GERRIT HORNUNG

Datenschutz durch Technik in Europa

Die Reform der Richtlinie als Chance für ein modernes Datenschutzrecht

Datenschutzfreundliche Technik (PET)
Privacy by Design/Privacy by Default
Effektive Datensicherheit
Gütesiegel und Audit
Selbstbestimmung

■ Sowohl in Deutschland als auch auf der europäischen Ebene werden derzeit intensive Diskussionen um die Reform des Datenschutzrechts geführt. Durch den Vorrang des Europarechts kommt der Überarbeitung der EU-Datenschutzrichtlinie (DS-RL) besondere Bedeutung zu. Dies wird durch die bisher sehr langen Reformzyklen verstärkt: Regelungen, die es nicht in die aktuelle Reform schaffen, könnten 15 bis 20 Jahre auf die nächste Chance warten müssen. Umso wichtiger ist es, die seit langem diskutierten Möglichkeiten eines rechtlich gesteuerten Datenschutzes durch Technik – also verbindliche Vorgaben für Hersteller und Anwender – an prominenter Stelle in die neuen europäischen Regelungen zu übernehmen.

■ Both in Germany and also on the European level there are currently intensive discussions regarding the reform of data protection law. Due to the primacy of European law, the revision of EU Data Protection Guidelines (DS-RL) are of particular importance. This is enhanced by the hitherto very long reform cycles: regulations which are not included in the current reform may have to wait 15 to 20 years for the next reform. Thus, it is all the more important to include – at a prominent position in the new European regulations – the long discussed possibility of legally controlled data protection through technology, i.e. binding requirements for producers and users.

I. Einführung

Nach Jahren der Stagnation hat die Reform des Datenschutzrechts in mehrfacher Hinsicht neuen Schwung gewonnen. In Deutschland wurden nach den sog. Datenschutzskandalen des Jahres 2008 mehrere Änderungen des Datenschutzrechts vorgenommen.[1] Überdies hat das Positionspapier der *Konferenz der Datenschutzbeauftragten des Bundes und der Länder*[2] einen neuen Impuls in der mehr als zehnjährigen Diskussion um grundlegende Reformen des Datenschutzrechts[3] gegeben.

Dieses Papier enthält wichtige Ideen und Vorschläge zur Überarbeitung des geltenden Rechtsrahmens in Deutschland, u.a. auch zu den Möglichkeiten eines technikgestützten Datenschutzes.[4] Es äußert sich jedoch weder insoweit noch an anderer Stelle zu den europarechtlichen Vorgaben und Grenzen einer nationalen Modernisierung des Datenschutzrechts – angesichts der in Teilen durchaus detaillierten Regelungen der DS-RL v. 24.10.1995[5] ein bemerkenswertes Unterlassen. Im November 2010 hat nunmehr die *EU-Kommission* die Initiative ergriffen und eine Mitteilung zu einem „Gesamtkonzept für den Datenschutz in der Europäischen Union" veröffentlicht.[6] Es steht zu erwarten, dass die auf dieser Basis angestrebte europäische Reform das Datenschutzrecht in Europa in den nächsten Jahren maßgeblich beeinflussen wird.

Vor diesem Hintergrund ist es von großer Bedeutung, dass diese Reform wichtige Erkenntnisse aus der Praxis und wissenschaftlichen Bearbeitung des Datenschutzrechts aufnimmt, die vor 15 Jahren noch nicht verfügbar waren. Ein zentraler Bereich ist dabei das Konzept eines Datenschutzes durch Technik, das große Chancen für den Datenschutz bietet, in der Mitteilung der *Kommission* aber deutlich zu kurz kommt.

II. Konzept: Datenschutz durch Technik

Die Grundidee eines technikgestützten Datenschutzes wird seit vielen Jahren diskutiert: Wenn Datenschutzgefahren und -verletzungen faktisch nicht möglich sind, müssen sie nicht rechtlich verboten werden. Recht und Technik erscheinen hier in einem Verhältnis gegenseitiger Ergänzung; sie bilden eine „Allianz"[7] zum Schutz der Persönlichkeitsrechte. Klassische Regelungsinstrumente enthalten Ge- und Verbote, ihre Sanktionsinstrumente denken den Verstoßfall immer schon mit. Da sie in ihrer hergebrachten Form an nationalstaatliche Vollzugsapparate gebunden sind, verlieren sie im „körperlosen Sozialraum"[8] des Internet an Effektivität.

Ein effektiver Datenschutz setzt unter diesen Bedingungen die Verfügbarkeit datenschutzfreundlicher Technik (Privacy Enhancing Technologies, PET)[9] voraus. Dies wird in Zukunft unter den Bedingungen allgegenwärtiger Datenverarbeitung noch wichtiger werden. In Anwendungsszenarien des Ubiquitous Comput-

1 Dazu *Eckhardt*, DuD 2009, 587; *Gola/Klug*, Sonderbeilage RDV 4/2009; *Roßnagel*, NJW 2009, 2716; *Scheuring*, NVwZ 2010, 809; *Kühling/Bohnen*, JZ 2010, 600.
2 *Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, Ein modernes Datenschutzrecht für das 21. Jahrhundert, 2010.
3 S. v.a. *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001; ferner z.B. *Ahrend u.a.*, DuD 2003, 433; *Bizer*, DuD 2001, 274; *ders.*, DuD 2004, 6; *Roßnagel*, MMR 2005, 71; 32. Sitzung des *BT-Innenausschusses* am 5.3.2007, Protokoll 16/32; BT-Drs. 16/4882.
4 *Konferenz der Datenschutzbeauftragten des Bundes und der Länder* (o. Fußn. 2), 7 f., 9 f., 18 ff.
5 RL 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG Nr. L 281 v. 23.11.1995, S. 31.
6 Mitt. der *Kommission* v. 4.11.2010, Gesamtkonzept für den Datenschutz in der EU, KOM(2010) 609 endg.; vgl. auch *Reding*, ZD 2011, 1.
7 *Roßnagel* (Hrsg.), Allianz von Medienrecht und Informationstechnik, 2001.
8 S. *Roßnagel*, ZRP 1997, 26 ff.
9 Zu diesem Konzept *Borking*, DuD 1998, 636; *ders.*, DuD 2001, 607; *Hansen*, in: Roßnagel (Hrsg.), Hdb. Datenschutzrecht, 2003, Kap. 3.3; s.a. *Scholz*, Datenschutz beim Internet-Einkauf, 2003, S. 357 ff. m.w.Nw. sowie die Beiträge in *Roßnagel* (o. Fußn. 7); zu den ökonomischen Chancen *London Economics*, Study on the economic benefits of privacy enhancing technologies, Juli 2010, abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf.

ing[10] erscheint es illusorisch, informationelle Selbstbestimmung ohne Technologien zu gewährleisten, die grundsätzlich nutzergesteuert, im Alltag aber im Hintergrund für Anonymität, Pseudonymität und Transparenz sorgen oder diese unterstützen. Konzepte für derartige Technologien bestehen schon heute:[11] Diese können Default-Einstellungen (z.B. für Einwilligungen nach dem Opt-in Prinzip) vorgeben, personalisierte Nutzereinstellungen für routinemäßige Datenverarbeitungen vorsehen, automatisierte Löschungsroutinen umsetzen, ein persönliches Identitätsmanagement unterstützen oder Einwilligungen übermitteln, organisieren und dokumentieren, die der Betroffene für eine Gruppe von Datenverarbeitungsvorgängen erteilt hat.

