4. DIE CODIERUNG DES DATENSCHUTZES

Johann Bizer

Der Code – gestaltbar für und gegen den Datenschutz

Die Verwendung eines neuen Begriffs in bereits mit Definitionen besetzten Anwendungsfeldern erfüllt vor allem eine heuristische Funktion. Eine andere Nomenklatur kann es jenseits kanonisierter Begriffsbildung erleichtern, bekannte Phänomene aus anderen Blickwinkeln zu sehen und zu interpretieren. In diesem Sinne ist »Code« kein juristischer, sondern eine von dem amerikanischen Rechtswissenschaftler Lawrence Lessig gewählte Bezeichnung für die technischen Gestaltungsprinzipien des Cyberspace (Lessig 1999). Der Code unterscheidet sich von den Gesetzen des Staates, den sozialen Normen des gesellschaftlichen Lebens sowie den Gesetzen des Marktes. Seine Grammatik ist die Software, die die Entfaltungsräume der Nutzer bestimmt. Der Code der Software legt fest, ob und welche Daten personenbezogen erhoben und gespeichert werden, mit welchen Daten sie korreliert und ob und wann sie wieder gelöscht werden. Auf diese Weise bestimmt der Code letztlich die Entfaltungsmöglichkeiten der informationellen Selbstbestimmung. Ist es also die Macht der Technik, die die Spielräume der bürgerlichen Freiheit zwischen ihre starken Arme nimmt?

Mitnichten: Die Entfaltungsmöglichkeiten informationeller Selbstbestimmung werden durch die Faktoren Markt, Recht, (soziale) Normen und schließlich den Code der technischen Architektur beeinflusst (Lessig 1999, 86, 2001, 159). Das Grundthema der Regulierung lautet damit »auf den [lessig'schen] Punkt« gebracht, die genannten Faktoren unter Beachtung ihrer Wechselwirkungen auf ein Ziel zu justieren. So wird die Steuerungswirkung des Marktes beispielsweise durch seine rechtlichen Rahmenbedingungen bestimmt, das staatliche Recht kann durch soziale Normen oder den Markt beeinflusst werden und die Architektur des Internets wird durch den Code geprägt, dessen Wirkungen und Steuerungsimpulse wiederum durch staatliches Recht ebenso wie durch den Markt oder soziale Normen beeinflusst werden. Lessig macht nun nicht nur auf die Gestaltungsmacht des Codes in seinen vielfältigen Ausprägungen, sondern vor allem auch auf seine Gestaltbarkeit aufmerksam. Der Code ist also alles andere als neutral, sondern er bestimmt die Entfaltungsmöglichkeiten informationeller Selbstbestimmung immer nur in den von staatlicher Regulierung, Markt und sozialen Normen vorgegebenen Grenzen.[1]

Unter diesen Voraussetzungen bezeichnet die »Codierung des Datenschutzes« also die Spielräume und Grenzen, die die technische Infrastruktur des Internets in ihren Protokollen und Anwendungen – also mit ihrer »Architektur« – der informationellen Selbstbestimmung einräumt, während umgekehrt der Code auch durch soziale Normen, Angebot und Nachfrage des Marktes sowie die Gesetze des Staates gestaltet wird.[2]

1. Datenschutz durch Technik

Für den deutschen Datenschutzrechtler ist der Zusammenhang von Recht und Technik alles andere als neu (siehe Roßnagel 1993).[3] Eine an den Zielen des Datenschutzrechts ausgerichtete Technikgestaltung ist für uns nicht nur theoretisches Konstrukt, sondern längst Wirklichkeit des Datenschutzrechts (Bizer 1999 a). Ihr geht zeitgeschichtlich betrachtet die kritische Analyse der Auswirkungen der modernen Datenverarbeitung auf das allgemeine Persönlichkeitsrecht – im heutigen Verständnis die informationelle Selbstbestimmung – voraus (Steinmüller/Lutterbeck/Mallmann 1973; Podlech, DVR 1972/73, 149). In Deutschland hat sie seit den 70er Jahren zu einer staatlichen Datenschutzgesetzgebung mit vornehmlich ordnungsrechtlichen Instrumenten geführt. Erst eine strategische Ausrichtung der Politik an dem Leitbild der Informationsgesellschaft hat Mitte der 90er Jahre auch die Einsicht von der Gestaltbarkeit der Informationstechnik begünstigt und gefördert. Als ein Beleg unter vielen mag die Feststellung des Forschungsrats aus dem Dezember 1995 dienen, der traditionell normative ausgestaltete Datenschutz müsse angesichts der neuen Bedingungen der Datenverarbeitung durch eine »Datenschutztechnologie« ergänzt werden (Forschungsrat 1995, 32). Eine vergleichbare Forderung nach der Entwicklung datenschutzfreundlicher Technologien haben die Datenschutzbeauftragten des Bundes und der Länder im Jahr 1997 gefordert (Konferenz 1997). Die frühzeitige Gestaltung der Datenverarbeitungssysteme als Ansatz datenschutzrechtlicher Regelung verfolgt auch die europäische Union: So heißt es beispielsweise im Erwägungsgrund 46 der EG-Datenschutzrichtlinie 46/95/EG vom 25. 10. 1995, dass die zum Schutz der personenbezogenen Daten geeigneten technischen und organisatorischen Maßnahmen insbesondere »zum Zeitpunkt der Planung des Verarbeitungssystems« getroffen werden müssen.

