Energie – Wirtschaft – Recht

Festschrift für Peter Salje

Zum 65. Geburtstag
am
9. Februar 2013

Herausgegeben von

Andreas Klees
Kai Gent

Sonderdruck

Carl Heymanns Verlag

Technische Sicherheit im digitalen Zeitalter

KLAUS VIEWEG*

I. EINLEITUNG – DAS DILEMMA DER JURISTEN

Als Jurist, der sich mit technischen Innovationen befasst, hat man eine ambivalente Rolle. Richtet man den Blick nicht nur auf die mit einer neuen Entwicklung, insbesondere technischer Art, verbundenen Vorteile, sondern auch auf die Nachteile, gilt man schnell als Blockierer und Verhinderer. Behält man die Bedenken für sich und realisiert sich später das eine oder andere Risiko, dann setzt man sich leicht dem Vorwurf aus, nicht rechtzeitig über juristische Tretminen informiert zu haben. Dies gilt insbesondere für den Bereich der technischen Sicherheit. Kollisionen mit dem allgemeinen Persönlichkeitsrecht und dem Datenschutzrecht sind ebenso vorprogrammiert wie Kosten-Nutzen-Überlegungen und diffizile Entscheidungsprozesse.

Erste Schwierigkeiten bestehen bei den Begriffen, die nicht nur für die quasi innerjuristische Kommunikation, sondern auch und gerade für die interdisziplinäre Lösung von Problemen hinreichend klar sein müssen. Wichtige Verständnisbrücken bilden insofern die technischen Normen (dazu II.). Weiter ist die überaus rasante technische Entwicklung in den Blick zu nehmen. Insbesondere die Digitalisierung und die Miniaturisierung haben zu einer Komplexität der Technik geführt, die die Beurteilung der technischen Sicherheit nicht nur für Juristen noch weiter erschwert, wenn nicht sogar unmöglich gemacht hat (dazu III.). Zum Dritten ist die technische Sicherheit immer mit der Wertungsfrage »Wie sicher ist sicher genug?« verbunden. Zielkonflikte sind unvermeidbar und besonders deutlich in § 1 EnWG angelegt (dazu IV.). Die Vielfalt technischer Risiken bedingt unterschiedliche rechtliche Sicherheitskonzepte, die häufig nur mit zeitlichem Verzug in Rechtsnormen ihren Niederschlag finden (dazu V.). Im Bereich der Verkehrssicherheit gibt es bereits zahlreiche Erfahrungen (dazu VI.), die auch für den Energiebereich nicht zuletzt deshalb wertvolle Anregungen geben können, weil neben den »klassischen« Mitteln der Sicherheitsgewährleistung die Digitalisierung zunehmend eine Rolle spielt.[1] Dasselbe gilt für die Problematik des Zugriffs auf Daten und den Datenschutz (dazu VII.).

* Der Verfasser erinnert sich gern und dankbar an die gemeinsamen (Lehr-) und Assistentenjahre mit dem Jubilar im Rechtswissenschaftlichen Seminar I der Universität Münster sowie an seine Vorträge in Erlangen (näher dazu Fn. 11).

1 Diesem Teil des Beitrags liegt der Vortrag zugrunde, den der Verfasser am 12. Januar 2012 im Rahmen des Braunschweiger Verkehrskolloquiums gehalten hat.

II. BEGRIFFE

1. Allgemeines

Technische Sicherheit ist eine interdisziplinäre Aufgabe, für deren Erledigung in erster Linie die entsprechenden (Fach-)Ingenieure zuständig sind. Diese müssen bei ihren Überlegungen und Entscheidungen allerdings die Rechtslage in den Blick nehmen,[2] sollen gravierende Vermarktungs- und Produkthaftungsprobleme vermieden werden. Umgekehrt müssen mit der Vertragsgestaltung beauftragte Juristen das ingenieurwissenschaftliche Begriffsvokabular kennen, um Fehlverständnisse und (kostenträchtige) Folgeprobleme von Anfang an auszuschließen. Die Frage lautet daher: Wissen alle an der technischen Sicherheit Beteiligten genau, wovon sie sprechen und wie sie verstanden werden? – Die Begriffsvielfalt[3] – hazard, (residual) risk, (acceptable) risk, damage, safety, security im englischsprachigen Raum sowie Gefährdung, Gefahr, Risiko, vertretbares Risiko, Restrisiko, Sicherheit[4] im deutschsprachigen Raum – lässt Zweifel aufkommen.

Nicht zuletzt durch den »New Approach«[5] und das »New Legislative Framework«[6] der Europäischen Kommission hat die technische Normung neben ihrem faktischen auch ein rechtliches Gewicht bekommen und sich zu einer wesentlichen Naht- und Schnittstelle sowie zu einer Kommunikationsbrücke zwischen Technik und Recht entwickelt. Von daher ist insbesondere danach zu fragen, ob in den technischen Normen Begriffe verwendet werden, die mit der Rechtsordnung in Einklang stehen. Im Fachbericht 144 des DIN »Sicherheit, Vorsorge und Meidung in der Technik«[7] hat sich eine Expertengruppe der Problematik angenommen. In terminologischer Hinsicht greift der Bericht die Begriffsdefinitionen der DIN 820-120[8] – der deutschen Übersetzung des ISO/IEC-Guide 51[9] – auf und kommt zu folgenden Definitionen:

2 So ausdrücklich IEC 61508-1 (2000), S. 17.
3 In meiner Dissertation »Atomrecht und technische Normung«, 1982, S. 223, habe ich die Überfülle begrifflicher Differenzierungen angesprochen. Nach meiner Erinnerung existierten seinerzeit über 70 unterschiedliche Begriffsvarianten.
4 Sicherheit wird z.T. sinnwidrig für Schutz verwendet. So heißt es z.B. »Sicherheitshelm« statt Schutzhelm.
5 Entschließung des Rates vom 07.05.1985 über eine neue Konzeption auf dem Gebiet der technischen Harmonisierung und Normung, ABl. EG Nr. C 136 v. 04.06.1985.
6 Beschluss Nr. 768/2008/EG über einen gemeinsamen Rechtsrahmen für die Vermarktung von Produkten und zur Aufhebung des Beschlusses 93/465/EWG des Rates, ABl. EU 2008 L 218/82.
7 DIN Deutsches Institut für Normung e. V. (Hrsg.), DIN-Fachbericht 144: Sicherheit, Vorsorge und Meidung in der Technik, 2005.
8 DIN 820-120 (Ausgabe 2008–2009) Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen.
9 ISO/IEC-Guide 51 (1999) Standardization – Part 120: Guidelines for the inclusion of safety aspects in standards.

Risiko ist durch die Kombination aus der Wahrscheinlichkeit des Schadenseintritts und dem Ausmaß des Schadens definiert. Die Berücksichtigung von Chancen sowie eine Verrechnung mit Nachteilserwartungen finden nicht statt. Die Begriffe *Gefahr* und *Sicherheit* sind komplementär, indem sie auf das Vorhandensein bzw. die Abwesenheit eines nach den gültigen Wertvorstellungen der Gesellschaft unvertretbaren Risikos hinweisen. Als Übersetzung des englischen Begriffs *hazard* wird der Begriff *Gefährdung* eingeführt, um eine potenzielle Schadensquelle zu bezeichnen. Von der *Gefährdungssituation* – einem Zustand, in dem Menschen, Güter und/oder die Umwelt einer oder mehreren konkreten Gefährdungen ausgesetzt sind – ist die *Vorsorgesituation* zu unterscheiden. Diese zeichnet sich dadurch aus, dass – ohne einen sicheren Beweis – ein begründeter Verdacht hinsichtlich eines kausalen Schadensablaufs besteht. Die Beantwortung der Frage, welche Vorkehrungen (vorsorglich) zu treffen sind, unterliegt auch Nützlichkeitserwägungen. Chancen und Risiken werden abgewogen und zu einer von Verhältnismäßigkeitsüberlegungen geprägten Lösung verarbeitet (sog. *risk management*). Hierin liegt ein wesentlicher Unterschied zur Risikobearbeitung (sog. *risk treatment*), bei der es ausschließlich um die Minderung von Risiken geht, ohne die Chancen zu berücksichtigen, die das Produkt mit sich bringt. Die Risiken sind vielmehr so lange zu mindern, bis das sog. Restrisiko nicht größer ist als das *maximal vertretbare Risiko.* Die Frage »Wie sicher ist sicher genug?« ist danach methodisch unterschiedlich zu beantworten, sobald das nach den »gültigen Wertvorstellungen der Gesellschaft unvertretbare Risiko« (= maximal vertretbares Risiko) in einem ersten Schritt festgestellt ist. Die damit verbundenen methodischen Schwierigkeiten, die Wertvorstellungen und wertenden Lösungen von Zielkonflikten zu präzisieren, liegen auf der Hand. Einigkeit besteht insofern, dass die Berücksichtigung von Chancen und Nutzen sowie Kosten – sozusagen als zweiter Prüfungsschritt – lediglich im sog. Vorsorgebereich erfolgen darf.