Darüber hinaus ist es möglich, über technikgestützte Verarbeitungsregeln dem Vorsorgeprinzip zu mehr Gewicht im Datenschutz zu verhelfen.[12] Dies wird in Zukunft immer wichtiger werden, weil durch die enorme Steigerung der verarbeiteten Daten das Risiko immer größer wird, dass Daten personenbeziehbar werden, bei denen dies anfänglich nicht der Fall ist.[13] Das führt im gegenwärtigen Datenschutzrecht zu Problemen, weil dieses die Daten anfänglich nicht erfasst (§ 1 Abs. 2 i.V.m. § 3 Abs. 1 BDSG) und für den Moment des Eintretens einer Personenbeziehbarkeit weder Anforderungen noch Rechtsfolgen normiert. Wenn man davon ausgeht, dass die weitere Speicherung oder sonstige Verarbeitung und Nutzung in diesem Moment rechtswidrig werden,[14] verbleibt immer noch das gravierende Problem, dass dies für verantwortliche Stellen häufig nur schwer erkennbar sein wird. Technische Instrumente können hier dabei helfen, auch „noch nicht" personenbeziehbare Daten ganz zu vermeiden oder Verarbeitungsregeln zu unterwerfen.

III. Adressaten des Konzepts

Datenschutz durch Technik kann nur erfolgreich sein, wenn datenschutzfreundliche Technik zum einen verfügbar ist, sie zum anderen auch tatsächlich praktisch eingesetzt wird. Diese Voraussetzungen sind komplementär: Die Konzeption, Erforschung und Entwicklung von Privacy Enhancing Technologies bleibt ohne Einfluss auf den Schutz von Persönlichkeitsrechten, wenn diese Technologien nicht in nennenswertem Umfang genutzt werden – sei es, dass sie zu wenig bekannt, zu schwer zu handhaben oder zu teuer sind, sei es, weil marktmächtige Akteure ihre Verbreitung verhindern. Umgekehrt nützt die größte Bereitschaft der Akteure des Rechts- und Geschäftsverkehrs zum Einsatz dieser Technologien nichts, wenn es an der Grundlagenforschung und praktischen Implementierung fehlt.

Aus dieser Erkenntnis folgt, dass ein Konzept eines Datenschutzes durch Technik zwei Adressaten haben muss:

- Hersteller (für die faktische Verfügbarkeit der Technik) und
- Anwender (für den tatsächlichen Einsatz).

Beide Adressaten benötigen dabei Kriterien für die Entwicklung und den Einsatz von Technik. An dieser Stelle kommt das Recht ins Spiel und gewinnt eine besondere Bedeutung: Aus ihm lassen sich zukunftsorientiert Kriterien für die Gestaltung von Technik gewinnen.[15] Gleichzeitig bietet das Recht auch Möglichkeiten, Vorgaben und Anreize für den Einsatz von Technik zu setzen.

Die Erfahrung lehrt, dass datenschutzfreundliche Technik nicht allein durch Marktmechanismen entsteht und sich verbreitet. Das hat vielfältige Gründe: Technik wird häufig maßgeblich nach funktionalen Anforderungen konstruiert, Datenschutzfreundlichkeit ist jedoch eine nicht-funktionale Anforderung. Das intrinsische Ziel von Herstellern und Anwendern liegt – legitimerweise – in der Gewinnmaximierung. Hier kann Datenschutz relevant werden, wenn eine entsprechende Nachfrage am Markt besteht. Umgekehrt wird er jedoch schnell zum reinen Kostentreiber, wenn diese Nachfrage fehlt, oder er spielt im Gestaltungsprozess keine Rolle, weil er weder Kosten verursacht noch einspart.

Gegenüber Herstellern muss deshalb der Gedanke der Produktverantwortung stark gemacht werden. Hier kann das Recht auf verschiedene Art und Weise wirksam werden: Erstens durch das Setzen extrinsischer Anreize, also Ge- und Verbote oder Haftungsregeln; zweitens durch eine Beeinflussung intrinsischer Ziele, also eine Stimulation des Markts für datenschutzfreundliche Technologien mittels Audits oder Gütesiegeln;[16] drittens durch die Mitwirkung von Rechtswissenschaftlern an interdisziplinärer Forschung, die Methoden für die datenschutzfreundliche Gestaltung neuer Technologien entwickelt.[17] Hier können auch Förderinstitutionen Einfluss nehmen, wenn sie bei der Entscheidung über die Vergabe von Drittmitteln berücksichtigen oder sogar verlangen, dass bei der Erforschung neuer Informationstechnologien datenschutzrechtliche Fragen mit bearbeitet werden.[18]

Die zweite Ebene der Umsetzung ist vielleicht ein noch größeres Problem. Denn vielfach sind datenschutzfreundliche Technologien tatsächlich verfügbar. Dazu trägt sicher auch die intrinsische Motivation von Wissenschaftlern aus dem Bereich der technischen Forschung bei, die z.B. Konzepte und Lösungen für einzelne Komponenten entwickeln: Verschlüsselungs- und Signaturverfahren, Systeme zur Anonymisierung und Pseudonymisierung, Methoden für ein selbstgesteuertes Identitätsmanagement, die Möglichkeit datenschutzfreundlicher Default-Einstellungen oder anonyme Bezahlverfahren. Daneben bestehen auch Konzepte für ganze Anwendungen wie Location Based Services.[19] Offenbar gibt es in der Praxis der Anwender aber deutliche Hemmnisse, die verfügbaren Technologien auch einzusetzen. Auch hier kann das Recht mit den beschriebenen Anreizsystemen Einfluss nehmen. Hinzu treten weitere Instrumente, die speziell für den Bereich der Anwender greifen können. Ein Beispiel ist die Normierung von Transparenzpflichten bei sog. „Datenpannen" (§§ 42a BDSG, 15a TMG, 93 Abs. 3 TKG), die die Anwender zum Einsatz effektiver Datensicherheitsmaßnahmen anhalten sollen.[20]

Perspektivisch werden derartige Mechanismen nur wirksam sein, wenn sie im europäischen, besser noch im globalen Maßstab eingesetzt werden. Betrachtet man die bisherige techni-

10 Zu diesen Visionen z.B. die Beiträge in *Fleisch/Mattern* (Hrsg.), Internet der Dinge, 2005; *Mattern* (Hrsg.), Die Informatisierung des Alltags, 2007; *Roßnagel/Sommerlatte/Winand* (Hrsg.), Digitale Visionen, 2008.