1.1 Datensparsamkeit

Mit dem Prinzip der datensparsamen Technikgestaltung hat der deutsche Gesetzgeber den Code der Internetarchitektur dem Primat seines Gesetzes unterworfen. Zunächst 1997 für die Online-Dienste (§ 3 Abs. 4 TDDSG 1997, § 12 Abs. 5 MD-StV 1997), später im Datenschutzrecht für Rundfunkdienste (§ 47 Abs. 5 Rdf-StV) wurde dieses Prinzip im Jahr 2000 auch auf geschäftsmäßige TK-Dienstleistungen ausgeweitet (§ 3 Abs. 4 TDSV) und schließlich im Jahr 2001 in das allgemeine Datenschutzrecht überführt (§ 3 a BDSG):

> »Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.«

Die besondere Bedeutung dieser Regelung liegt in ihrer »proaktiven« Wirkung (Bizer 2000, § 3, Rn. 132) als präventives und gleichzeitig innovatives Technikgestaltungsrecht (Bizer 1999 a, 46). Der Gesetzgeber selbst hat zur Begründung der damaligen Regelung im TDDSG vor allem den präventiven Aspekt dieser Maßnahme hervorgehoben.

> »Bereits durch die Gestaltung der Systemstrukturen, in denen personenbezogene Daten erhoben und verarbeitet werden können, soll die Erhebung und Verwendung personenbezogener Daten vermieden und die Selbstbestimmung der Nutzer sichergestellt werden« (BT-Drs. 13/7934, S. 22).

Die damalige Koalitionsmehrheit aus CDU/CSU und FDP feierte das »Prinzip der Datenvermeidung« in einem Entschließungsantrag am 11. 6. 1996 als ein Kernelement des Gesetzes (BT-Drs. 7935, S. 3). Und die SPD-Fraktion zählte die »Datenvermeidung« zu den »Grundvoraussetzungen eines effektiven Schutzes der Beteiligten in elektronischen Netzen« (BT-Drs. 13/7936, S. 4).

Im Schlussbericht der Enquete-Kommission »Deutschlands Weg in die Informationsgesellschaft« vom 22. 6. 1998 wird die Regulierung des Codes als eine Folge der Globalisierung der Datenverarbeitung und dem verbundenen Verlust an Kontrolle über die Verarbeitung personenbezogener Daten begründet.

> »Richtungsweisend ist der Ansatz, das Datenschutzrecht um technikrechtliche Elemente zu ergänzen, um Anbieter zum Einsatz von datenminimierenden Einrichtungen der Informations- und Kommunikationstechnik anzuhalten.« (BT-Drs. 13/11004, S. 17).

Die Aufnahme des Prinzips der datensparsamen Technikgestaltung in das allgemeine Datenschutzrecht begründete der Gesetzgeber damit, dass »durch die Gestaltung der Systemstrukturen die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten soweit wie möglich vermieden und dadurch Gefahren für das informationelle Selbstbestimmungsrecht des Betroffenen von vornherein minimiert werden« (BT-Drs. 14/4329, S. 33). Weder der Bundesrat noch die Opposition erhoben gegen diese Regelung Einwände, die Abgeordnete Gisela Schröter (MdB, SPD) bezeichnete sie in der Debatte des Deutschen Bundestages als einen »guten Weg«, um Gefahren für die informationelle Selbstbestimmung »systematisch zu reduzieren« (BT-Prot. 14/128, 12390 (C) vom 27. 10. 2000) und der Abgeordnete Jörg Tauss (MdB, SPD) nannte sie ein »zentrales Instrument eines neuen Datenschutzes« (BT-Prot. 14/365, 16180 (B) vom 6. 4. 2001).

1.2 Technische Vorkehrungen

Das Prinzip der datensparsamen Technikgestaltung hat in den rechtlichen Anforderungen an die Datensicherheit der Verarbeitung personenbezogener Daten einen Vorläufer. Sowohl § 9 BDSG mit seiner Anlage bzw. Art. 17 der EG-Datenschutzrichtlinie 46/95/EG zielen auf die Gestaltung technischer (sowie organisatorischer) Maßnahmen, um die Verarbeitung personenbezo-

gener Daten zu schützen. Eine vergleichbare Regelung enthält das deutsche Recht in § 87 Abs. 1 TKG, der die Betreiber von TK-Anlagen für Zwecke geschäftsmäßiger Telekommunikation zu »angemessenen technischen Vorkehrungen« insbesondere zum Schutz des Fernmeldegeheimnisses und personenbezogener Daten verpflichtet.