Zwei im Erlanger Institut für Recht und Technik erstellte Beiträge[10] kommen zu dem erfreulichen Ergebnis, dass der Fachbericht 144 des DIN dem juristischen Begriffsverständnis der gesetzlichen Regelungen im Bundesimmissionsschutzgesetz, der Störfallverordnung, dem Geräte- und Produktsicherheitsgesetz sowie dem Produkthaftungsgesetz sehr nahe kommt und damit eine wertvolle Verständnisbrücke zwischen Technik und Recht bildet.

10 *F. Dietz/T. Regenfus* Risiko und technische Normung im Spannungsfeld von Recht und Technik, in: K. Vieweg (Hrsg.), Risiko – Recht – Verantwortung, 2006, S. 403–429; *T. Regenfus/K. Vieweg* Sicherheits- und Risikoterminologie im Spannungsfeld von Technik und Recht, in: P. Winzer/E. Schnieder/F.-W. Bach (Hrsg.), Sicherheitsforschung – Chancen und Perspektiven, 2010, S. 131–144.

2. Anwendung auf das Produkthaftungsgesetz

Da Haftungsfragen für Peter Salje immer von besonderem Interesse waren,[11] sollen die für das Produkthaftungsgesetz erzielten Ergebnisse kurz referiert werden. In seinem Anwendungsbereich kann beim Produkthaftungsgesetz (ProdHaftG) zumindest im Ansatz zwischen dem Schutz- und dem Vorsorgeprinzip differenziert werden. Dabei kommt dem Schutzprinzip eine überragende Bedeutung zu. Eine zentrale Rolle spielt der Fehlerbegriff des § 3 Abs. 1 ProdHaftG. Danach ist ein Produkt fehlerhaft, wenn es nicht die Sicherheit bietet, die unter Berücksichtigung aller Umstände, insbesondere seiner Darbietung, des Gebrauchs, mit dem billigerweise gerechnet werden kann, sowie des Zeitpunkts, in dem es in den Verkehr gebracht wurde, berechtigterweise erwartet werden kann. Im Hinblick auf den Gebrauch des Produkts gilt es zu berücksichtigen, dass dieser grundsätzlich nicht nur die bestimmungsgemäße Verwendung, sondern auch den vorhersehbaren Fehlgebrauch umfasst. Es bedarf insoweit einer Abgrenzung zwischen einem (noch) haftungsrelevanten Fehlgebrauch und einem der Risikosphäre des Herstellers nicht mehr zurechenbaren Missbrauch des Produkts. Die maßgeblichen Sicherheitserwartungen sollen nach vielfach vertretener Auffassung[12] anhand des Horizonts der durch die fehlende Produktsicherheit betroffenen Allgemeinheit bestimmt und beurteilt werden. Teilweise[13] wird auch auf das Verständnis eines verständigen Verbrauchers abgestellt. Unter Ausblendung einiger Detailfragen ist insoweit nach allgemeiner Auffassung eine objektive Betrachtungsweise geboten. Einzubeziehen sind dabei nicht nur die berechtigten Sicherheitserwartungen der Produktnutzer selbst, sondern auch diejenigen außenstehender Dritter (sog. »innocent bystanders«).[14]

Die Feststellung des Vorliegens eines Produktfehlers orientiert sich demnach grundsätzlich an den im Hinblick auf die Risikobearbeitung dargestellten Erwägungen.[15] Die Perspektive ist jedoch insoweit eine etwas andere, als das Haftungsregime des ProdHaftG reaktiv und retrospektiv auf den Eintritt eines Schadens abstellt. Das

11 Der Verfasser denkt dankbar an seine Vorträge im Rahmen von Erlanger Symposien zurück. Vgl. *P. Salje* Ökonomische Analyse des Technikrechts, in K. Vieweg (Hrsg.), Techniksteuerung und Recht, 2000, S. 151 ff; *ders.* Zivilrechtliche Aspekte des Datencontents beim Sacherwerb – Hersteller-Produkthaftung für elektonische Bauteile, in: K. Vieweg/H. Gerhäuser (Hrsg.), Digitale Daten in Geräten und Systemen, 2010, S. 221 ff. Grundlegend für das Technikrecht *P. Salje* Anlagenhaftungsrecht, in: M. Schulte/R. Schröder (Hrsg.), Handbuch des Technikrechts, 2. Aufl., 2011, S. 281 ff.

12 So etwa Staudinger/*J. Oechsler* (2009) § 3 ProdHaftG Rn. 15 m. w. N.; Soergel/*R. Krause* 13. Aufl. 2005, § 3 ProdHaftG Rn. 3.

13 So etwa *U. Foerste* in: U. Foerste/F. Graf von Westphalen (Hrsg.), 3. Aufl. 2012, § 24 Rn. 4 ff.; Erman/*G. Schiemann* 13. Aufl. 2011. § 3 ProdHaftG Rn. 2.

14 MünchKomm/*G.* Wagner 5. Aufl. 2009, § 3 ProdHaftG Rn. 5; Staudinger/*J. Oechsler* (Fn. 12) Rn. 17, 20; *Soergel/R. Krause* 13. Aufl. 2005, § 3 ProdHaftG Rn. 3; *F. Graf v. Westphalen* in: U. Foerste/F. Graf v. Westphalen (Hrsg.), Produkthaftungshandbuch, 3. Aufl. 2012, § 74 Rn. 13.

15 Siehe oben II.

Nichtvorliegen einer hinreichenden Risikobearbeitung wird als Ansatzpunkt für eine Haftung für Personen- und Vermögensschäden genommen. Es gilt demnach auch für das Haftungsrecht zu klären, wie sicher sicher genug ist. Die Abgrenzung zur Vorsorge ist allerdings im Bereich der Haftung nicht vergleichbar konsequent realisiert. So können nach nahezu unbestrittener Auffassung – anders als im Bereich der Risikobearbeitung – auch wirtschaftliche Erwägungen miteinbezogen werden.[16] Insbesondere soll dem Preis des Produkts eine erhebliche Bedeutung zukommen können.[17] Eine Schranke, die nicht unterschritten werden darf, bildet allerdings die sog. Basissicherheit. Zumindest elementarsten Sicherheitsanforderungen muss das Produkt unabhängig von einem unter Umständen niedrigen Preis genügen.[18]