11 S. ausf. *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007; s.a. *Kühling*, Die Verwaltung 40/2007, S. 152 ff.; *Hornung*, in: Hempel/Krasmann/Bröckling (Hrsg.), Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert, Leviathan Sonderheft 25/2010, S. 245 ff.

12 *Roßnagel*, in: Eifert/Hoffmann-Riem (Hrsg.), Innovation, Recht und öffentliche Kommunikation, 2011, S. 43 ff.

13 S. *Roßnagel/Scholz*, MMR 2010, 721, 728 ff.; *Roßnagel* (o. Fußn. 11), S. 185 ff.

14 *Roßnagel/Scholz*, MMR 2010, 721, 730.

15 Grundlegend zur Techniksteuerung durch Recht *Roßnagel*, Rechtswissenschaftliche Technikfolgenforschung. Umrisse einer Forschungsdisziplin, 1993; zur Umsetzung im Datenschutz *ders.* (o. Fußn. 12), S. 54 ff.

16 Dazu *Roßnagel*, DuD 1997, 505; *ders.*, Datenschutzaudit. Konzeption, Durchführung, gesetzliche Regelung, 2000; *ders.*, in: ders. (o. Fußn. 9), Kap. 3.7; *ders.*, in: Hempel/Krasmann/Bröckling (o. Fußn. 11), S. 263; *Bäumler*, CR 2001, 795; *ders.*, DuD 2002, 325; *ders.*, DuD 2004, 80; zu praktischen Beispielen s.u. IV.

17 S. als aktuelles Beispiel das Projekt „Gestaltung technisch-sozialer Vernetzung in situativen ubiquitären Systemen (VENUS)", abrufbar unter: http://www.uni-kassel.de/einrichtungen/iteg/venus.

18 S. z.B. *Europäischer Datenschutzbeauftragter*, Der EDSB und Forschung und technologische Entwicklung in der EU, v. 28.4.2008, abrufbar unter: http://www.edps.europa.eu/.

19 S. aus rechtlicher Sicht *Ranke*, M-Commerce und seine rechtsadäquate Gestaltung, 2004; *Jandt*, Vertrauen im Mobile Commerce, 2008; *Schnabel*, Datenschutz bei profilbasierten Location Based Services, 2009.

20 Dazu *Gabel*, BB 2009, 2045; *Eckhardt/Schmitz*, DuD 2010, 390; *Hanloser*, MMR 2010, 300; *Hornung*, NJW 2010, 1841.

sche Entwicklung insbesondere des Internet, so kann man den Eindruck gewinnen, dass Unternehmen wie *Apple*, *Google* oder *Facebook* die maßgeblichen Akteure bei der Formulierung von Standards für die Verarbeitung personenbezogener Daten sind. Das gilt auch für neue Anwendungen wie das Cloud Computing: Hier setzen Anbieter wie *Amazon* und *Google* technische Standards, deren datenschutzrechtliche Probleme erst in Ansätzen erfasst sind, jedenfalls aber kaum dazu führen werden, dass Infrastrukturentscheidungen nachträglich revidiert werden. Dies birgt die Gefahr, dass weltweit agierende Konzerne faktische Regeln setzen, so wie dies historisch im Fall der lex mercatoria, also dem im Mittelalter entstandenen Gewohnheitsrecht der Handelsleute, der Fall war.[21] Perspektivisch könnte ein derartiges Gewohnheitsrecht des virtuellen Raums, eine Art lex mercatoria digitalis, wichtiger sein als nationale Bestrebungen – schlicht und einfach deswegen, weil sich (regelmäßig US-amerikanische) Marktmacht mit hunderten von Millionen Nutzern selbst ihre Regeln gibt. Will man dem entgegensteuern, so ist es erforderlich, den Einsatz datenschutzfreundlicher Technik als soziotechnisches System zu begreifen und eine akteurszentrierte Perspektive einzunehmen: Es geht dann nicht so sehr um Vorgaben für das Ergebnis, also die Gestaltung einer konkreten Technik (von der man regelmäßig im Voraus ohnehin noch nicht sagen kann, wie sie aussehen wird oder soll), sondern um Vorgaben und Anreize für das Verhalten von Akteuren und die Organisation von Prozessen.

IV. Regelungsinstrumente: Status quo

Betrachtet man Regelungsinstrumente für einen Datenschutz durch Technik de lege lata, so ist es vor diesem Hintergrund sinnvoll, zwischen materiellen Anforderungen an die Technik selbst und verfahrenstechnischen Anforderungen an den Prozess der Technikentwicklung und Technikanwendung zu unterscheiden. Beides lässt sich sowohl für die deutsche als auch für die europäische Ebene durchführen.

Im deutschen Datenschutzrecht gibt es seit 1997 Normen, die mit den Grundsätzen der Datenvermeidung und Datensparsamkeit Regelungen für die Auswahl und Gestaltung von Datenverarbeitungssystemen enthalten. Zunächst bereichsspezifisch für Tele- und Mediendienste durch die wortgleichen § 3 Abs. 4 TDDSG 1997 und § 12 Abs. 5 MDStV 1997 eingeführt,[22] wurde im Zuge der Novellierung 2001 mit § 3a BDSG eine Norm im allgemeinen Datenschutzrecht geschaffen,[23]die 2009 um Vorgaben für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten erweitert wurde.[24] § 3a BDSG erfasst damit seit der letzten Novelle zwei Akteure und drei Schritte: Die Vorschrift richtet sich an Hersteller (Gestaltung der Systeme) und Anwender (Auswahl und Einsatz) und verlangt, diese drei Schritte an dem Ziel „auszurichten", so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind diese zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert. Letzteres Kriterium wurde 2009 verschärft; bis dahin musste der Aufwand „in einem angemessenen Verhältnis" stehen.

