG-SH). Im Volkszählungsurteil hat das BVerfG festgestellt, dass der Gesetzgeber zur Sicherung des Rechts auf informationelle Selbstbestimmung organisatorische und verfahrensrechtliche Vorkehrungen zu treffen hat, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.[87] Diese Absicherung bezeichnete das BVerfG als „weitere verfahrensrechtliche Schutzvorkehrungen“.[88] Diese Schutzvorkehrungen finden sich heute als konkrete Betroffenenrechte[89] (z.B. Auskunft, Benachrichtigung, Löschung oder Sperrung) in datenschutzrechtlichen Regelungen wieder.

## 4.2 Datensicherheit im Energiewirtschaftsgesetz (EnWG)

Aus der nunmehr geltenden Pflicht zum Einbau von intelligenten Messsystemen unter den Voraussetzungen des § 21c Abs. 1 EnWG resultiert die potentielle Gefährdung der informationellen Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.[90] Der geforderte datenschutzrechtliche „Maßnahmenkatalog“ zur Sicherung des

[82] [Bu83], S. 45.
[83] [BM12], S. 428.
[84] [Bu83], S. 46.
[85] [RB11], S. 33 mit weiteren Anwendungsbeispielen.
[86] [Bu83], S. 46.
[87] [Bu83], S. 44.
[88] [Bu83], S. 46.
[89] z.B. in §§ 6, 19, 20, 34, 35 BDSG bzw. §§ 26-30 LDSG-SH.
[90] [RJ10], S. 374; [Ka10], S. 365.

Grundrechtsschutzes im novellierten EnWG wurde in einem auf drei Säulen basierenden gesetzlichen Schutzkonzept statuiert.[91] Dieses Säulenmodell verfügt über einen materiell-rechtlichen Grundbestand (§§ 21g und h EnWG), die Ermächtigung für Rechtsverordnungen (§ 21i EnWG) und verbindliche am Stand der Technik orientierte Schutzmaßnahmen (§ 21e EnWG).[92] Letztgenannte Schutzmaßnahmen finden sich in ihrer konkreten Ausprägung in § 21e EnWG als zentrale Datensicherheitsvorschrift des novellierten EnWG. Dort werden zentrale Datenschutzziele, -prinzipien und darauf bezogene Maßnahmen genannt, deren Gewährleistung dem Schutz der informationellen Selbstbestimmung dienen soll.

### 4.2.1 Schutzmaßnahmen in § 21e EnWG

Mit § 21e EnWG wurde eine bereichsspezifische Regelung geschaffen, die dazu verpflichten soll „datenschutzfördernde Technik" einzusetzen.[93] In § 21e Abs. 1 EnWG wird neben der Einhaltung eichrechtlicher Vorschriften die Gewährleistung von Datenschutz, Datensicherheit und Interoperabilität in Bezug auf Messsysteme zwingend vorgeben. Detaillierte Regelungen dazu finden sich in den Absätzen 2 bis 4. Demnach müssen Messsysteme den Anforderungen aus Schutzprofilen entsprechen und Interoperabilität gewährleisten (Abs. 2), dem Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit treffen (Abs. 3) sowie in Schutzprofilen festgelegte Zertifizierungsverfahren einhalten (Abs. 4). Für die praktische Umsetzung sind insbesondere die Anforderungen der Schutzprofile[94] und der Technischen Richtlinie[95] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu berücksichtigen, die ihrerseits der nach den §§ 21e Abs. 4 S. 2, 21i Abs. 1 Nr. 12 EnWG zu erlassenden datensicherheitsrechtlichen Verordnung zugrunde gelegt werden sollen.