Besonderheiten können sich bei Vorliegen zwingender gesetzlicher Vorgaben ergeben. Soweit dem Hersteller der Nachweis gelingt, diese vollumfänglich beachtet zu haben, scheidet gemäß § 1 Abs. 2 Nr. 4 ProdHaftG eine Haftung aus. Anders zu beurteilen ist dies im Hinblick auf die Einhaltung technischer Normen, die aus Sicht des Haftungsrechts zumeist nicht mehr als einen unabdingbaren Mindeststandard beschreiben.[19] Insoweit kommt das Vorsorgeprinzip – anders als etwa im Bereich der Produktsicherheit – nicht zum Tragen. Als eine weitere wichtige Haftungsausschlussnorm ist in diesem Zusammenhang § 1 Abs. 2 Nr. 5 ProdHaftG zu nennen. Dieser stellt im Zusammenwirken mit § 3 Abs. 2 ProdHaftG klar, dass eine Haftung ausscheidet, soweit der Fehler nach dem Stand der Wissenschaft und Technik in dem Zeitpunkt, in dem der Hersteller das Produkt in den Verkehr brachte, nicht erkannt werden konnte (sog. Entwicklungsfehler). Die Erkennbarkeit richtet sich dabei wiederum nicht nach individuellen, sondern vielmehr nach rein objektiven Maßstäben.[20] Von einem derartigen Entwicklungsfehler sind sog. Entwicklungslükken abzugrenzen, bei denen der Hersteller den Fehler zwar erkennen, ihn jedoch nach dem Stand der Wissenschaft und Technik nicht verhindern konnte. Bei Vorliegen einer Entwicklungslücke hat ein Inverkehrbringen ggf. zu unterbleiben.[21] Falls sich der Hersteller trotz erkannter, technisch nicht zu vermeidender Produktfehler für ein Inverkehrbringen entscheidet, folgt daraus eine Haftung des Herstellers nach dem ProdHaftG. Im Ergebnis verlangt auch das ProdHaftG vom Hersteller grundsätzlich eine hinreichende Risikobearbeitung. Eine Haftung scheidet nur dann aus, wenn der Produktfehler objektiv im Zeitpunkt des Inverkehrbringens nicht erkannt werden konnte.

16 Vgl. Staudinger/*J. Oechsler* (Fn. 12), Rn. 86 ff. m. w. N.
17 Vgl. *K. Vieweg* Produkthaftung, in: *M. Schulte/R. Schröder* Handbuch des Techniksrechts, 2. Aufl. 2011, S. 337 (348, 377); Staudinger/*J. Oechsler* (Fn. 12), Rn. 36, 86 ff.
18 Vgl. Staudinger/*J. Oechsler* (Fn. 12), Rn. 88 m. w. N.; vgl. auch BGHZ 51, 91 (108) (Hühnerpest); BGH NJW 1972, 2217 (2220) (Kurznarkosemittel ESTIL); BGHZ 114, 284 (291 f.) (Blutkonserve).
19 *K. Vieweg* (Fn. 17), S. 337 (366 f.).
20 BGH NJW 2009, 2952 Tz. 28 (Auto-Airbag); *K. Vieweg* (Fn. 17), S. 337 (380); vgl. auch *U. Foerste* in: U. Foerste/F. Graf von Westphalen (Hrsg.), 3. Aufl. 2012, § 24 Rn. 103 ff.
21 *K. Vieweg* (Fn. 17), S. 337 (379).

III. ENTWICKLUNGSTENDENZEN: DIGITALISIERUNG UND MINIATURISIERUNG

Drei Schlüsselfaktoren prägen die technische Entwicklung der letzten Jahre.[22] Erster und besonders wichtiger Schlüsselfaktor für die technische Entwicklung ist die *Digitalisierung.* Durch die einheitliche Verwendung von Bits und Bites unabhängig von der Art der Information – Text, Sprache, Musik, Graphik, Bilder, Videos, Kommandos – und die einheitliche Technik für die digitale Signalverarbeitung sowie die Datenreduktion durch Quellenkodierung wird eine – nur durch den technischen Aufwand begrenzte – hohe Qualität der Darstellung von Informationen gewährleistet. Hinzu kommt – in praktischer Hinsicht ein ganz wesentlicher Aspekt – die Möglichkeit des verlustfreien Kopierens. Als zweiter Schlüsselfaktor der Entwicklung ist die *Mikroelektronik* zu nennen.[23] Konkret geht es um zunehmende Taktraten, große Speicher, kleinere Abmessungen und höhere Integrationsdichten sowie einen immer geringer werdenden Stromverbrauch und stetig sinkende Kosten pro Bit bzw. Transistor. Prägnant gibt das sog. Moor'sche Gesetz diese Entwicklung wieder. Danach verdoppeln sich die Rechenleistung, die Anzahl und die Dichte von Transistoren auf einem Chip in einem relativ kurzen Zeitraum von etwa zwei Jahren, halbieren sich die Kosten pro Transistorfunktion alle drei Jahre und verdoppelt sich der Entwurfsaufwand für einen Chip alle drei Jahre.[24] Als dritter Schlüsselfaktor lässt sich die *drahtlose Kommunikation* identifizieren. Sie ermöglicht einen »grenzenlosen« Informationsaustausch unabhängig von Ort und Zeit.[25]

Die beschriebene Entwicklung hat selbstverständlich auch den Kraftfahrzeugbereich erfasst, eine Vielzahl von Automatisierungs- und Assistenzsystemen hervorgebracht und das Kraftfahrzeug zum »rollenden Computer« werden lassen. Dabei haben die Miniaturisierung und die Verwendung von Software in eingebetteten Systemen (mechatronic implementation) zu einer Komplexität des technischen Produkts Kraftfahrzeug geführt, die nicht nur für den Nutzer Funktionsstörung und -ausfall nicht nachvollziehbar macht. Auch die Fachleute in den Werkstätten stehen bisweilen vor einem Rätsel und haben das Problem, den Fehler im Zusammenspiel von Mechanik, Elektronik und Software herausfinden zu müssen.

22 Hierzu im Einzelnen *H. Gerhäuser* Digitale Daten in Geräten und Systemen – Entwicklung und Perspektiven, in: K. Vieweg/H. Gerhäuser (Hrsg.), Digitale Daten in Geräten und Systemen, 2010, S. 1 (3 f.).
23 *H. Gerhäuser* (Fn. 22), S. 4 ff.
24 *H. Gerhäuser* (Fn. 22), S. 10.
25 *H. Gerhäuser* (Fn. 22), S. 4.

IV. ZIELKONFLIKTE UND WERTUNGSPROBLEME

§ 1 EnWG dokumentiert in geradezu klassischer Weise die Zielkonflikte, die sich im Zusammenhang mit der technischen Sicherheit stellen. Zu den bereits im EnWG 1935 formulierten energiepolitischen Zielen Versorgungssicherheit und Preisgünstigkeit trat mit der Novelle des EnWG 1998 die Umweltverträglichkeit hinzu. Mit den Aspekten Verbraucherfreundlichkeit und Effizienz entstand im Zuge der Novelle 2005 das *Ziele-Fünfeck* des § 1 Abs. 1 EnWG. Die fünf Ziele stehen zueinander nicht in einem Rangverhältnis.[26] Das zwischen ihnen bestehende Spannungsverhältnis kann deshalb nur im Sinne einer Optimierung unter Berücksichtigung der jeweiligen Wechselwirkungen im Einzelfall im Wege der Abwägung aufgelöst werden.[27]

Ähnlich differenziert formuliert die Satzung des Deutschen Instituts für Normung (DIN) die Normungsziele. In §1 (2) Satzung des DIN heißt es, dass das DIN »durch Gemeinschaftsarbeit der interessierten Kreise, zum Nutzen der Allgemeinheit Deutsche Normen oder andere Arbeitsergebnisse, die der Rationalisierung, der Qualitätssicherung, dem Umweltschutz, der Sicherheit und der Verständigung in Wirtschaft, Technik, Wissenschaft, Verwaltung und Öffentlichkeit dienen, aufstellt, sie veröffentlicht und ihre Anwendung fördert.«[28]

Konflikte bestehen regelmäßig zwischen den Zielen Sicherheit, Praktikabilität, Umweltverträglichkeit und Wirtschaftlichkeit. Mit diesen Zielkonflikten sind Wertungsfragen verbunden: Wie sicher ist sicher genug? Wie umweltverträglich ist hinreichend umweltverträglich? Welches Maß an Praktikabilität reicht aus? Wo ist die Grenze zwischen wirtschaftlich und unwirtschaftlich zu ziehen?

Selbst wenn die rechtlichen Vorgaben dem von einem technischen Risiko Betroffenen die Entscheidung über die Sicherheitsmaßnahmen überlassen – Steuerungsmodell der Selbstregulierung –, wird sich der Betroffene vor seiner Entscheidung im Regelfall nicht alle möglichen Entscheidungsvarianten deutlich machen, sondern mehr oder weniger spontan eine Entscheidung anhand seines Informationsstandes treffen.