§ 3a BDSG wird in datenschutzrechtlichen Diskussionen häufig als unterstützendes Argument eingesetzt, wenn es um die Begründung von Verhaltenspflichten für verantwortliche Stellen geht. Das gilt sowohl für die Praxis der Datenschutzbehörden als auch für wissenschaftliche Veröffentlichungen. In Letzteren ist daneben die Frage erörtert worden, ob es sich bei der Norm um eine echte Rechtspflicht handelt.[25] Richtigerweise ist dies insofern der Fall, als die Norm verbindlich („sind") einen Korridor („auszurichten") für Gestaltung, Auswahl und Einsatz der Technik vorgibt. Letztlich ist die rechtliche Wirksamkeit der Vorschrift aber dadurch behindert, dass ihre Verletzung weder zur Unzulässigkeit der resultierenden Datenverarbeitungsvorgänge führt, noch andere Rechtsfolgen wie Ansprüche der Betroffenen, Zulässigkeit von Aufsichtsmaßnahmen oder Verwirklichung von Ordnungswidrigkeiten nach sich zieht. Es handelt sich damit weithin um „soft law". Die praktische Wirksamkeit von § 3a BDSG ist denn auch, soweit ersichtlich, bislang nicht empirisch erforscht worden.[26]

Auf der verfahrenstechnischen Seite – die die Umsetzung der Norm befördern könnte – fehlen in Deutschland weithin rechtliche Vorgaben. Die seit 1997 durch § 17 MDStV und seit 2001 durch § 9a Satz 2 BDSG angekündigte Verabschiedung eines Gesetzes über ein Datenschutzaudit ist zuletzt i.R.d. kleinen Novellen 2009 gescheitert, nachdem die Referentenentwürfe auf einhellige Kritik in der Fachwelt gestoßen waren.[27] Demgegenüber gibt es in Deutschland auch Erfolgsbeispiele: In Schleswig-Holstein vergibt das *Unabhängige Landeszentrum für Datenschutz* (*ULD*) auf Basis der schleswig-holsteinischen Datenschutzauditverordnung[28] ein Gütesiegel für IT-Produkte, deren Datenschutzkonformität durch anerkannte Sachverständige bestätigt wird. Die Möglichkeit hat inzwischen eine Reihe von Herstellern sehr unterschiedlicher Produkte wahrgenommen.[29] Dazu trägt sicher bei, dass gem. § 4 Abs. 2 Satz 1 LDSG SH in der Landesverwaltung vorrangig Produkte eingesetzt werden sollen, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in dem Verfahren nach der Datenschutzauditverordnung festgestellt wurde. Eine solche Regelung besteht auch in § 4 Abs. 2 Satz 2 LDSG NRW, ohne dass dort jedoch ein Audit im Landesrecht geregelt wäre. Ein weiteres, weniger erfolgreiches Beispiel gibt es sonst nur in Bremen.[30] 2007 und 2008 wurde die Auditierung durch das *ULD* und mehrere europäische Partner als „European Privacy Seal (EuroPriSe)" auf die EU ausgeweitet.[31]

Jenseits dieses Projekts, das durch die *Europäische Kommission* gefördert wird, gibt es auf europäischer Ebene weder verfahrenstechnische noch materielle Regelungen zu einem Daten-

21 S. zu diesem Gedanken näher *Hornung*, Regelungsinstrumente im virtuellen Raum, Vortragsmanuskript zur Sommerakademie 2010 des *Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein* (*ULD*): „Codex digitalis. Optimierter Persönlichkeitsschutz – digital und vernetzt", abrufbar unter: https://www.datenschutzzentrum.de/sommerakademie/2010/.

22 Grundlage war ein Entwurf von *provet*, Vorschläge zur Regelung von Datenschutz und Rechtssicherheit in Online-Multimedia-Anwendungen, Gutachten im Auftrag des BMBF, 1996, abrufbar unter: www.provet.org/bib/mmge.

23 Zu Entwicklung und Konzept s. *Roßnagel* (o. Fußn. 12), S. 42 ff., 49 ff.; *Scholz*, in: Simitis, BDSG, 7. Aufl. 2011, § 3a Rdnr. 1 ff.; krit. z.B. *Albers*, Informationelle Selbstbestimmung, 2005, S. 554; *Bull*, NJW 2006, 1617. Die meisten Landesdatenschutzgesetze enthalten vergleichbare Regelungen.

24 Gesetz zur Änderung datenschutzrechtlicher Vorschriften v. 14.8.2009, BGBl. I, S. 2814.

25 Dafür *Bäumler*, DuD 1999, 258, 260 (zu § 3 Abs. 4 TDDSG); *Dix*, in: Roßnagel (o. Fußn. 9), Kap. 3.5 Rdnr. 23 (zu § 3 Abs. 4 TDDSG und § 12 Abs. 5 MDStV); *Bizer*, in: Simitis, BDSG, 6. Aufl. 2006, § 3a Rdnr. 41; *Scholz* (o. Fußn. 23), § 3a Rdnr. 27 f.; a.A. *Wuermeling*, DSB 7+8/1997, 6, 8 (zu § 3 Abs. 4 TDDSG 1997: Zielvorgabe); *Gola/Schomerus*, § 3a Rdnr. 2 und *Schaffland/Wiltfang*, BDSG, § 3a Rdnr. 2: Programmsatz.

26 Zu den marktwirtschaftlichen Chancen von PETs s. *London Economics* (o. Fußn. 9).

27 S. den Entwurf v. 7.9.2007 und den überarbeiteten Entwurf v. 29.10.2007; zur Kritik an den Entwürfen *Roßnagel*, in: Hempel/Krasmann/Bröckling (o. Fußn. 11), S. 274 ff.

28 Landesverordnung über ein Datenschutzaudit v. 18.11.2009, GVOBl. 2008, S. 562; 2009, S. 742 (Basis ist § 4 Abs. 2 LDSG SH); s.a. *Bäumler*, DuD 2002, 325; *ders.*, DuD 2004, 80; *Schläger*, DuD 2004, 459.

29 Die Liste der vergebenen Gütesiegel, weitere Informationen und Berichte zu praktischen Erfahrungen sind abrufbar unter: https://www.datenschutzzentrum.de/guetesiegel/index.htm.

30 Basis ist die Bremische Datenschutzauditverordnung (BremDSAuditV) v. 15.10.2004, Brem.GBl., S. 515; s. *Holst*, DuD 2004, 710.

31 S. *Meissner*, DuD 2008, 525 und http://www.european-privacy.seal.eu.

schutz durch Technik. Man kann zwar § 3a BDSG zu Bestimmungen der DS-RL in Bezug setzen, etwa dem Prinzip der Erforderlichkeit (Art. 6 Abs. 1 lit. c DS-RL).[32] Die Zielrichtung der Regelung geht aber darüber hinaus, weil sie eine Präferenzregel für die Gestaltung und Auswahl von Datenverarbeitungssystemen darstellt und von der verantwortlichen Stelle sogar verlangt, ihre Verarbeitungszwecke i.S.e. – optimierten – „datensparsamen" Konkretisierung zu überdenken.[33] Sowohl die materiellen Vorgaben in § 3a BDSG als auch die Verfahrensregeln in Schleswig-Holstein und Bremen wurden also auf der mitgliedstaatlichen Ebene entwickelt; darauf ist bei der Frage der künftigen europäischen Regulierungsdichte zurückzukommen.