### 4.2.2 Datenschutzkonforme Technikgestaltung (§ 21e EnWG)

Die konkrete technische Umsetzung der Datensicherheit in Bezug auf Messsysteme wird schon anhand der Normstruktur des § 21e EnWG deutlich: Der Gesetzgeber hat sich eine weitergehende technische Ausgestaltung anhand der Verweise auf den umfangreichen Verordnungsermächtigungskatalog in § 21i Abs. 1 EnWG offen gehalten.[96] Diese Vorgehensweise wird innerhalb des komplexen Normgefüges der bereichsspezifischen Regelungen zum Datenschutz im EnWG an mehreren Stellen angeordnet. So wird unter anderem in den §§ 21e Abs. 3 S. 3, 21g Abs. 6 S. 1 EnWG auf eine Konkretisierung

[91] [Ra11], S. 831, die sich auf die neu eingeführten datenschutzrechtlichen Regelungen nach BGBl. I 2011, S. 1554, 1577 beziehen.
[92] [Ra11], S. 835 ff.
[93] [JRV11], S. 101.
[94] Schutzprofil für ein Smart Meter Gateway online abrufbar unter: https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Gateway/schutzprofil_smart_meter_gateway_node.html [abgerufen am 26.6.2013] sowie Schutzprofil für das Sicherheitsmodul eines Smart Meter Gateway online abrufbar unter: https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Security/security_module_node.html [abgerufen am 26.6.2013].
[95] Technische Richtlinie online abrufbar unter: https://www.bsi.bund.de/DE/Themen/SmartMeter/TechnRichtlinie/TR_node.html [abgerufen am 26.6.2013].
[96] [JRV11], S. 101.

durch Rechtsverordnung nach § 21i Abs. 1 Nr. 4 EnWG verwiesen.[97] Diese Methodik entspricht dem Grundgedanken, weitgehend technikneutrale Gesetze zu formulieren, „die nicht mit der Dynamik der Technikentwicklung novelliert werden müssen und dennoch die Technikgestaltung unmittelbar steuern können".[98] Insbesondere unter Berücksichtigung der verfassungsrechtlichen Vorgaben zur Ausgestaltung des technischen Datenschutzes, erscheint im Bereich der intelligenten Infrastrukturen dieser Ansatz angemessen. Mit der stetigen Weiterentwicklung komplexer technischer Systeme steigen auch die rechtlichen Anforderungen an eben diese. Somit bietet dieser Ansatz den Vorteil, auf Entwicklungen in der Informations- und Kommunikationstechnologie flexibel reagieren zu können.

### 4.3 Technischer Datenschutz nach dem Entwurf der EU-Datenschutz-Grundverordnung

Der Entwurf zur EU-Datenschutz-Grundverordnung (DS-GVO-E)[99] enthält in Art. 23 Regelungsvorschläge zu Datenschutz durch Technik und datenschutzfreundlichen Voreinstellungen. Damit rekurriert Art. 23 auf die Begriffe „data protection by design" und „data protection by default".[100] Danach ist es für den Schutz der Rechte und Freiheiten der Person bzgl. der Verarbeitung personenbezogener Daten „erforderlich, dass geeignete technische und organisatorische Maßnahmen" getroffen werden. Diese Maßnahmen sollen sich sowohl auf den Zeitpunkt der Konzipierung der Verarbeitungsvorgänge wie auch den Zeitpunkt der Verarbeitung beziehen, „damit die Anforderungen dieser Verordnung erfüllt werden".[101]

Der Vorschlag dieser Normierungen wird zwar als dringend erforderlicher Schritt hin zu modernen technischen Datenschutzinstrumenten angesehen[102], jedoch bleibt die konkrete Ausgestaltung der Maßnahmen unklar. Die Vorschläge „data protection by design" und „data protection by default" in Erwägungsgrund (EG) 61 sind zu oberflächlich und stellen lediglich eine „bloße Ankündigung" dar, weil in Art. 23 Abs. 1 und 2 DS-GVO-E jede verbindliche Aussage zur Technikgestaltung fehlt.[103] Es wird lediglich eine Verpflichtung zu datenschutzfreundlichen bzw. -gerechten Voreinstellungen[104] in „Verfahren" erwähnt, deren konkrete Ausgestaltung aber völlig unklar bleibt. Auch werden Grundprinzipien des technischen Datenschutzes, wie sie das deutsche Datenschutzrecht kennt, nicht erwähnt. Zu denken ist hierbei an die Verfahren der Anonymisierung und Pseudonymisierung.[105] Damit bleibt im Hinblick auf konkrete