Sollten die rechtlichen Vorgaben eine der vielen Varianten kooperativer oder imperativer Steuerung[29] vorsehen, so sind die Entscheidungsprozesse zur Lösung

26 Vgl. BT-Drucks. 13/7274 vom 23.03.1997, S. 31.

27 So zutreffend *C. Theobald* in: W. Danner/C. Theobald, Energierecht, Kommentar (Bd. 1), Stand: Januar 2007, § 1 Rn. 26.

28 Vgl. zur Satzungserweiterung auf das Ziel Umweltschutz und den sich daraus ergebenden Konsequenzen *K. Vieweg* Produktbezogener Umweltschutz und technische Normung, in: P. Marburger (Red.), Jahrbuch des Umwelt- und Technikrechts, 1995, S. 509 ff.

29 Vgl. hierzu z.B. *W. Hoffmann-Riehm* Innovation durch Recht und im Recht, in: Schulte (Hrsg.), Technische Innovation und Recht, 1997, S. 3 (13 ff.) sowie *A. Röthel* Europarechtliche Vorgaben für das Technikrecht, in: M. Schulte/R. Schröder (Hrsg.), Handbuch des Technikrechts, 2. Aufl. 2011, S. 201 (214 ff.).

dieser Zielkonflikte und zur Beantwortung der Wertungsfragen für die Betroffenen keineswegs immer transparent, sondern gleichen häufig eher einer Blackbox.[30]

Dabei lehrt die Erfahrung, dass Transparenz nicht zwangsläufig zu einem höheren Maß an Akzeptanz führt. So bestand in den 1970er Jahren verbreitet die Idee, mit einer Quantifizierung der von technischen Anlagen, insbesondere von Kernenergieanlagen ausgehenden Risiken und einem Vergleich mit Naturrisiken wie Blitzschlag oder mit den von anderen Industrien ausgehenden Risiken zu einer breiteren Akzeptanz zu gelangen. Die Anwendung probabilistischer Methoden erlaubte zwar eine Quantifizierung der Risiken. Der sich anschließende Risikovergleich – z.B. mit der chemischen Industrie – führte allerdings nicht zur Lösung des Akzeptanzproblems, sondern eher zu einer Ausweitung der Akzeptanzprobleme auf diese Industriezweige.[31]

V. SICHERHEITSKONZEPTE

Die gesetzlichen Vorgaben in § 3 (1), (2) ProdSG, in § 3 ProdHaftG und in § 19 StVZO[32] enthalten im Hinblick auf die technische Sicherheit unbestimmte, konkretisierungsbedürftige Rechtsbegriffe. Als Verständigungsbrücke zwischen Recht und Technik kommen insofern die einschlägigen technischen Normen in Betracht. So ist aus juristischer Sicht interessant, welche Sicherheitskonzepte die ISO (International Standardization Organization) und die IEC (International Electrotechnical Commission) vorgeben.

Das technische Sicherheitsrecht hat in den letzten drei Jahrzehnten einen erheblichen Wandel durchgemacht. Grund hierfür ist zum einen die üblicherweise mit Verzögerung auf technische Entwicklungen reagierende Rechtsordnung – der »legal lag«.[33] So werden die mit der Digitalisierung neu aufgetretenen Probleme erst sukzessive erkannt und rechtlich erfasst. Zum anderen hat uns Europa nicht nur die Idee eines dynamischen Binnenmarkts beschert, sondern zu seiner Realisierung auch eine Harmonisierung in vielen technikrelevanten Bereichen. So wurde das

30 Zu den Entscheidungsprozessen s. im Einzelnen *K. Vieweg* Thesen zum Problemfeld Technische Sicherheit aus juristischer Sicht, in: P. Winzer/E. Schnieder/F.-W. Bach (Hrsg.), Sicherheitsforschung – Chancen und Perspektiven, 2010, S. 117 (123 ff.).

31 Vgl. *K. Vieweg* Diskussionsbericht, in: R. Lukes (Hrsg.), Gefahren und Gefahrenbeurteilungen im Recht – Rechtliche und technische Aspekte von Risikobeurteilungen, insbesondere bei neuen Technologien, Teil I: Vorträge und Diskussionsberichte, 1980. S. 177 (188 ff.).

32 Umsetzung von Art. 4 der Richtlinie 2007/46/EG des Europäischen Parlaments und des Rates v. 05.09.2007 zur Schaffung eines Rahmens für die Genehmigung von Kranftfahrzeugen und Kraftfahrtzeuganhängern sowie von Systemen , Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge, ABl. L 263 v. 09.10.2007, S. 1 ff.

33 *K. Vieweg* Reaktionen des Rechts auf Entwicklungen der Technik, in: M. Schulte (Hrsg.), Technische Innovation und Recht, 1997, S. 35 (36) m.w.N.; insb. *ders.* JuS 1993, 896.

Produkthaftungsrecht weitgehend vereinheitlicht.[34] Dasselbe gilt für die Produktsicherheit.[35] Die deutsche Rechtsentwicklung lässt sich stichworthaft an den Gesetzen ablesen: Es beginnt mit dem Gesetz über technische Arbeitsmittel GTA (1968), zunächst Maschinenschutzgesetz, dann (1980) Gerätesicherheitsgesetz, GSG genannt. Es folgte die GSG-Novellierung 1992 zur Umsetzung der sog. Maschinenschutzrichtlinie,[36] der sich eine weitere Novellierung im Jahr 2000 anschloss. 1997 wurde das Produktsicherheitsgesetz ProdSiG geschaffen, welches 2004 mit dem GSG im Geräte- und Produktsicherheitsgesetz GPSG zusammengeführt wurde. Vorläufiger Endpunkt ist das zum 1. Dezember 2011 in Kraft getretene neue Produktsicherheitsgesetz (Gesetz über die Bereitstellung von Produkten auf dem Markt – ProdSG).[37]

Die gesetzlichen Vorlagen z.B. in § 3 (1), (2) ProdSG enthalten im Hinblick auf die technische Sicherheit konkretisierungsbedürftige, unbestimmte Rechtsbegriffe. Dass es sich hierbei um praktisch unvermeidbare Gesetzesmethodik handelt, zeigen das zeitweise erfolgte, allerdings missglückte Streben der EG-Kommission nach Harmonisierungsrichtlinien. In diesen Richtlinien wurden die technischen Spezifikationen akribisch aufgelistet. Folge war der spöttische Vergleich der Wörterzahl der Zehn Gebote mit derjenigen sehr spezieller EG-Richtlinien wie beispielsweise der Richtlinie zur Harmonisierung der technischen Anforderungen an die Beifahrersitze von Traktoren.[38] Der Dynamik der technischen Entwicklung vermochten weder umfangreiche Richtlinienanhänge mit technischen Spezifikationen noch die vollständige Inkorporation technischer Normen oder die starre Verweisung auf technische Normen hinreichend Rechnung zu tragen. Zudem dauerten die Erlassverfahren derartiger Richtlinien nicht selten ca. zehn Jahre.[39] Diesem Missstand begegneten der sog. New Approach vom Mai 1985[40] und das New Legislative Framework des Jahres 2008[41]. Sie haben dazu geführt, dass die europäische technische Normung insbesondere durch CEN und CENELEC mit ihren konkretisierten Sicherheitsanforderungen das von den europäischen Richtlinien vorgegebene »hohe Sicherheitsniveau« in praktische Beschaffenheits- und Verhaltensanforderungen umsetzen. Damit wird die Beantwortung der Frage »Wie sicher ist sicher genug?« und die

34 Vgl. Richtlinie 85/374/EWG des Rates v. 25.07.1985 zur Angleichung der Rechts und Verwaltungsvorschriften der Mitgliedsstaaten über die Haftung von fehlerhaften Produkten, ABl. Nr. L 210 vom 07/08/1985 S. 29 ff.

35 Vgl. Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates v. 03.12.2001 über die allgemeine Produktsicherheit, ABl. EG Nr. L 11/4 v. 15.01.2002.

36 Richtlinie 89/392/EWG des Rates v. 14.06.1989 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten für Maschinen, ABl. EG Nr. L 183 S. 9.