V. Novellierung der Richtlinie

Der aktuelle Prozess der Überarbeitung der DS-RL bietet die Chance, auch auf europäischer Ebene Regelungen für einen Datenschutz durch Technik vorzusehen. Hierzu gibt es entsprechende Äußerungen der *Kommission* (V.1.), die aber erheblich weiter ausgebaut werden müssen (V.2.). Schließlich lassen sich aus den nationalen Erfahrungen mit dem Konzept des Datenschutzes durch Technik auch Schlussfolgerungen für die künftige Regulierungsstrategie der Union ableiten (V.3.).

1. Äußerungen der Kommission

In der Mitteilung der *Kommission* v. 4.11.2010 wird die Bedeutung des Datenschutzes durch Technik an mehreren Stellen betont. So heißt es u.a., Technologien zum Schutz der Privatsphäre, für deren Förderung sich die *Kommission* bereits 2007 in einer Mitteilung ausgesprochen habe,[34] sowie die Anwendung des Konzepts „Privacy by Design" könnten für die Datensicherheit und die mögliche Einführung des Rechenschaftsgrundsatzes („accountability")[35] eine wichtige Rolle spielen.[36] So zutreffend dies ist, so undeutlich bleiben die Folgerungen: Als i.R.d. weiteren Novellierungsprozesses zu prüfende Maßnahme wird lediglich die „weitere Förderung von Technologien zum Schutz der Privatsphäre und der Möglichkeiten für die konkrete Umsetzung des Privacy-by-Design-Konzepts" genannt.[37] Diese Formulierung klingt nach einer Fortsetzung der Aktivitäten der *Kommission* im Bereich der Forschungsförderung. So wichtig diese ist, so wenig kann sie rechtlich geregelte Pflichten für Hersteller und Anwender ersetzen. Die Mitteilung bleibt an dieser Stelle noch hinter dem „Korridor" zurück, den § 3a BDSG vorgibt.[38]

An anderer Stelle heißt es, die *Kommission* werde „sondieren, ob EU-Zertifizierungsregelungen (z.B. Datenschutzsiegel) für Verfahren, Technologien, Produkte und Dienste, die hinsichtlich des Datenschutzes unbedenklich sind, eingeführt werden sollten".[39] Dies diene nicht nur den Nutzern dieser Technologien, Produkte und Dienste, sondern sei auch eine Möglichkeit für verantwortliche Stellen, die Einhaltung datenschutzrechtlicher Pflichten nachzuweisen. Die Absicht der *Kommission* liest sich konkreter als im Beispiel davor, auch wenn der Inhalt und insbesondere die Maßstäbe einer Zertifizierung (was genau bedeutet „unbedenklich"?)[40] noch offen sind. Auffällig ist jedenfalls, dass die *Kommission* beide Punkte, an denen der Datenschutz durch Technik erwähnt wird, nicht unter dem Gliederungspunkt der „Stärkung der Rechte des Einzelnen", sondern unter dem der „Stärkung der Binnenmarktdimension" eingeordnet hat.[41] Was dies für den weiteren Prozess der Novellierung bedeutet, muss abgewartet werden. Es ist jedenfalls zu hoffen, dass das Konzept des Datenschutzes durch Technik nicht vorrangig unter dem Gesichtspunkt der Harmonisierung wirtschaftlicher Rahmenbedingungen diskutiert werden wird. So unverzichtbar dies in bestimmten Bereichen ist – rein national ausgerichtete und anerkannte Gütesiegel sind im gemeinsamen Markt nicht sinnvoll –, so wenig würde es dem Grundansatz des Konzepts gerecht, die Betroffenen durch technische Mittel beim selbstbestimmten Umgang mit ihren personenbezogenen Daten zu unterstützen.

Die Formulierung, entsprechende Maßnahmen würden i.R.d. weiteren Verfahrens „geprüft", wird in der Mitteilung durchgängig verwendet. Es besteht also kein Anlass, der *Kommission* Vorbehalte gegen den Regelungsbereich zu unterstellen. Dennoch ist zu betonen, dass es i.R.d. Novellierung allenfalls um das Wie, nicht aber um das Ob der Einführung von Regelungen zum Datenschutz durch Technik gehen darf. Die Bedeutung des Ansatzes ist in der Fachdiskussion praktisch unbestritten, und es gibt inzwischen so viele konzeptionelle Vorarbeiten und praktische Erfahrungen (gerade im Bereich von Audits und Gütesiegeln), dass eine Aufnahme in eine novellierte DS-RL geboten ist.

2. Erforderliche Inhalte einer Reform

Will man technischen Mechanismen für einen selbstbestimmten Datenschutz zum Erfolg verhelfen, so kann man erstens spezifische Technologien verbindlich vorschreiben, zweitens reinen Marktmechanismen vertrauen und drittens gemischte Ansätze verfolgen. Der erste Ansatz ist dann erfolgversprechend, wenn es um die Einführung einer konkreten Technologie geht, deren Gestaltung und Einsatz staatlicherseits verbindlich vorgegeben werden kann. Die datenschutzfreundliche Gestaltung des elektronischen Identitätsnachweises des neuen Personalausweises ist hierfür ein Beispiel.[42] Die direkte technikspezifische Regulierung taugt aber nicht als allgemeines Regelungskonzept des Datenschutzrechts, weil der permanente technische Fortschritt entweder zu unangemessenen Vorgaben oder zu einer Datenschutzrechtsreform in Permanenz führen würde.

Der zweite Ansatz ist dort sinnvoll, wo erkennbar ist, dass entsprechende Angebots- und Nachfragemechanismen tatsächlich vorhanden sind. Dies ist jedoch ganz offensichtlich weithin nicht der Fall. Wenn es zutreffend wäre, dass „alle an der Verarbeitung personenbezogener Daten beteiligten Akteure von einer breiteren Verwendung von Technologien zum Schutz der Privatsphäre profitieren würden" – so die *Kommission* in ihrer Mitteilung von 2007, auf die sie in dem Papier von 2010 verweist[43] –, dann würden sich diese von allein am Markt durchsetzen. Es könnte dann nur darum gehen, durch entsprechende Aufklärungsmaßnahmen das Wissen um die Vorteile bei den Marktteilnehmern zu verbreiten. Derartige Informationsbemühungen sind sinnvoll und wichtig. Angesichts der intensiven Diskussion

---

32 So *Brühann*, in: Roßnagel (o. Fußn. 9), Kap. 2.2 Rdnr. 30; *Bizer* (o. Fußn. 25), Rdnr. 32; *Scholz* (o. Fußn. 23), Rdnr. 17.