Vergleichbare Regelungen kennt das Recht der Onlinedienste, das die Dienstanbieter dazu verpflichtet, die Einhaltung ihrer datenschutzrechtlichen Pflichten durch technische und organisatorische Vorkehrungen sicherzustellen. So hat der Dienstanbieter bspw. nach § 4 Abs. 4 Satz 1 Nr. 2 TDDSG durch besondere Vorkehrungen die Einhaltung seiner sich aus § 6 Abs. 1 TDDSG ergebenden Löschungspflicht sicherzustellen, nämlich dass

> »die anfallenden personenbezogenen Daten über den Ablauf eines Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht und gesperrt werden können«.

1.3 Förderung von Forschung und Technologie

Damit die rechtliche Gestaltung der Technik nicht nur normatives Postulat im Gesetzblatt bleibt, bedürfen ihre Anforderungen der Übersetzung in den Code der Standardisierung (vgl. Büllesbach 1999, 459). Diese Übersetzung muss auf mindestens zwei verschiedenen Ebenen ansetzen, nämlich der Förderung der Forschung und Entwicklung von datenvermeidenden Technologien und ihrer Implementierung in konkrete Anwendungen und Produkte (s. u. 1.4).

Die Entwicklung und Förderung datenvermeidender Technologien ist in Europa vor allem unter dem Begriff der Privacy Enhanced Technologies (PET) thematisiert worden (Registratiekammer 1995; Burkert 1996; Borking DuD 1998, Borking DuD 2001). Das Fünfte Rahmenprogramm »Forschung, technologische Entwicklung und Demonstration (1998 – 2002)« vom 22. 12. 1998 enthält nicht nur ein eigenes Themenfeld »Benutzerfreundliche Informationsgesellschaft«, sondern nennt auch die Entwicklung von »Technologien für einen besseren Schutz der Privatsphäre« ausdrücklich als einen Schwerpunkt (Abl. EG L 25/1 S. 14 f. vom 1.2.1999). Der derzeit diskutierte Gemeinsame Standpunkt des Rates 27/2002 vom 28. 1. 2002 über ein Sechstes Rahmenprogramm (2002 – 2006) wiederholt diese Zielsetzung zwar nicht ausdrücklich, erwartet aber im Schwerpunkt »Entwicklung des elektronischen und behördlichen Geschäftsverkehrs« eine Berücksichtigung der »Bedürfnisse der Nutzer« (Abl. C 113 E /54 (61) vom 14. 5. 2002), zu dem auch die Förderung datenschutzfreundlicher Technologien gehört. Ein konkretes Beispiel liefert die Mitteilung der EU-Kommission »Internet der nächsten Generation – Vorrangige Maßnahmen beim Übergang zum neuen Internet-Protokoll IPv6« vom 21. 2. 2002. Danach sollen die Normen und Spezifikationen insbesondere der neuen Protokollgeneration IPv6 den Grundrechten auf Schutz der Privatsphäre und des Datenschutzes umfassend Rechnung tragen (KOM (2002) 96, S. 16).[4]

Aber nicht nur die Europäische Union, sondern auch der Bund fördert im

Rahmen des Aktionsprogramms »Innovation und Arbeitsplätze in der Informationsgesellschaft des 21. Jahrhunderts« die Entwicklung von technischen Werkzeugen für den Datenschutz.[5] Im Rahmen dieses Programms wurde bspw. der Aufbau einer Infrastruktur unabhängiger Mix-Netzknoten im Internet unterstützt, die eine verschlüsselte und anonyme Nutzung von Internetseiten ermöglichen soll (Bäumler DuD 2001).[6] Bereits abgeschlossen ist das Projekt »Datenschutz in Telediensten – DASIT«, in dem ein Konzept für eine datensparsame Abwicklung elektronischer Bestellungen einschließlich der Lieferung und Bezahlung entwickelt und erprobt wurde (Roßnagel 2002 b, Grimm/Löhndorf/Scholz DuD 1999).