37 Überblick bei *A. Kapoor/Th. Klindt* in NVwZ 2012, 719 ff.

38 Richtlinie des Rates 76/763/EWG v. 27.07.1976 zur Angleichung der Rechtsvorschriften der Mitgliedsstaaten über die Beifahrersitze von land- oder forstwirtschaftlichen Zugmaschinen auf Rädern, ABl. Nr. L 262 v. 27.09.1976 S. 135.

39 *K. Vieweg* Technische Normen im EG-Binnenmarkt, in: P.-C. Müller-Graff (Hrsg.), Technische Regeln im Binnenmarkt, 1991, S. 57 (63) m. w. N.

40 Siehe oben Fn. 5.

41 Siehe oben Fn. 6.

Entscheidung von Zielkonflikten zwischen Sicherheit, Praktikabilität, Umweltverträglichkeit und Wirtschaftlichkeit im harmonisierten Bereich (zunächst) auf die Normungsorganisationen verlagert.

Überzeugend ist aus meiner Sicht, dass die IEC 61508[42] alle Phasen des »gesamten Sicherheitszyklus« – vom Konzept und der Planung über die Inbetriebnahme bis zur Außerbetriebnahme und Deinstallation – sowohl des gefahrverursachenden Systems als auch der risikomindernden Systeme erfasst. Mit der Einführung des Kunstbegriffs »Sicherheitsintegrität« (safety integrity) – gemeint ist die Schutzfunktion mit dem Ziel eines sicheren Zustandes – trägt die IEC 51568 dem Umstand Rechnung, dass die Wirksamkeit von Sicherheitsfunktionen nicht nur von der Zuverlässigkeit im Gefährdungsfall, sondern auch durch Ausschaltung der gefahrverursachenden Systeme bei Erkennung von Fehlern in den sicherheitsbezogenen Systemen erreicht werden kann. Zweckmäßig ist jedenfalls die Differenzierung in vier Sicherheitsanforderungsstufen (Safety Integrity Level – SIL) als Maß für die notwendige bzw. erreichte risikominimierende Wirksamkeit der Sicherheitsanforderungen. Dies gilt vor allem, weil die Bestimmung der SIL über qualitative oder quantitative Risikoanalysen erfolgt.

Im Kfz-Bereich gilt der Automative Safety Integrity Level (ASIL), der ebenfalls vier Sicherheitsanforderungsstufen kennt, deren Ermittlung ebenso durch quantitative und qualitative Methoden erfolgt (z.B. Failure Mode and Effects Analysis – FMEA; Fault Tree Analysis – FTA). Dabei sind der Verletzungsgrad, die Häufigkeit der Situation und die Beherrschbarkeit der Situation durch den Fahrzeugführer für die Risikoeinschätzung maßgeblich.

Anders als in der IEC 61508 geschieht die Risikoanalyse in der ISO/DIS 26262 mittels einer festgelegten qualitativen Methodik. Jede identifizierte Gefährdung muss einzeln auf die Schwere ihrer Auswirkung, die Häufigkeit der Fallsituation und die Beherrschbarkeit durch den Fahrer abgeschätzt werden. Aus einer Tabelle lässt sich dann für jede Gefährdung die Einstufung ablesen.

Bei der Auswahl der von IEC 61508-5 vorgesehenen Methoden zur Bestimmung der SIL-Voraussetzungen fällt die ALARP-Methode auf. Hier zeigen sich Parallelen zur Gesetzgebung im Vereinigten Königreich: »So far as is reasonably practicable«[43], »as low as reasonably practicable« und »as low as reasonably achievable« sind verbreitete Gesetzesformulierungen.

VI. VERKEHRSSICHERHEIT UND TECHNISCHE ENTWICKLUNG

Die Entwicklung moderner Fahrzeugelektronik hat dazu geführt, dass Kraftfahrzeuge als »rollende Computer« bezeichnet werden und dass bei Unfällen »klassische

42 Näher dazu unter VI.

43 *K. Vieweg* Gefahren und Gefahrenbeurteilungen in der Rechtsordnung Großbritanniens, in: H. Lukes (Hrsg), Gefahren und Gefahrenbeurteilungen im Recht, Teil III, 1980, S. 1 (42 f.).

Unfallspuren« (wie Bremsspuren) zusehends verschwinden. Polizei und Sachverständige werden deshalb mehr und mehr mit »sauberen Unfallorten« konfrontiert.[44] Kommt es zu einem Unfall von zwei nach neuestem Stand mit Assistenzsystemen ausgestatteten Kraftfahrzeugen, so stellen sich interessante Fragen, insbesondere hinsichtlich des Zugriffs auf die gespeicherten Daten und des Datenschutzes. Gewiss haben diese technischen Entwicklungen zur Erhöhung der aktiven und passiven Sicherheit ihren Beitrag dazu geleistet, dass die Anzahl der Verkehrstoten in den letzten Jahrzehnten erfreulich zurückgegangen ist. Daneben dürften aber auch die Verbesserung der Infrastruktur sowie die Einführung von Tempolimit, Promillegrenze, Helm- und Gurtpflicht eine Rolle spielen. Das offene System der Verkehrssicherheit ist und bleibt ein Experimentierfeld mit technischen, ökonomischen, ökologischen, psychologischen und juristischen Aspekten. So bleibt abzuwarten, welche Erfolge mit der Einführung des Führerscheins auf Probe verbunden sind. Zurzeit werden außerdem diskutiert die Veröffentlichung der Standorte von Radarfallen im Internet, die Helmpflicht für Radfahrer und die Spurbreite bei Autobahn-Baustellen.

Die zur Steigerung der Verkehrssicherheit eingeführten Automatisierungs- und Assistenzsysteme sind ein gutes Beispiel für die Ambivalenz technischer Entwicklungen. Nutzen und Vorteile einerseits sowie Nachteile und Herausforderungen andererseits liegen auf der Hand. Dazu einige Beispiele:

- Antiblockiersystem (ABS), Elektronisches Stabilitätsprogramm (ESP), Abstandsregeltempomat (Adaptive Cruise Control – ACC), Notbremssystem (Advanced Emergency Braking System – AEBS), Spurhalte-,Spurwechsel- und Einparkassistent sowie »Eye-Tracker« helfen, Unfälle zu vermeiden. Kommt es dennoch zum Unfall, so gibt es am Unfallort (häufig) nicht mehr die »klassischen« Bremsspuren, die für Polizei und Sachverständige Grundlage der Unfallrekonstruktion hätten sein können. »Digitale Spuren« in Unfalldatenspeichern und in den eingebetteten Systemen müssen ausgelesen werden. Wer kann das überhaupt? Wer darf das? Wem gehören diese Daten?
- Car to car bzw. infrastructure communication soll helfen, Kollisionen zu vermeiden, Staus zu reduzieren und Kraftstoff zu sparen, setzt aber die Übermittlung von Standortdaten (über GPS) voraus. Aufenthaltsorte und Bewegungsprofile sind sensible personenbezogene Daten und damit datenschutzrechtlich brisant.
- »Eye-Tracker« – vom Fraunhofer Institut für Digitale Medientechnologie als Prototyp vorgestellt[45] – sollen dazu dienen, das Problem des Sekundenschlafs in den Griff zu bekommen. Doch wie ist zu verfahren, wenn das System versagt und

44 *M. Münchhausen* Die Auswertung von Fahrzeugdaten bei der Unfallanalyse, in: Deutsche Akademie für Verkehrswissenschaft (Hrsg.), 45. Verkehrsgerichtstag 2007, 2007, S. 275; *K. Vieweg* eda., S. 292 ff.

45 Vgl. Presseinformation des Fraunhofer Instituts vom 12.10.2010, abrufbar unter http://www.fraunhofer.de/de/presse/presseinformationen/2010/10/eye-tracker-sekundenschlaf-blickrichtungserkennung.html (abgerufen am 08.08.2012).

der ermüdete Fahrer sich trotz gegenteiligen Hinweises darauf verlassen hat, dass es sicher funktioniert und er wachgehalten wird? Wer muss das Funktionieren bzw. das Versagen des Systems im Schadensfall beweisen?