33 S. *Roßnagel/Pfitzmann/Garstka* (o. Fußn. 3), S. 101 f.; *Bizer* (o. Fußn. 25), Rdnr. 2; *Scholz* (o. Fußn. 23), Rdnr. 34; *Roßnagel* (o. Fußn. 12), S. 44 ff.

34 S. Mitteilung über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre v. 2.5.2007, KOM(2007) 228 endgültig.

35 Dazu noch unten V.2.

36 Mitt. der *Kommission* (o. Fußn. 6), S. 13.

37 Mitt. der *Kommission* (o. Fußn. 6), S. 14.

38 S.o. IV.

39 Mitt. der *Kommission* (o. Fußn. 6), S. 14.

40 Die Frage der Vergabekriterien war in Deutschland eine der umstrittensten des gescheiterten Gesetzgebungsverfahrens (o. Fußn. 27). Am ersten Entwurf wurde kritisiert, dass das Auditzeichen durch einen privaten Gutachter ohne weitere Kontrolle schon bei Einhalten der allgemeinen datenschutzrechtlichen Vorgaben vergeben werden sollte, s. *Roßnagel*, in: Hempel/Krasmann/Bröckling (o. Fußn. 11), S. 276 f.

41 Diese beiden Dimensionen finden sich auch in der aktuellen DS-RL und sind eines ihrer Grundprobleme: Sie soll sowohl zum Funktionieren des Binnenmarkts beitragen als auch die Privatsphäre der Betroffenen effektiv schützen, s. *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, 1999, Einl. Rdnr. 4; *Kuner*, European Data Protection Law, 2nd Ed. 2007, S. 20. Am Rande erwähnt die Mitt. der *Kommission* technische Lösungen auch an anderer Stelle, so bei der Umsetzung von Betroffenenrechten (8).

42 S. *Roßnagel/Hornung/Schnabel*, DuD 2008, 168; *Roßnagel/Hornung*, DÖV 2009, 301; zum Inhalt der Neuregelungen s. *Hornung/Möller*, Passgesetz und Personalausweisgesetz, Komm., 2011.

43 S. die Mitt. der *Kommission* (o. Fußn. 34), S. 7 f.

um den Datenschutz durch Technik in den letzten Jahren sollte aber nicht angenommen werden, die fehlende Verbreitung des Konzepts liege allein an der Unfähigkeit oder Unwilligkeit der Hersteller und Anwender, die Vorteile zu erkennen, die sie mit datenschutzfreundlicher Technik für sich selbst erreichen könnten.

Für ein allgemeines Konzept eines Datenschutzes durch Technik ist deshalb der dritte Ansatz am erfolgversprechendsten. In ihm werden rechtlich gesteuerte Marktanreize gesetzt, Konzepte einer regulierten Selbstregulierung verfolgt und Vorgaben für die Prozesse der Technikentwicklung und -implementierung gesetzt.[44] Dies beinhaltet – anders als in den bisherigen Konzepten der *EU-Kommission* – auch verbindliche Anforderungen. Diese sind nicht klassisch ordnungsrechtlich strukturiert, machen aber Vorgaben für Hersteller und Technikgestalter, enthalten Anforderungen an Datenverarbeiter, zielen auf die Stärkung der datenschutzrechtlichen Betroffenenrechte und nehmen eine rechtlich induzierte Beeinflussung des Markts vor.

Im Bereich der Organisation von Technikentwicklung könnte dies durch mehrere Mittel befördert werden: Branchen- oder technologiespezifische Zielvorgaben können datenschutzfreundliche Ergebnisse festlegen, deren Erreichung der Kreativität und Innovationsfähigkeit der Entwickler überlassen bleibt. Prüf- und Berichtspflichten ermöglichen eine Kontrolle der Ergebnisse, regen aber darüber hinaus auch zur Selbstreflexion der Entwickler über die datenschutzrechtlichen Auswirkungen ihres Tuns an. Die Einbeziehung von und Kooperation mit internen und externen Datenschutzbeauftragten nutzt deren Kompetenzen und sorgt für eine größere Transparenz des Gestaltungsprozesses. Die Stärkung der *Art. 29-Datenschutzgruppe* könnte zu einer stärkeren Strukturierung des Prozesses der Entwicklung von Privacy Enhancing Technologies beitragen. Die Ergebnisse dieses Prozesses werden schließlich am Markt gestärkt, wenn Audits und Gütesiegel Marktanreize setzen, indem sie ein hohes Datenschutzniveau ausweisen, das in einem rechtlich geregelten Verfahren überprüft wird; hier wird es insbesondere darum gehen, ob entsprechende Audits und Gütesiegel auf der europäischen Ebene vergeben werden sollten oder Vorgaben für nationale Vergabeprozesse geschaffen werden. Schließlich ist auch Raum für direkte rechtliche Ansprüche der datenschutzrechtlich Betroffenen, nämlich dort, wo es um klar abgrenzbare Pflichten der verantwortlichen Stellen geht, die diese leicht erfüllen können. Die datenschutzfreundliche Voreinstellung von Datenverarbeitungsregeln (Default-Einstellungen) ist hierfür ein Beispiel.

In den weiteren Reformprozess sollte insbesondere der *Europäische Datenschutzbeauftragte* (*EDSB*) einbezogen werden,[45] der am 18.1.2011 eine Stellungnahme zu der Mitteilung der *Kommission* veröffentlicht hat.[46] In dem Papier setzt der *EDSB* das Konzept des Privacy by Design ebenso wie die *Kommission* in Bezug zu dem Grundsatz der „accountability". Anders als in den Überlegungen der *Kommission* werden daraus aber Konsequenzen für verbindliche Rechtspflichten abgeleitet: Verantwortlichen Stellen sollen unter bestimmten Voraussetzungen belegen müssen, dass sie datenschutzfreundliche Technologien einsetzen.[47] Der *EDSB* schlägt hierfür eine verbindliche Regelung („binding provision setting forth a „privacy by design" obligation")[48] vor. Diese Form der Verbindlichkeit wird durch den bisherigen Inhalt des Prinzips der accountability gestützt. Dieses ist im Datenschutzrecht bislang unbekannt, wurde durch ein Arbeitspapier der *Art. 29-Datenschutzgruppe* in die Reformdiskussion eingebracht[49] und wird derzeit in der Fachöffentlichkeit intensiv diskutiert.[50]

Das Konzept entstammt dem angelsächsischen Rechts- und Sprachraum. Es hat keine direkte Entsprechung im deutschen Recht, sodass schon die Übersetzung nicht unproblematisch ist, da denkbare deutsche Begriffe (Verantwortlichkeit, Haftung, Zurechnung, Rechenschaft) teilweise spezifisch rechtliche Bedeutungen aufweisen.[51] Die deutsche Fassung der Stellungnahme der *Art. 29-Datenschutzgruppe* wählt den Ausdruck der „Rechenschaftspflicht", die der Mitteilung der *Kommission* den des „Rechenschaftsgrundsatzes".[52]

Bei aller begrifflichen und inhaltlichen Unsicherheit ist aber deutlich, dass es darum geht, dass Verantwortung nachprüfbar wahrgenommen wird.[53] Wenn man mit der *Art. 29-Datenschutzgruppe* unter Rechenschaftspflicht die Normierung von Vorschriften versteht, die die für die Verarbeitung Verantwortlichen verpflichtet, angemessene und wirksame Maßnahmen zu ergreifen, um die Grundsätze und Verpflichtungen der Richtlinie umzusetzen und dies auf Verlangen nachzuweisen,[54] so könnte eine Verbindung mit Konzepten des Datenschutzes durch Technik tatsächlich ein Schritt nach vorn sein.