1.4 Technische Implementierung

Datenschutzgerechte Technikgestaltung ist auf verschiedene Weise möglich: Sie kann bspw. das Erheben und Verarbeiten personenbezogener Daten in den Rechnern der elektronischen Netze minimieren oder den Nutzer mit Werkzeugen zum Selbstschutz ausstatten, damit er seine Daten selbst verschlüsseln oder unter Pseudonym kommunizieren kann. Einen anderen Ansatzpunkt hat das Projekt P3P – Platform für Privacy Preferences des W3C-Konsortiums – gewählt.[7] In seiner derzeitigen Form ermöglicht P3P die Erstellung maschinenlesbarer Datenschutzerklärungen, die von den Clienten übersetzt werden können. Das Ziel von P3P beschränkt sich also zunächst auf die Transparenz der Datenschutzerklärung des Anbieters. In weiteren Ausbaustufen soll P3P einen Kommunikationsprozess über den Inhalt der Datenschutzerklärung zwischen Server und Client unterstützen (Cranor DuD 2000; Cavoukian/Gurski/Mulligan/Schwartz DuD 2000). P3P bietet also einen technischen Rahmen für die Kommunikation über Datenschutzstandards, ersetzt aber keine Formulierung materieller Regelungen zum Schutz der informationellen Selbstbestimmung (Greß DuD 2001). Seine Praxistauglichkeit hat der P3P-Standard in einer ersten Version im bereits erwähnten Projekt DASIT bewiesen (Enzmann/Schulze 2002, 115). Die Fortschreibung des P3P-Standards um den Prozess einer interaktiven Aushandlung zwischen Anbieter und Nutzer über ein konsentiertes Datenschutzniveau steht allerdings noch aus.

1.5 Akzeptanz

Eine Datenschutzpolitik, die auf die Verbreitung datenschutzgerechter oder sogar -sparsamer Technologien setzt, ist jedoch nur erfolgreich, wenn entsprechende Produkte von den Anwendern auch in ihre Systeme implementiert werden. Eine wichtige Motivation für eine derartige Diffusion ist, dass nach Umfragen und Marktstudien zwischen dem gebotenen Datenschutzniveau und der Akzeptanz der Nutzer ein signifikanter Zusammenhang besteht, der die Ausgestaltung des Datenschutzes für Unternehmen zu einem

relevanten Wettbewerbsfaktor aufwertet (Büllesbach 2002, 53, ders. 1999, 449 ff.; RDV 1997, 239 ff.).[8]

Nach einer 2001 in Deutschland durchgeführten Umfrage wünschen 53% der Befragten, dass dem Datenschutz künftig mehr Bedeutung zukommen soll (Opaschowski, DuD 2001, 678). Bemerkenswert ist, dass diese Haltung alles andere als eine deutsche Besonderheit darstellt. Nach einer Umfrage unter US-Bürgern vom August 2000 zeigten sich in den USA bspw. 84% der Einwohner besorgt, wenn Geschäftsleute oder Unbekannte Informationen über sie oder ihre Familie bekommen (The Pew Internet & American Life Project, 2000, pg 25 Question 3).[9] In Sachen Datenschutz nach der Vertrauenswürdigkeit von Institutionen befragt, liegen in Deutschland am untersten Ende des Rankings der Adresshandel, den nur 8% für zuverlässig halten, der Versandhandel (10%) sowie Internetanbieter (10%). Versicherungen werden immerhin von 31% der Befragten und Banken von 52% für zuverlässig gehalten (Opaschowski DuD 2001, 673 ff.). Aber auch für diese letzten beiden gilt, dass ihre Werte negativ formuliert (69% bzw. 58%) kaum als zufriedenstellend angesehen werden können.

Eine Länder vergleichende Untersuchung aus dem Jahr 1999 zeigt, dass die deutschen Umfragewerte einen internationalen Trend widerspiegeln (vgl. IBM 1999). Während die Vertrauenswürdigkeit der Banken in Sachen Datenschutz in den USA (77%) und Deutschland (70%) überwiegend positiv bewertet wird, schneidet der Versandhandel in der Bewertung des Datenschutzes deutlich schlechter ab: Nur 45% der in den USA Befragten sowie 42% in Großbritannien und Deutschland kommen zu einer positiven Bewertung dieser Anbieter. Geradezu vernichtend lautet das Urteil der Nutzer und Verbraucher über die kommerziellen Internetanbieter: Nur 21% USA, 13% Großbritannien und 10% Deutschland brachten nach dieser Untersuchung den kommerziellen Internetanbietern in Sachen Datenschutz Vertrauen entgegen.

Die Zustimmung zum und die Erwartung an den Datenschutz sind vor allem deswegen von Bedeutung, weil ein deutlicher Zusammenhang zwischen der Einschätzung des Datenschutzes einerseits und dem Kaufverhalten andererseits nachgewiesen werden kann. Datenschutz ist ein Akzeptanzfaktor für die Entwicklung von Märkten. Bereits die IBM–Studie aus dem Jahr 1999 belegt einen Zusammenhang zwischen dem Vertrauen der Kunden in den Datenschutz eines Anbieters und seinem Kaufverhalten.