– Zum Versagen von Automatisierungs- und Assistenzsystemen kann es auch durch Eingriffe von außen kommen. Dass die Fahrertür nicht geöffnet werden kann, wenn jemand sich vor die Tür stellt, und dass damit das zur Vermeidung von Kollisionen insbesondere mit Fahrradfahrern dienende System funktioniert, ist ein vergleichsweise harmloses Beispiel. Die Umgehung elektronischer Wegfahrsperren dadurch, dass der Fahrer zum Anhalten veranlasst und mit Waffengewalt zum Aussteigen gezwungen wird (sog. Carjacking), zeigt die Reaktion Krimineller auf technische Innovationen. Erfreulich ist, dass die Technik ihrerseits darauf reagiert hat und mit der Telematikbox Novanto eine ferngesteuerte Außerbetriebsetzung ermöglicht.[46] Ernste Gefahren ergeben sich aber beispielsweise, wenn vom Straßenrand aus mit einem Laptop in die Car to car bzw. infrastructure communication eingegriffen wird.

Die Begleitung der technischen Entwicklung durch eine Fortentwicklung der einschlägigen technischen Normung ist in diesem konkreten Bereich besonders interessant: Die IEC 61508 (Functional safety of electrical/electronic/programmable electronic safety-related systems) wurde 2010 in überarbeiteter Form veröffentlicht. Die Neufassung der ISO/DIS 26262 (Road vehicles – Functional safety) wurde am 14. November 2011 in Kraft gesetzt und erfasst vom Anwendungsbereich her Kraftfahrzeuge bis 3,5 t.

VII. Zugriff auf Daten und Datenschutz

1. Zugriff auf Daten

Die Anzahl der elektronischen Steuergeräte in Kraftfahrzeugen steigt stetig an. Das Bild des »rollenden Computers« beschreibt treffend die Situation. Konsequenz der modernen Assistenz- und Sicherheitssysteme ist unter anderem, dass »klassische« Unfallspuren verschwinden und zusehends »saubere« Unfallorte hinterlassen werden. Über diese Tatsache und die Speicherung punktueller Daten informieren die Hersteller den Kunden regelmäßig nicht.

46 Pressemittelung Continental vom 23.09.2010, abrufbar unter http://www.conti-online.com/generator/www/com/de/continental/presseportal/themen/pressemitteilungen/1_topics/conticompact/md_2010_09_23_diebstahltracker_de.html (abgerufen am 08.08.2010).

Bei digitalen Daten ist zu unterscheiden zwischen Diagnosedaten[47] – sie dienen ausschließlich der Wartung und Weiterentwicklung –, punktuellen Daten[48] – diese werden ereignisbedingt in den Steuergeräten gespeichert – und Unfalldaten[49] – sie dienen der umfassenden Rekonstruktion eines Unfallgeschehens. Diagnose- und punktuelle Daten sind zur Unfallrekonstruktion nur eingeschränkt nutzbar. Die Speicherung von Unfalldaten wird – so führende Hersteller – von den Kunden z. Zt. nicht gewünscht und unterbleibt daher bislang.[50]

Für die Frage, wem die gespeicherten Daten »gehören«, wer also die Befugnis hat, sie auszulesen bzw. auslesen zu lassen und zu verwerten, ist zunächst die Interessenlage zu berücksichtigen. Diese erweist sich aus mehreren Gründen als komplex. Zum einen ist sie für jeden der unmittelbar oder mittelbar am Unfall Beteiligten ambivalent, je nachdem, ob die aus den gespeicherten digitalen Daten ableitbaren Informationen für ihn nützlich oder nachteilig sind. Zum anderen ist nach den drei Datenarten zu differenzieren. Hinsichtlich der Unfalldaten und der punktuellen Daten ist im Hinblick auf die Interessenlage zwischen Produkthaftungs- und -gewährleistungsfällen einerseits sowie Verkehrsunfällen andererseits zu unterscheiden.

So sind in Produkthaftungs- und Gewährleistungsfällen die Interessen von Kunden und Herstellern (Lieferanten) gegenläufig. Dabei ist aber unklar, welche Interessen außer der Abwehr von Produkthaftungs- und Gewährleistungsklagen mit dem einheitlichen Verzicht der Speicherung von Unfalldaten bzw. punktuellen Daten durch deutsche Hersteller verfolgt werden.[51] Bei Verkehrsunfällen stehen sich die Interessen der am Unfall Beteiligten bzw. der jeweiligen Versicherer gegenüber.[52]

Neben diesen Konstellationen tritt der generelle Aspekt der Verkehrssicherheit – die Prävention – in den Blick. Nach den im Rahmen von Pilotversuchen mit dem Unfalldatenspeicher gewonnenen Erfahrungen wird überwiegend prognostiziert, dass die Speicherung digitaler Unfalldaten einen durchaus erheblichen Präventiveffekt mit sich bringen und damit wesentlich zur Verkehrssicherheit beitragen würde.[53] Diese Prävention liegt im Allgemeininteresse.

47 Vgl. *K. Vieweg* Die Auswertung von Fahrzeugdaten bei der Unfallanalyse, in: Deutsche Akademie für Verkehrswissenschaft (Hrsg.), 45. Verkehrsgerichtstag 2007, 2007, S. 292 (294).

48 Vgl. *K. Vieweg* (Fn. 47), S. 292 (294).

49 Vgl. *K. Vieweg* (Fn. 47), S. 292 (294).

50 *F. Zeidler* Die Auswertung von Fahrzeugdaten bei der Unfallanalyse, in: Deutsche Akademie für Verkehrswissenschaft (Hrsg.), 45. Verkehrsgerichtstag 2007, 2007, S. 321. Zu einer möglichen Produkthaftung wegen unterbliebener Speicherung, siehe *P. Salje* Zivilrechtliche Aspekte des Datencontents beim Sacherwerb – Hersteller-Produkthaftung für elektonische Bauteile, in: K. Vieweg/H. Gerhäuser (Hrsg.), Digitale Daten in Geräten und Systemen, 2010, S. 221 (232 ff.).

51 *K. Vieweg* (Fn. 47), S. 292 (296).

52 Vgl. *K. Vieweg* (Fn. 47), S. 292 (296).

53 Vgl. *K. Vieweg* (Fn. 47), S. 292 (297) m.w.N.

Die Frage, wem die gespeicherten digitalen Daten »gehören«, wird erst seit kurzem in der juristischen Fachwelt diskutiert. Die Rechtslage ist alles andere als einfach. Neben dem Bürgerlichen Recht, insbesondere dem Vertragsrecht, ist auch das Urheberrecht und das Datenschutzrecht zu berücksichtigen.

Nach meiner Auffassung liegt die alleinige Auslesebefugnis grundsätzlich beim Kraftfahrzeugeigentümer, der zugleich Inhaber der digitalen Daten ist.[54] Dabei ist jedoch zu beachten, dass – sollten Eigentümer und Fahrer des Fahrzeugs verschieden sein – die Verfügungsbefugnis des Eigentümers durch das Recht auf informationelle Selbstbestimmung, Art. 2 (1) i.V.m. Art. 1 (1) GG, des Fahrers beschränkt sein kann.[55] Konsequenz ist aus datenschutzrechtlicher Sicht gem. § 4 (1) BDSG, dass der Hersteller nur mit Einwilligung des Eigentümers oder bei Vorliegen eines normativen Verarbeitungstatbestandes auf die Daten zugreifen darf.