Die Pflichten der verantwortlichen Stellen sollen nach den Vorstellungen des *EDSB* darüber hinaus um eine Bestimmung für Technikentwickler und Hersteller ergänzt werden; auch hierfür werden verbindliche Regelungen angeregt.[55] Des Weiteren wird vorgeschlagen, den Datenschutzaufsichtsbehörden zumindest in den Fällen Sanktionsinstrumente zu ermöglichen, in denen klare Verstöße gegen diese Pflichten vorliegen. Auch diese Vorschläge sind begrüßenswert und weisen für den weiteren Reformprozess in die richtige Richtung. Schließlich unterstützt die Stellungnahme auch die Pläne für Zertifizierungssysteme.[56]

3. Spielräume der Mitgliedstaaten: Richtlinie oder Verordnung?

Betrachtet man die bisher gewonnenen Ergebnisse zum Datenschutz durch Technik unter dem Gesichtspunkt denkbarer Regulierungsstrategien der Union, so lassen sich einige Schlussfolgerungen ziehen. In den Brüsseler Gremien wird derzeit diskutiert, ob anstelle der DS-RL für die künftige Regulierung das Instrument der Verordnung gewählt werden sollte.

Hierfür spricht sich insbesondere der *EDSB* aus, der sich davon sowohl einen effektiven Grundrechtsschutz als auch einen ein-

44 S. näher *Hoffmann-Riem*, AöR 123, 513, 535 ff.; *ders.*, DuD 1998, 684, 687 ff.; *Nedden*, in: Roßnagel (o. Fußn. 7), S. 67 ff.; *Roßnagel*, in: ders. (o. Fußn. 9), Kap. 3.6; *ders.* (o. Fußn. 11), S. 175 ff.; *ders.* (o. Fußn. 12), S. 62 ff.; s.a. die Beiträge in: Die Verwaltung 2001, Beiheft 4; vgl. bereits *Podlech*, DVR 1972/73, 149, 155; *ders.*, in: Brückner/Dalichau (Hrsg.), Beiträge zum Sozialrecht. FG Hans Grüner, 1982, S. 451 ff.

45 Zu seinen Aufgaben gehört nach Art. 46 lit. d der VO (EG) Nr. 45/2001 (ABl. EG Nr. L 8 v. 12.1.2001, S. 1) die Beratung aller Organe und Einrichtungen der Union „in allen Fragen, die die Verarbeitung personenbezogener Daten betreffen".

46 Opinion on the Communication from the Commission – „A comprehensive approach on personal data protection in the European Union", abrufbar unter: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf.

47 S. Stellungnahme (o. Fußn. 46), S. 23.

48 S. Stellungnahme (o. Fußn. 46), S. 23.

49 *Art. 29-Datenschutzgruppe*, WP 173: Stellungnahme 3/2010 zum Grundsatz der Rechenschaftspflicht vom 13.7.2010, abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_de.pdf.

50 S. insb. die Konferenz „Privacy and Accountability 2011", die aus dem Projekt *PATS* (http://pats-project.eu/) heraus entstanden ist.

51 S. zum Konzept und zu seinen vielfältigen Bedeutungsinhalten aus europäischer Perspektive z.B. *Harlow*, Accountability in the European Union, 2002; *Arnull/Wincott* (Hrsg.), Accountability and Legitimacy in the European Union, 2002; *Bovens*, European Law Journal 2007, 447 ff.

52 Mitt. der *Kommission* (o. Fußn. 6), S. 13; hier wird der englische Begriff hinzugesetzt.

53 S. Stellungnahme der *Art. 29-Datenschutzgruppe* (o. Fußn. 49), S. 8; s.a. *Fisher*, Oxford Journal of Legal Studies 24 (2004), 495, 496 ff.

54 *Art. 29-Datenschutzgruppe* (o. Fußn. 49), S. 21.

55 S. Stellungnahme (o. Fußn. 46), S. 23 f.

56 S. Stellungnahme (o. Fußn. 46), S. 24.

heitlichen Binnenmarkt für personenbezogene Daten verspricht.[57] Dahinter dürfte die zutreffende Überlegung stehen, dass die Richtlinie zwar zu einer formalen Vereinheitlichung des Datenschutzrechts in Europa geführt hat, das tatsächliche Schutzniveau aber deutliche Unterschiede aufweist.

Inhaltlich knüpft die Diskussion an die umstrittene Frage an, ob es sich bei der derzeitigen DS-RL um eine Teil- oder Vollharmonisierung handelt. Nach Ansicht des *EuGH* führt die Richtlinie zu einer „grundsätzlich umfassenden Harmonisierung".[58] Allerdings räume sie den Mitgliedstaaten dennoch einen weiten Handlungsspielraum ein und ermächtige sie, für bestimmte Fälle besondere Regelungen beizubehalten oder einzuführen, solange dies im Einklang mit dem Ziel der Richtlinie geschehe, ein Gleichgewicht zwischen dem freien Verkehr personenbezogener Daten und dem Schutz der Privatsphäre zu wahren.[59]

Letztlich dürfte die Frage der mitgliedstaatlichen Spielräume kaum pauschal für die gesamte Richtlinie beantwortbar sein.[60] Vielmehr ist in jedem Einzelfall zu fragen, was genau ihre Vorschriften zu einer konkreten Regelungsfrage vorgeben und wie viel Freiheit für Abweichungen durch die Mitgliedstaaten übrig bleibt.

Diese Überlegung weist auch den Weg für die künftige Regulierungsstrategie. Da einerseits Richtlinien auch sehr umfassende und detaillierte Vorgaben enthalten, andererseits Verordnungen auch Spielräume für mitgliedstaatliche Abweichungen definieren können, ist die Frage des Instruments weniger entscheidend als die der Spielräume, die den Mitgliedstaaten gewährt werden sollten.