In der Offline-Welt zeigte sich, dass 54% in den USA, 32% in Großbritannien und 35% in Deutschland wegen fehlender Sicherheit über die Verwendung ihrer Daten auf die Nutzung oder den Kauf eines Angebots verzichteten. Bei den kommerziellen Internetanbietern zeigte sich eine noch stärkere Angleichung im internationalen Vergleich, nämlich 57% in USA, 41% in Großbritannien und 56% in Deutschland (IBM 1999, pg 23, 27). Dass dieses Ergebnis keine »Eintagsfliege« ist, beweist eine Umfrage vom Oktober 2000 der Mannheimer Forschungsgruppe Wahlen im Auftrag des Bundesverbandes der Banken. Danach erklärten 62% der Internetnutzer in Deutschland, sie hätten im Internet noch nicht online bestellt oder gekauft, weil ihrer Meinung nach der Datenschutz unzureichend gewährleistet sei (BvB 2001). Zu ver-

gleichbaren Ergebnissen kommt die Opaschowski-Studie für das Jahr 2001: Nur 23% gehen davon aus, dass ihre Daten bei der Nutzung im Internet hinreichend geschützt sind und halten eine Nutzung für unbedenklich. Hingegen gaben 46% an, wegen Mängeln bei Datenschutz und Datensicherheit das Internet nicht zu nutzen. Noch 26% sahen sich nicht in der Lage, zu dieser Frage Stellung zu beziehen (»weiß nicht«). 5% war diese Frage »egal«.

1.6 Marktwirtschaftlicher Datenschutz

Das moderne Datenschutzrecht versucht der zunehmenden Bedeutung des Datenschutzes als Akzeptanzkriterium der Nutzer und als Wettbewerbsfaktor der Anbieter durch eine stärkere Implementierung marktwirtschaftlicher Instrumente gerecht zu werden (Büllesbach RDV 1997, Roßnagel 2002a; Bäumler 2002). Datenschutzaudit und Gütesiegel zielen ihrer Intention nach auf eine Prämierung der in den Datenschutz getätigten Anstrengungen und Investitionen durch eine Bescheinigung, mit der im Wettbewerb geworben werden kann. Nach der Bundesregelung des § 9a BDSG können

> Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen »zur Verbesserung des Datenschutzes und der Datensicherheit (...) ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen«.

Die Regelung der näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter bleiben allerdings einem besonderen Gesetz überlassen, das der Bund bislang noch nicht verabschiedet hat.

Unter den Landesgesetzgebern, die neben dem Bund eine Regelung für ein Datenschutzaudit im Rahmen ihrer Gesetzgebungskompetenz (Bizer/Petri 2001) in ihr Gesetz aufgenommen haben, hat bislang nur Schleswig-Holstein für seinen öffentlichen Bereich eine Ausführungsregelung erlassen (Bäumler DuD 2002, 326, Golembiewski 2002). Nach dieser Regelung können öffentliche Stellen des Landes ihr Datenschutzkonzept durch das Unabhängige Landeszentrum für Datenschutz prüfen und beurteilen lassen. Methodische Elemente dieses Verfahrens sind eine Bestandsaufnahme, die Festlegung von Datenschutzzielen sowie die Einrichtung eines Managementsystems, die abschließend in einer Datenschutzerklärung zusammengefasst werden. Abgeschlossen wird das Verfahren durch ein zu veröffentlichendes Kurzgutachten des Datenschutzzentrums und der Verleihung eines Auditzeichens. Für die Implementierung einer datenschutzgerechten Technik ist nach der Konzeption des Audits vor allem die Zielvereinbarung von Bedeutung (näher Petri 2002).

Eine noch stärkere Steuerungswirkung auf die Ebene der Technik wird das Gütesiegel nach dem Datenschutzrecht in Schleswig-Holstein ausüben. Das Gütesiegels wird für IT-Produkte (Hard- und Software) verliehen, die mit den Vorschriften für den Datenschutz und die Datensicherheit vereinbar sind (§ 4

Abs. 2 SG LDSG). Darüber hinaus muss das Produkt aber auch besondere Eigenschaften, insbesondere in Hinblick auf die Datenvermeidung und die Datensparsamkeit, die Datensicherheit und die Revisionssicherheit der Datenverarbeitung sowie die Gewährleistung der Betroffenenrechte aufweisen (§ 2 Abs. 2 Nr. 4 SH GütesiegelVO). Eine unmittelbare Steuerungswirkung entfaltet das Gütesiegels zunächst nur für den Einsatz in der schleswig-holsteinischen Verwaltung. § 4 Abs. 2 SH LDSG verpflichtet die Behörden des Landes, »vorrangig« solche Produkte einzusetzen, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit »in einem förmlichen Verfahren« festgestellt wurde. Eine mittelbare Steuerungswirkung wird das Gütesiegel jedoch auch über die Grenzen Schleswig-Holsteins entfalten, weil Anbieter eines mit einem Gütesiegel versehenen Produkts nicht gehindert sind, gegenüber anderen öffentlichen und privaten Kunden auf die besondere Qualitätsauszeichnung durch das schleswig-holsteinische Gütesiegel zu verweisen. Unter diesem Gesichtspunkt erstaunt es wenig, dass die Ministerpräsidentin von Schleswig-Holstein den Datenschutz als einen »Standortvorteil für das Land Schleswig-Holstein« entdeckt hat (Simonis 2002).