Die Information des Kunden über die Existenz digitaler Speichermedien sowie über die Möglichkeiten und Grenzen der Auslesung gehört zur kaufvertraglichen Leistungspflicht.[56] Diese Information sollte z.B. in die Betriebsanleitung aufgenommen werden.[57] Als kaufvertragliche Nebenpflicht trifft den Hersteller weiterhin die Pflicht zum Abschluss eines auf Auslesung und Interpretation gerichteten Werkvertrags.[58] Diese ergibt sich aus einem Kontrahierungszwang, sofern nur der Hersteller zur Vornahme der Leistung in der Lage ist.[59] Die Kostenlast der Auslesung trifft dabei den Kunden.[60]

In urheberrechtlicher Hinsicht ließe sich an den Datenbankschutz gem. §§ 87 ff. UrhG denken. Allerdings setzt § 87a (1) S. 1 UrhG eine nach Art und Umfang wesentliche Investition voraus. Zu berücksichtigen sind insofern nur Investitionen für Beschaffung, Überprüfung oder Darstellung der Daten. Da derartige Investitionen erheblichen Umfangs nicht vorliegen, unterfallen Daten in Kraftfahrzeugen nicht dem Schutz der §§ 87 ff. UrhG.[61]

54 Vgl. *K. Vieweg* (Fn. 47), S. 292 (297 f.). Wie hier im Hinblick auf die Verknüpfung von Datenträger und Daten: Larenz/Canaris, Schuldrecht II/2, 13. Aufl. 1994, § 76 II 3b; *J. Hager* in: Staudinger/Eckpfeiler (2012), T. Rn. 223. A.A. *A. Ohly* Digitale Datenbanken aus immaterialgüter- und persönlichkeitsrechtlicher Sicht, in: K. Vieweg/H. Gerhäuser (Hrsg.), Digitale Daten in Geräten und Systemen, 2010, S. 123 (134 f.), der mit dem Hinweis auf die Entkörperlichung von Daten eine Anknüpfung an das Eigentum am Datenträger ablehnt. Kritisch auch *P. Salje* (Fn. 50), S. 224.

55 *K. Vieweg* (Fn. 47), S. 292, (297).

56 *K. Vieweg* (Fn. 47), S. 292, (300); dem folgend *A. Ohly* (Fn. 54), S. 123 (125 f.).

57 *K. Vieweg* (Fn. 47), S. 292, (300).

58 *K. Vieweg* (Fn. 47), S. 292, (301, 302).

59 vgl. *K. Vieweg* (Fn. 47), S. 292, (301); *A. Ohly* (Fn. 614), S. 123 (126 f.); *P. Salje* (Fn. 50), S. 225.

60 *K. Vieweg* (Fn. 47), S. 292, (302).

61 *A. Ohly* (Fn. 54), S. 123 (133 f.).

Die Voraussetzungen einer wirksamen Einwilligung regelt § 4a (1) BDSG. Dessen Satz 3 verlangt grundsätzlich Schriftform i. S. d. § 126 BGB, deren Nichtbeachtung die Formnichtigkeit der Einwilligung zur Folge hat, §§ 125, 126 BGB.[62] Besondere Verarbeitungsumstände können allerdings auch eine andere Form rechtfertigen, § 4a (1) S. 3 BDSG. Derartige Umstände – etwa eine besondere Eilbedürftigkeit auch im Interesse des Betroffenen[63] oder die Neuerhebung von Daten in langjährigen Geschäftsbeziehungen[64] – dürften in aller Regel nicht vorliegen. Eine wirksame Einwilligung in die Datenerhebung und -verarbeitung ist damit normalerweise nicht gegeben. Ein vergleichbarer Fall der Eilbedürftigkeit liegt beim Auslesen von Fahrzeugdaten aber nicht vor. Nur in Ausnahmefällen wird daher eine wirksame Einwilligung in die Datenerhebung und -verarbeitung vorliegen.

Interessant sind in diesem Zusammenhang die Regelungen, die § 6c BDSG für mobile personenbezogene Speicher- und Verbreitungsmedien enthält. Zwar ist der Hauptanwendungsbereich der Vorschrift bei mit Mikroprozesssoren ausgestatteten Chipkarten (sog. Smartcards – z.B. SIM-Karten oder RFID-Chips) zu sehen,[65] jedoch unterfallen auch Speicher in anderen mobilen Geräten, wie etwa Kraftfahrzeugen, dem § 6c BDSG.[66] Dies hat zur Folge, dass gem. § 6c (1) Nr. 2 BDSG die ausgebende Stelle über die Funktion des Mediums einschließlich der Art der personenbezogenen verarbeiteten Daten informieren muss. Die oben bereits bejahte kaufvertragliche Informationspflicht des Herstellers bzw. Händlers lässt sich damit nicht nur kaufvertraglich, sondern auch datenschutzrechtlich herleiten.[67] Daneben muss die ausgebende Stelle aber auch sicherstellen, dass Geräte oder Einrichtungen, die zur Wahrnehmung des Auskunftsrechts aus § 34 BDSG erforderlich sind, in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen, § 6c (2) BDSG. Hinsichtlich der Kostenlast kommt es damit zu Friktionen zwischen der schuldrechtlichen und der datenschutzrechtlichen Ausgestaltung der Rechtsbeziehung zwischen den Parteien.

Hinsichtlich der datenschutzrechtlichen Problematik wäre aus meiner Sicht wünschenswert, wenn der Gesetzgeber Regelungen schaffen würde, die – im Interesse der Verkehrssicherheit und der Prävention – die Auslesung der Daten erlauben, die bei Einbau eines digitalen Unfallrekorders oder von elektronischen Fahrerassistenzsystemen und elektronisch kontrollierten passiven Sicherheitssystemen gewonnen

62 *S. Simitis* in: S. Simitis (Hrsg.), Bundesdatenschutzgesetz, 7. Aufl. 2011, § 4a Rn. 35; *G. Spindler/J. Nink* in: G. Spindler/F. Schuster (Hrsg.), Recht der elektronischen Medien, 2. Aufl. 2011, § 4a Rn. 6; *P. Gola/R. Schomerus* in: P. Gola/R. Schomerus (Hrsg.), Bundesdatenschutzgesetz, 11. Aufl. 2012, § 4a Rn. 19.

63 *S. Simitis* (Fn. 62), § 4a Rn. 45; *B. Holznagel/M. Sonntag*, in: A. Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 4.8 Rn. 29.

64 *S. Simitis* (Fn. 62), § 4a Rn. 46; *B. Holznagel/M. Sonntag* (Fn. 63), 4.8 Rn. 29.

65 Vgl. *S. Simitis* (Fn. 62), § 6a Rn. 5; *P. Gola/R. Schomerus* (Fn. 62), § 6a Rn. 2 ff.

66 *A. Ohly* (Fn. 54), S. 123 (128 f., 130).

67 *A. Ohly* (Fn. 54), S. 123 (130).

werden. Auch müsste geregelt werden, ob die Löschung der Daten zulässig sein soll und welche rechtlichen Wirkungen die Löschung der Daten mit sich bringen soll.

2. Datenschutz

Datenschutz ist auch unter Juristen ein Reizthema. Aktuell sieht man das z.B. an der Vorratsdatenspeicherung. Die Bundesjustizministerin hält die Vorgabe in der betreffenden europäischen Richtlinie, die Vorratsdaten für sechs Monate zu speichern, für unverhältnismäßig und für nicht generell erforderlich.[68] Anders sieht es der Bundesinnenminister.[69] Da Deutschland die Umsetzungsfrist nicht eingehalten hat, hat die Europäische Kommission im Mai 2012 Klage gegen die Bundesrepublik Deutschland eingereicht.[70]

Der 5. Europäische Datenschutztag befasste sich im Januar 2011 mit dem Thema »Verkehrsmobilität und Datenschutz«. Der hessische Datenschutzbeauftragte konstatierte aus diesem Anlass, dass »Automobilität und Datenschutz aus der Spur zu geraten drohen«.[71] Als Problembereiche Mobilen Datenschutzes identifizierte er unter anderem die Videoüberwachung, die Funkortung und die Kennzeichenerfassung (auch das E-Ticketing).

Die europäische Richtlinie 2010/40/EU vom 7. Juli 2010 »Zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr (IVS) und für deren Schnittstellen zu anderen Verkehrsträgern« greift die Datenschutzproblematik auf. In den Erwägungsgründen wird ein »Zielpatchwork« deutlich, wenn es darin wie folgt heißt: »Der Einsatz von Informations- und Kommunikationstechnologien im Straßenverkehrssektor und an dessen Schnittstellen zu anderen Verkehrsträgern wird einen wesentlichen Beitrag zur Verbesserung der Umweltleistung, der Effizienz, einschließlich der Energieeffizienz, der Straßenverkehrssicherheit, auch bei der Beförderung gefährlicher Güter, der öffentlichen Sicherheit sowie der Mobilität

68 Vgl. faz.net vom 27.01.2012, abrufbar unter http://www.faz.net/aktuell/politik/inland/vorratsdatenspeicherung-disput-zwischen-den-ministerien-11627230.html (abgerufen am 10.08.2012).