[97] Dazu [Ra11], S. 835.
[98] [JRV11], S. 101.
[99] KOM(2012) 11 – Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung).
[100] Siehe Erwägungsgrund (EG) 61 DS-GVO-E.
[101] Ebd.
[102] [Ho12], S. 103; [Ho11], S. 54; [KDB10], S. 7 f., 9 f., 18 ff.
[103] [Ho12], S. 103.
[104] [La11a], S. 148.
[105] [Ho12], S. 103.

technische und organisatorische Maßnahmen der Schutzgehalt der DS-GVO-E hinter dem deutschen Datenschutzrecht zurück.[106]

## 5 Fazit und Ausblick

Die voranschreitende technische Entwicklung intelligenter Infrastrukturen führt gleichsam zu neuen juristischen Herausforderungen im Kontext Datenschutz und Datensicherheit. Intelligente Infrastrukturen können sich als informationstechnische Systeme qualifizieren lassen, sodass sie dann den verfassungsrechtlichen Anforderungen an Vertraulichkeit und Integrität entsprechen müssen. Auch wird die Frage zu beantworten sein, welche Grundrechtsausprägung des Allgemeinen Persönlichkeitsrechts künftig zur Anwendung kommt und welche konkreten Rechtsfolgen sich daraus ableiten lassen.

Unter Berücksichtigung der Vorgaben zur Datensicherheit aus dem Urteil zur Vorratsdatenspeicherung bedürfen intelligente Infrastrukturen normenklarer Regelungen, die einen besonders hohen Sicherheitsstandard vorgeben. Diesen Vorgaben ist der moderne Gesetzgeber beispielsweise in § 21e EnWG im Rahmen der Anforderungen an Messsysteme zur Erfassung elektrischer Energie nachgekommen. Zudem könnte eine Verordnungsermächtigung vergleichbar mit dem Katalog des § 21i EnWG die notwendige „Technikoffenheit“ gewährleisten. Auch der Schleswig-Holsteinische Landesgesetzgeber hat mit § 5 LDSG-SH eine verfassungsrechtlich gebotene Datensicherheitsnorm erlassen. Gemessen daran ist der Kritik an § 9 BDSG i.V.m. der Anlage zu § 9 S. 1 BDSG zuzustimmen.

In der Konsequenz bedeutet dies, dass für intelligente Infrastrukturen nach geltender Rechtslage unterschiedliche Datensicherheitsstandards Anwendung finden. Auf Intelligente Videoüberwachung ist § 9 BDSG anzuwenden, auf Smart Metering Systeme hingegen § 21e EnWG, der modernere Sicherheitsstandards normiert und daher das Schutzniveau von § 9 BDSG überwiegt. Dass unterschiedliche Vorgaben für vergleichbar dynamische und komplexe Infrastrukturen gelten, leuchtet in diesem Zusammenhang jedoch nicht ein.

Die Normierungsvorschläge zu technischem Datenschutz im Entwurf der EU-Datenschutz-GVO stellen eine unvollständige und intransparente Materie dar. Es bleibt in EG 61 bei vagen Ankündigungen zu „data protection by design“ und „data protection by default“, die in Art. 23 keinen adäquaten Niederschlag finden. Diese Normierungsvorschläge bleiben daher hinter dem hier geforderten Datensicherheitsprogramm zurück. Allerdings bleibt abzuwarten, welche Änderungen und Ergänzungen das weitere EU-Normsetzungsverfahren bringen werden.

Somit ist der Gesetzgeber aufgefordert neue Datensicherheitsregelungen zu gestalten und insbesondere § 9 BDSG einer Novellierung zu unterziehen.

[106] So auch [Ho12], S. 103.

## Literaturverzeichnis


[BA10] Bedner, M./Ackermann, T.: Schutzziele der IT-Sicherheit. In: Datenschutz und Datensicherheit 2010, S. 323 – 328.

[Be05] Bechtold, S.: Trusted Computing - Rechtliche Probleme einer entstehenden Technologie. In: Computer und Recht 2005, S. 393 – 404.