Nicht übersehen werden darf jedoch, dass es anderen Anbietern nicht verwehrt ist, neben den gesetzlichen auch privatrechtlich gestaltete Instrumente eines marktwirtschaftlichen Datenschutzes zu entwickeln und anzubieten. Das vielleicht bekannteste unter ihnen ist das Gütesiegel »Quid« (Wedde/Schröder 2001). Daneben sind eine Reihe weiterer Entwicklungen kurz vor der Markteinführung (bspw. Rieß 2001, Schaar/Stotz DuD 2002, 330), deren Entwicklung und Wirkung in den nächsten Jahren zu verfolgen sein wird.[10] Die umfassendsten Anforderungen hat wohl die Initiative D21 mit ihren Qualitätskriterien für Internet-Angebote vorgelegt.

2. Die Instrumentalisierung des Code

Das Konzept einer datenschutzfreundlichen Technikgestaltung ist als Antwort auf die durch Digitalisierung und Vernetzung zunehmenden Risiken für das informationelle Selbstbestimmungsrecht zu verstehen (Bizer 2000, § 3 Rn. 132 ff.). Während im nichtöffentlichen Bereich vor allem die Gefährdungen durch neue Kundenprofile zunehmen, bemächtigt sich zunehmend auch der Staat der Architektur des Internets für Zwecke der Inneren Sicherheit. Letztlich ist die Strategie dieselbe: Der Code ist neutral, aber seine Grammatik kann funktionsbezogen nicht nur zur Förderung der informationellen Selbstbestimmung, sondern auch zu ihrer Einschränkung geschrieben werden. Die folgenden Beispiele beschränken sich auf die staatliche Steuerung bzw. Steuerungsversuche des Codes im Recht der TK-Überwachung. Gemeinsam ist ihnen eine tiefgreifende Einflussnahme der rechtlichen Regulierung auf die Struktur der Verarbeitung personenbezogener Daten. Angesichts der zunehmenden Bedeutung der vernetzten elektronischen Kommunikation kommt der Überwachbarkeit der Datenflüsse dieser Netze eine zentrale Bedeutung zu.

2.1 TKÜV

Um den Sicherheitsbehörden auf der Grundlage der gesetzlichen Regelungen eine TK-Überwachung zu ermöglichen, bedarf es geeigneter technischer Einrichtungen auf Seiten der Dienstanbieter. § 88 Abs. 1 TKG verpflichtet die Betreiber von TK-Anlagen, die technischen Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation »auf eigene Kosten zu gestalten und zu betreiben«. Die näheren technischen Anforderungen sind in der TK-Überwachungsverordnung (TKÜV vom 22.1.2002, BGBl. I S. 458) konkretisiert (Pernice DuD 2002, 207), die wiederum in einer der Geheimhaltung unterliegenden Technischen Richtlinie (§ 11 TKÜV) präzisiert werden.

Art und Ausmaß der rechtlichen Steuerung des Codes verdeutlichen jüngste Forderungen des Bundesrates, der mit Beschluss vom 31.5.2002 einen Gesetzesvorschlag verabschiedet hat, in dem von der Bundesregierung eine Ausweitung der technischen Infrastruktur zur TK-Überwachung gefordert wird (BT-Drs. 275/02). Danach sollen die Internet-Provider verpflichtet werden, die im Wege der DSL-Technik anfallenden Verbindungs- und Kommunikationsdaten den zuständigen Behörden »zeitgleich automatisch zu übermitteln«. Die Mobilfunkprovider sollen ferner hardwarebezogene Kennungen der Mobilfunkgeräte an die zuständigen Behörden übermitteln, um die Verwendung mehrerer Karten in einem Gerät zu unterbinden (Entschließung BR-Drs. 275/02, S. 1 f.).