69 Vgl. SPON vom 16.04.2012, abrufbar unter http://www.spiegel.de/politik/deutschland/friedrich-lehnt-leutheusser-entwurf-zur-vorratsdatenspeicherung-ab-a-827939.html (abgerufen am 10.08.2012).

70 Faz.net am 31.05.2012, abrufbar unter http://www.faz.net/aktuell/politik/europaeische-union/vorratsdatenspeicherung-bruessel-verklagt-deutschland-auf-300-000-euro-taeglich-11769781.html (abgerufen am 10.08.2012); SPON am 31.05.2012 http://www.spiegel.de/politik/deutschland/vorratsdatenspeicherung-eu-kommission-verklagt-deutschland-a-836221.html (abgerufen am 10.08.2012).

71 *M. Ronellenfitsch* Mobilität unter Aufsicht – Freie Fahrt und jeder weiß wohin, 2011, S. 3, abrufbar unter http://www.datenschutz.hessen.de/download.php?download_ID=227&download_now=1 (abgerufen am 01.08.2012).

von Personen und Gütern leisten und gleichzeitig das Funktionieren des Binnenmarkts gewährleisten sowie für eine Zunahme der Wettbewerbsfähigkeit und der Beschäftigung sorgen.«[72] Hinsichtlich des Datenschutzes verweist die Richtlinie auf die Datenschutz-Richtlinie von 1995 und regt an, den Rat der sog. Art.-29-Gruppe der europäischen Datenschutzbeauftragten einzuholen.

Die in Art. 10 der Richtlinie erwähnten Vorschriften über Vertraulichkeit, Sicherheit und Weiterverwendung von Informationen sind sehr allgemein gehalten. So heißt es z.B. in Art.10 Abs. 3: »… wird zum Schutz der Privatsphäre, soweit angemessen, die Verwendung anonymer Daten für den Betrieb von IVS-Anwendungen und -Diensten gefördert.«

Wohin die Datenschutzreise geht, ist schwer zu sagen. Immer ist das Verhältnis kollidierender Grundrechte nach dem Grundsatz der praktischen Konkordanz[73] auszutarieren. Damit kommen Verhältnismäßigkeitsüberlegungen ins Spiel. Auch stellt sich die Frage nach einem datenschutzrechtlichen Mindeststandard. Insofern sind aktuelle europäische Entwicklungen in den Blick zu nehmen Dem Urteil des Europäischen Gerichtshofs vom 24. November 2011[74] zufolge ist das Verhältnis des deutschen zum europäischen Datenschutzrecht neu auszuloten. Bisher war die wohl herrschende Meinung in Deutschland, dass die europäischen Richtlinien lediglich datenschutzrechtliche Mindeststandards vorgeben und das deutsche Datenschutzrecht ein höheres Niveau verlangen konnte.[75] Der EuGH sieht das anders. Er sieht die Richtlinien als Beitrag zur Vollharmonisierung, der nicht durch nationale Vorschriften überboten werden dürfe.[76] Damit kommt der europäischen Entwicklung, insbesondere dem Vorschlag der Kommission für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung),[77] eine besondere Bedeutung zu.

72 Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 07.07.2010, ABl. EU 2010 Nr. L 207/1, Erwägungsgrund 4.

73 *K. Hesse* Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, Neudruck der 20. Aufl. 1999, S. 28 Rn. 72 (S. 142 Rn. 317 f.); BVerfGE 28, 243 (260 f.);. 32, 98 (107 f.); 93, 1 (21).

74 EuGH, Urt. v. 24.11.2011 – C-468, 469/10 = EuGH NZA 2011, 1409 = EuGH EuZW 2012, 37.

75 So etwa *M.-T. Tinnefeld/E. Ehmann/R.W. Gerling* Einführung in das Datenschutzrecht, 4. Aufl. 2005, S. 123; *S. Simitis* (Fn. 62), Einl. Rn. 230; *J. Taeger/B. Schmidt* in: J. Taeger/D. Gabel (Hrsg.), Kommentar zum BDSG, 2010, Einf. Rn. 35.

76 EuGH EuZW 2012, 37 Tz. 24 ff.

77 Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) KOM (2012) 11 endgültig (2012/0011).

Die Datenschutzproblematik hat nicht nur eine europäische, sondern auch eine globale Bedeutung. Die International Working Group on Data Protection in Telecommunication hat im April 2011 nach ihrer Sitzung in Montreal ein kluges Arbeitspapier[78] erstellt. Mit der Forderung »Privacy by Design« – also der Einbeziehung des Datenschutzes und des Schutzes der Privatsphäre von vornherein in die Gesamtkonzeption – liegt sie meines Erachtens richtig. Auf das für Juristen bestehende Dilemma habe ich anfangs hingewiesen.

VIII. ZUSAMMENFASSUNG UND AUSBLICK

1. Juristen finden sich in einer zweckmäßigerweise interdisziplinär geführten Diskussion in einer ambivalenten Rolle, wenn es darum geht, etwaige Rechtsprobleme vorsorglich anzusprechen. Dies gilt insbesondere für Fragen der technischen Sicherheit im digitalen Zeitalter.
2. Die interdisziplinäre Zusammenarbeit sollte wechselseitig die Entwicklungen in den Blick nehmen, um das nötige Problembewusstsein und Verständnis zu schaffen. In technischer Hinsicht sind als Entwicklungstendenzen insbesondere die Digitalisierung und die Miniaturisierung, in juristischer Hinsicht vor allem die Zunahme europäischer Vorgaben zu berücksichtigen.
3. Begriffliche Klarheit trägt dazu bei, die zwangsläufig vorhandenen Zielkonflikte methodisch an der richtigen Stelle zu lösen. Für die notwendige Kommunikation zwischen Technik und Recht erweist sich die technische Normung als wertvolle Verständnisbrücke.
4. Wichtig ist, dass die zur Lösung technischer Aufgaben verwendeten Sicherheitskonzepte transparent gemacht werden. Das trägt in der interdisziplinären Diskussion zum Verständnis bei. Die Differenzierung in Sicherheitsanforderungsstufen (SIL, ASIL) ist hilfreich. Die alternativen Sicherheitskonzepte (z.B. ALARP) sollten angesichts der europäischen Entwicklung im Blick bleiben.
5. Innovationen zur Förderung der Straßenverkehrssicherheit, insbesondere Automatisierungs- und Assistenzsysteme, führen zu einem Spannungsfeld von Technik, Recht, Ökonomie und Ökologie. Es ergeben sich zahlreiche Rechtsfragen wie die nach der Zugriffsbefugnis auf digitale Daten und den Datenschutz.
6. Die Zugriffsbefugnis auf digitale Daten in den »rollenden Computern Kraftfahrzeuge« ist juristisch noch nicht hinreichend geklärt. Neben vertragsrechtlichen Fragen ist vor allem das Datenschutzrecht zu beachten. Der Gesetzgeber muss sich m. E. mit den Problemen befassen. Dazu gehören:

78 International Working Group on Data Protection in Telecommunication, Arbeitspapier – Datenaufzeichnung in Fahrzeugen (Event Data Recording – EDR): Fragestellungen zu Datenschutz und zum Schutz der Privatsphäre für Regierungen und Hersteller, 49. Sitzung, 04.-05.04.2011 in Montreal (abrufbar unter http://www.datenschutz-berlin.de/attachments/844/675.42.20.pdf?1322224432 (abgerufen 03.08.2012).

- Klärung des Verhältnisses von Fahrerassistenz und Fahrerverantwortlichkeit unter Berücksichtigung der Wiener Konvention, der zufolge die Entscheidung beim Fahrer bleiben muss;
- die Speicherung der digitalen Daten (auch zur Dokumentation bei Unfällen, damit nicht wechselseitig der »schwarze Peter« zugeschoben wird);
- die endgültige Klärung des Verhältnisses von deutschem und europäischem Datenschutzrecht.