[Bö08] Böckenförde, T.: Auf dem Weg zur elektronischen Privatsphäre. In: Juristenzeitung 2008, S. 925 – 939.

[Br08] Britz, G.: Vertraulichkeit und Integrität informationstechnischer Systeme. In: Die öffentliche Verwaltung 2008, S. 411 – 415.

[BM12] Bock, K./Meissner, S.: Datenschutz-Schutzziele im Recht - Zum normativen Gehalt der Datenschutz-Schutzziele. In: Datenschutz und Datensicherheit 2012, S. 425 – 431.

[Bu83] Bundesverfassungsgerichtentscheidungen (BVerfGE), 1983, Band 65, S. 1 ff.

[Bu07] Kammerentscheidungen des Bundesverfassungsgericht (BVerfGK), 2007, Band 10, S. 330 ff.

[Bu08] Bundesverfassungsgerichtentscheidungen (BVerfGE), 2008, Band 120, S. 274 ff.

[Bu10] Bundesverfassungsgerichtentscheidungen (BVerfGE), 2010, Band 125, S. 260 ff.

[Do98] Donos, P.: Datenschutz – Prinzipien und Ziele, 1998.

[Ei12] Eiermann, H.: Das IT-Grundrecht und seine Folgen. In: Datenschutz und Datensicherheit 2012, S. 452.

[Er03] Ernestus, W.: Konzept der Datensicherung. In: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003.

[Er11] Ernestus, W.: Kommentierung zu § 9 BDSG. In: Simitis (Hrsg.), BDSG, 7. Auflage 2011.

[Fa13] di Fabio, U.: Kommentierung zu Art. 2 GG. In: Maunz/Dürig (Hrsg.), GG, 67. Ergänzungslieferung 2013.

[FP03] Federrath, H./Pfitzmann, A.: Grundlagen des Datenschutzes. In: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003.

[GS10] Gola/Schomerus, BDSG, 10. Auflage, 2010.

[Gu12] Guckelberger, A.: Smart Grids/Smart Meter zwischen umweltverträglicher Energieversorgung und Datenschutz. In: Die öffentliche Verwaltung 2012, S. 613 – 622.

[Ha12] Hansen, M.: Vertraulichkeit und Integrität von Daten und IT-Systemen im Cloud-Zeitalter. In: Datenschutz und Datensicherheit 2012, S. 407 – 412.

[He03] Heibey, H.-W.: Datensicherung. In: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003.

[He06] Heckmann, D.: Rechtspflichten zur Gewährleistung von IT-Sicherheit im Unternehmen. In: Multimedia und Recht 2006, S. 280 – 285.

[HF12] Hornung, G./Fuchs, K.: Nutzerdaten im Smart Grid – zur Notwendigkeit einer differenzierten grundrechtlichen Bewertung. In: Datenschutz und Datensicherheit 2012, S. 20 – 25.

[Ho08] Hoffmann-Riem, W.: Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme. In: Juristenzeitung 2008, S. 1009 – 1022.

[Ho08a] Hornung, G.: Ein neues Grundrecht - Der verfassungsrechtliche Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme. In: Computer und Recht 2008, S. 299 – 306.

[Ho11] Hornung, G.: Datenschutz durch Technik in Europa – Die Reform der Richtlinie als Chance für ein modernes Datenschutzrecht. In: Zeitschrift für Datenschutz 2011, S. 51 – 56.

[Ho12] Hornung, G.: Eine Datenschutz-Grundverordnung für Europa? – Licht und Schatten im Kommissionsentwurf vom 25.1.2012. In: Zeitschrift für Datenschutz 2012, S. 99 – 106.