Die Codierung der technischen Infrastruktur der TK-Überwachung ist alles andere als ein nationales Projekt. sondern wird seit Jahren innerhalb der westlichen Welt (EU, USA und Verbündete) koordiniert. Ein erster umfangreicher Anforderungskatalog findet sich in der Entschließung des Rats der Europäischen Union vom 17.1.1995 »über die rechtmäßige Überwachung des Fernmeldeverkehrs«, der erst knapp zwei Jahre später veröffentlicht wurde (96/C 329/01, Abl. EG C vom 4.11.1996). Die in dieser Entschließung formulierten Anforderungen entsprechen weitgehend dem US-amerikanischen Communications Assistance for Law Enforcement Act (CALEA vom 24.10.1994, U.S. Public Law 103-414; 47 U.S.C 1001 – 1010). Seit spätestens 1993 werden die Anforderungen an TK-Betreiber in einer internationalen Arbeitsgruppe (International Law Enforcement Telecommunications Seminar – ILETS) koordiniert (Statewatch, DuD 1997, 346)[11] sowie eine Zusammenarbeit mit der Internationalen Fernmeldeunion (ITU) und zu den internationalen Standardisierungsgremien angestrebt (BMWi BMWi, DuD 1999, 717, 720). Das europäische Standardisierungsinstitut ETSI (European Telecommunications Standards Institute) erarbeitet technische Abhörstandards für öffentliche TK-Systeme.[12] In die gleiche Richtung zielt auch die Empfehlung R (95)13 des Europarates vom 11.9.1995.[13] Mit Hilfe der technischen Normung und der weltweiten Verbreitung derartiger TK-Anlagen versuchen sich die führenden Industriestaaten des Westens die Möglichkeit zu sichern, die Telekommunikation auch in nicht kooperationswilligen Staaten zu überwachen (Bogonikolos 1999, pg 11).

2.2 IMSI-Catcher

Das zweite Beispiel für eine Instrumentalisierung des Codes für Zwecke der Inneren Sicherheit ist der Einsatz des sogenannten IMSI-Catchers zur Ermittlung und Überwachung mobil geführter elektronischer Kommunikation. Zentrale Eigenschaft des IMSI-Catchers ist die Möglichkeit, die International Mobile Subscriber Identity (IMSI) eines Mobilfunkgerätes im Einzugsbereich des Catchers zu ermitteln sowie seinen genauen Standort festzustellen (Fox DuD 1997, 539, DuD 2002, 212). Mit Kenntnis der IMSI können die Sicherheitsbehörden von den TK-Dienstanbietern nach § 89 Abs. 6 bzw. § 90 Abs. 1 TKG Auskunft über die von ihnen über den jeweiligen Anschlussinhaber gespeicherten Informationen verlangen (BT-Drs. 13/8453, S. 3). Mit einer Variante des IMSI-Catchers ist es ferner möglich, die Kommunikationsinhalte unmittelbar zu überwachen (BT-Drs. 13/8453, S. 3). Der IMSI-Catcher könnte in dieser technischen Variante, die lediglich eine andere Software erfordert, dazu dienen, die rechtsstaatlichen Sicherungen der TK-Überwachung, insbesondere ihre richterliche Anordnung zu umgehen (BT-Drs. 13/8453, S. 3 zu Nr. 4).

Die Funktionalität des IMSI-Catchers beruht im Wesentlichen auf einer konzeptionellen »Einbruchstelle« im Mobilfunkstandard GSM. Das Sicherheitsprotokoll des GSM-Standard sieht nur eine einseitige anstelle einer gegenseitigen Authentifizierung zwischen Sendestation und Endgerät vor (Fox DuD 1997, 539; Pütz DuD 1997, 321). Diese Schwachstelle ermöglicht es dem IMSI-Catcher, gegenüber dem Handy bzw. seiner IMSI-Karte eine Festnetzstation zu simulieren, ohne dass beim Austausch der Verschlüsselungsschlüssel aufgedeckt werden kann. Erst das UMTS-Protokoll arbeitet mit einer gegenseitigen Authentifizierung und soll derartige Angriffe (»Maskerade« bzw. »Man-in-the-Middle«) verhindern (Pütz/Schmitz/Martin DuD 2001, Fox DuD 2002, 215).

Datenschutzrechtlich problematisch ist diese Schwachstelle in der Sicherheitsarchitektur des GSM-Standards nicht nur, weil mit einem illegalen Einsatz des IMSI-Catchers durch auswärtige Dienste im Inland zu rechnen ist, sondern weil seine Verwendung immer auch die Erfassung der im Einzugsbereich des überwachten Handys befindlichen Kommunikationspartner umfasst. Die TK-Dienstanbieter verweisen ferner auf eine nicht unerhebliche Beeinträchtigung der angebotenen Dienstqualität durch den IMSI-Catcher, da dieser zeitweise den Empfang von Signalen stört, so dass die Verbindungen nicht verfügbar sind (Fox DuD 2002, 214 f.).

Der Einsatz des IMSI-Catchers blieb lange Zeit im Dunkeln. Eine erste Regelungsinitiative ging vom Bundesrat aus, der im Rahmen der Beratungen zum Begleitgesetz zum Telekommunikationsgesetz eine gesetzliche Rechtsgrundlage für den Einsatz des IMSI-Catchers sowohl im G-10-Gesetz als auch in der Strafprozessordnung vorschlug (BT-Drs. 13/8453, S. 3 zu Nr. 4, S. 7 zu Nr. 15). In dem damaligen Gesetzgebungsverfahren lehnte die Bundesregierung eine solche Rechtsänderung ab, deutete aber die Verwendung des IMSI-Catchers »zum Zweck der Ermittlung technischer Identifikationsmerkmale als Ersatz für unbekannte Rufnummern« an (BT-Drs. 13/8453, S. 11 zu. Nr. 11, S. 15 zu Nr. 15).