Letzteres kann aber nicht pauschal für alle Bereiche des Datenschutzrechts beantwortet werden. Vielmehr ist entsprechend dem Grundsatz der Subsidiarität (Art. 5 Abs. 3 EUV) zu differenzieren und zu fragen, ob der jeweilige Regelungsinhalt wegen seines Umfangs oder seiner Wirkungen besser auf der Unionsebene zu verwirklichen ist. Dies wird z.B. bei Begriffsdefinitionen der Fall sein, wo ein Bedürfnis nach nationalen Abweichungen nicht erkennbar ist – die unterschiedliche Terminologie in Art. 2 DS-RL einerseits, § 3 BDSG andererseits hat keine erkennbaren Vorteile. In anderen Bereichen sollte hingegen Raum für mitgliedstaatliche Innovation sein.

Gerade das Konzept des Datenschutzes durch Technik bietet hierfür ein gutes Beispiel: Die materiellen Anforderungen in § 3a BDSG und die Audit- und Gütesiegelverfahren haben sich i.R.d. Gestaltungsspielräume der DS-RL entwickelt und werden nun in der aktuellen europäischen Reformdiskussion an die europäische Ebene zurückgegeben. Dies wäre unter anderen, engeren europäischen Rahmenbedingungen (also z.B. einer Verordnung ohne explizite Öffnungsklauseln) nicht möglich gewesen.

Diese Erfahrung spricht nicht prinzipiell gegen eine weitergehende Harmonisierung oder den Wechsel zur Form der Verordnung. Wohl aber spricht sie deutlich dafür, den Mitgliedstaaten Innovationsspielräume dort zu lassen, wo wegen der Aktualität der Entwicklungen (noch) keine Festlegungen für längere Zeiträume möglich sind und deshalb der Ideenwettbewerb zwischen den Mitgliedstaaten nicht behindert, sondern gefördert werden sollte. Dies ist gerade bei der Entwicklung neuer Schutzkonzepte im Bereich des Datenschutzes durch Technik, bei der Konkretisierung allgemeiner datenschutzrechtlicher Prinzipien auf neue Technologien und der Entwicklung von Vorgaben für neuartige Privacy Enhancing Technologies der Fall.

VII. Schlussfolgerungen

Das Konzept des Datenschutzes durch Technik ist ein wesentlicher Baustein eines modernen Datenschutzrechts und durch Vorarbeiten und Erfahrungen so weit konkretisiert, dass die Neuregelung in der EU hierfür verbindliche Vorgaben enthalten sollte.

Hierauf zu verzichten hieße, ein sinnvolles Konzept für einen langen Zeitraum zu behindern, da die Reformzyklen in der Union eine beträchtliche Länge aufweisen: Der erste Vorschlag der *Kommission* zur derzeitigen DS-RL datiert v. 5.11.1990[61] – ein Zeitpunkt, zu dem es kein World Wide Web gab. Dies hatte sich bei der Verabschiedung am 24.10.1995 zwar bereits geändert, die heutige Art und Weise der Datenverarbeitung hat aber mit der damaligen kaum etwas gemein.

Sollte die nächste Reform erneut erst mit einem Abstand von 20 Jahren erfolgen, so muss die aktuelle Modernisierung Instrumente beinhalten, die mit der technischen Entwicklung Schritt halten. Da diese Entwicklung heute noch unbekannt ist, sind „lernende" Mechanismen erforderlich.

Hierzu kann als europäisches Instrument die Verabschiedung von sog. tertiärem Unionsrecht durch die *EU-Kommission* genutzt werden (Art. 290 AEUV).[62] Angesichts der bislang geringen Erfahrung mit diesem Instrument sollte dies aber durch Spielräume für einen Ideenwettbewerb unter den Mitgliedstaaten ergänzt werden. Dies wird umso wichtiger werden, je mehr neue technische Entwicklungen nicht nur die spezifische Konkretisierung allgemeiner datenschutzrechtlicher Prinzipien erfordern, sondern das Datenschutzrecht insgesamt vor konzeptionelle Probleme stellen.[63]

Hierauf kann das System des europäischen Datenschutzrechts nur reagieren, wenn es Spielräume für lernende Prozesse aufweist. Insgesamt muss die Handlungsempfehlung deshalb lauten, i.R.d. aktuellen Reform zum einen den Einstieg in verbindliche Vorgaben für die Gestaltungs- und Anwendungsprozesse der Hersteller und Anwender und rechtlich regulierte Anreizsysteme im Binnenmarkt zu schaffen. Zum anderen ist von einer Regulierung von Technologien abzusehen, die heute noch wenig bekannt sind. Stattdessen müssen hier Rahmen für technische, aber auch für rechtliche Innovationen gesetzt werden.

Prof. Dr. Gerrit Hornung, LL.M.
ist Inhaber des Lehrstuhls für Öffentliches Recht, IT-Recht und Rechtsinformatik an der Universität Passau, der auch in das Institute of IT-Security and Security Law (ISL) der Universität eingebunden ist. Der Beitrag ist aus einem Vortrag auf der Tagung „Datenschutz in Europa. Recht und Technik in der Novellierung der europäischen Datenschutzrichtlinie" der Alcatel-Lucent Stiftung für Kommunikationsforschung am 6.5.2011 in Stuttgart hervorgegangen. Eine erweiterte Fassung wird im Konferenzband erscheinen.

57 S. Stellungnahme (o. Fußn. 46), S. 15.
58 *EuGH* MMR 2004, 95 m. Anm. *Roßnagel* – Lindqvist; bekräftig in *EuGH* MMR 2009, 171 – Huber.
59 *EuGH* MMR 2004, 95 m. Anm. *Roßnagel* – Lindqvist.
60 S. insoweit einerseits eher die Spielräume betonend: *Jacob*, RDV 1993, 11; *Simitis*, NJW 1998, 2473, 2476; s.a. *ders.*, DuD 2000, 714; *ders.*, NJW 1997, 281, 282; *Dammann/Simitis*, EG-Datenschutzrichtlinie, 1997, Einl. Rdnr. 10; *Roßnagel/Pfitzmann/Garstka* (o. Fußn. 3), S. 55 ff.; andererseits *Brühann*, EuZW 2009, 639 ff.; ähnlich *Hoeren*, RDV 2009, 89 ff.; differenzierend *Lütkemeier*, DuD 1995, 597, 598.
61 ABl. EG Nr. C 277 v. 5.11.1990, S. 3.
62 Dafür auch der *EDSB* (o. Fußn. 46), S. 24; ebenso *Roßnagel*, FAZ v. 1.6.2011, S. 7.
63 Das gilt insb. für die Entwicklungstendenzen des Ubiquitous Computing, die im Datenschutzrecht nicht nur ein Vollzugs-, sondern auch ein Konzeptproblem verursachen, s. *Roßnagel* (o. Fußn. 11), S. 155.