[HS10] Hornung, G./Schnabel, C.: Verfassungsrechtlich nicht schlechthin verboten - Das Urteil des Bundesverfassungsgerichts in Sachen Vorratsdatenspeicherung. In: Deutsches Verwaltungsblatt 2010, S. 824 – 833.
[JRV11] Jandt, S./Roßnagel, A./Volland, B.: Datenschutz für Smart Meter – Spezifische Neuregelungen im EnWG. In: Zeitschrift für Datenschutz 2011, S. 99 – 103.
[Ka10] Karg, M.: Datenschutzrechtliche Rahmenbedingungen beim Einsatz intelligenter Zähler. In: Datenschutz und Datensicherheit 2010, S. 365 – 372.
[KDB10] Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Ein modernes Datenschutzrecht für das 21. Jahrhundert, 2010.
[Ku08] Kutscha, M.: Mehr Schutz von Computerdaten durch ein neues Grundrecht? In: Neue Juristische Wochenschrift 2008, S. 1042 – 1044.
[La11] Laupichler, D./Vollmer, S./Bast, H./Intemann, M.: Das BSI-Schutzprofil: Anforderungen an den Datenschutz und die Datensicherheit für Smart Metering Systeme, S. 542 – 546.
[La11a] Lang, M.: Reform des EU-Datenschutzrechts - Einheitliche Regelungen mit hohem Datenschutzniveau geplant. In: Kommunikation und Recht 2012, S. 145 – 151.
[Le08] Lepsius, O.: Das Computer-Grundrecht: Herleitung – Funktion – Überzeugungskraft. In: Roggan (Hrsg.), Online-Durchsuchungen, 2008.
[Lu11] Luch, A.: Das neue "IT-Grundrecht" - Grundbedingung einer "Online-Handlungsfreiheit". In: Multimedia und Recht 2011, S. 75 – 79.
[Mü11] Müller, K.J.: Verordnete Sicherheit – das Schutzprofil für das Smart Metering Gateway. In: Datenschutz und Datensicherheit 2011, S. 547 – 551.
[Ra11] Raabe, O./Lorenz, M./Pallas, F./Weis, E.: Harmonisierung konträrer Kommunikationsmodelle im Datenschutzkonzept des EnWG - "Stern" trifft "Kette". In: Computer und Recht 2011, S. 831 – 840.
[RB11] Rost, M./Bock, K.: Privacy By Design und die Neuen Schutzziele. In: Datenschutz und Datensicherheit 2011, S. 30 – 35.
[RJ10] Roßnagel, A./Jandt, S.: Datenschutzkonformes Energieinformationsrecht. In: Datenschutz und Datensicherheit 2010, S. 373 – 378.
[RP09] Rost, M./Pfitzmann, A.: Datenschutz-Schutzziele – revisited. In: Datenschutz und Datensicherheit 2009, S. 353 – 358.
[RS08] Roßnagel, A./Schnabel, C.: Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht. In: Neue Juristische Wochenschrift 2008, S. 3534 – 3538.
[SK08] Sachs, M./Krings, T.: Das neue Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. In: Juristische Schulung 2008, S. 481 – 486.
[Sc05] Schultze-Melling, J.: IT-Sicherheit in der anwaltlichen Beratung. In: Computer und Recht 2005, S. 73 – 80.
[Sc10] Schultze-Melling, J.: Kommentierung zu § 9 BDSG. In: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010.
[Sc11] Schneider, J.: Die Datensicherheit – Eine vergessene Rechtsmaterie? Ein Plädoyer für Aufwertung, stärkere Integration und Modernisierung des § 9 BDSG. In: Zeitschrift für Datenschutz 2011, S. 6 – 12.
[SH11] Schneider, J./Härting, N.: Warum wir ein neues BDSG brauchen – Kritischer Beitrag zum BDSG und dessen Defiziten. In: Zeitschrift für Datenschutz 2011, S. 63 – 68.
[Si09] Sick, P.: Objektiv-rechtlicher Gewährleistungsgehalt oder Abwehrfunktion des neuen "Computergrundrechts"? In: Verwaltungsblätter für Baden-Württemberg 2009, S. 85 – 91.
[Sp13] Spiecker gen. Döhmann, I.: Die Online-Durchsuchung als Instrument der Sicherheitsgewährleistung. In: Heckmann/Schenke/Sydow (Hrsg.), Festschrift für Thomas Würtenberger zum 70. Geburtstag, 2013.
[Sz11] Szuba, D.: Vorratsdatenspeicherung - Der europäische und deutsche Gesetzgeber im Spannungsfeld zwischen Sicherheit und Freiheit, 2011.