Die Rechtsgrundlagen ermöglichen zwar eine TKÜ-Anordnung gegen den Anschluss einer bestimmten Person unter Nennung der Rufnummer oder einer anderen Kennung (§ 100 b Abs. 2 Satz 2 StPO), aber nicht einen Eingriff in das Fernmeldegeheimnis zur Ermittlung einer unbekannten Kennung einer unbekannten Person.[14] Gleichwohl wurde das Gerät nach einem Bericht des Spiegels zumindest von dem Bundeskriminalamt und dem Bundesgrenzschutz eingesetzt (Spiegel 33/2001, 54; Bundesregierung 2001, BT-Drs. 14/6885). Das hierbei eingesetzte Gerät verfügte nach Angaben des Bundesbeauftragten für den Datenschutz nicht einmal über eine Betriebsgenehmigung nach § 47 TKG (Löwenau-Iqbal, DuD 2001, 578).

Mittlerweile hat der Gesetzgeber Rechtsgrundlagen für den Einsatz des IMSI-Catchers durch den Verfassungsschutz sowie die Strafverfolgungsbehörden geschaffen. Der Einsatz ist jeweils auf die Standortermittlung beschränkt. Die Rechtsgrundlage für das Bundesamt für Verfassungsschutz hat der Gesetzgeber im Rahmen des Terrorismusbekämpfungsgesetzes vom 9.1.2002 (BGBl. I S. 361, 362) erlassen. Danach darf der IMSI-Catcher – bezeichnet als »technisches Mittel« – unter näher bestimmten Voraussetzungen »zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes und zur Ermittlung der Geräte- und Kartennummer« eingesetzt werden.

Für die Straftatverfolgungsbehörden hat der Bundestag eine Rechtsgrundlage in § 100 i StPO für den IMSI-Catcher im Schnellverfahren am 17.5.2002 auf der Grundlage einer Beschlussempfehlung des Rechtsausschusses (BT-Drs. 14/9088) verabschiedet (BT-Prot. 14/237, S. 23742), die jetzt noch den Bundesrat passieren muss. Die Regelung ermöglicht den Einsatz technischer Mittel (IMSI-Catcher) zum einen zur Ermittlung der Geräte- und Kartennummer zur Vorbereitung einer TK-Überwachung nach § 100 a StPO und den Voraussetzungen dieser Regelung. Zum anderen darf der IMSI-Catcher zur Standortermittlung eines aktiv geschalteten Handys zur vorläufigen Festnahme nach § 127 StPO oder zur Vollstreckung eines Haft- oder Unterbringungsbefehls eingesetzt werden, bei Straftaten von erheblicher Bedeutung auch zur Eigensicherung der eingesetzten Beamten.

Nach beiden Regelungen dürfen personenbezogene Daten Dritter anlässlich dieser Maßnahmen nur erhoben werden, wenn dies aus technischen Gründen zur Zweckerreichung unvermeidbar ist, sie dürfen nur für den erforderlichen Datenabgleich verwendet werden und sind nach Beendigung der Maßnahme unverzüglich zu löschen. Die im Bundesrat von den Ländern Bayern und Thüringen mit einem Gesetzentwurf vom 27.11.2001 verfolgte Linie, eine Rechtsgrundlage zur Ermittlung des Standortes und zur Ermittlung der Geräte- und Kartennummer in § 100 c Abs. 1 Nr. 1 b StPO aufzunehmen (BR-Drs. 1014/01, S. 2, 11), konnte sich nicht durchsetzen. Eine weitere Variante hat der Bundesrat am 30.5.2002 in das Gesetzgebungsverfahren eingebracht mit einer Ergänzung des § 100 g StPO – der Nachfolgeregelung des außer Kraft getretenen § 12 FAG (BR-Drs. 275/02).[15] Der Bundesrat will darüber hinaus den Einsatz des IMSI-Catchers auch für die Fahndung nach entflohenen Sexualstraftätern anwenden (§ 457 Abs. 4 (neu) E-StPO, § 463 Abs. 4 (neu) E-StPO).

2.3 Vorratsspeicherung

Ein weiteres Beispiel für die sicherheitspolitisch motivierte Einflussnahme des Gesetzgebers auf den Codes ist die Diskussion über die Einführung von Mindestspeicher- bzw. Vorratsspeicherpflichten im Onlinerecht. Das Beispiel illustriert dass eine staatliche Regulierung sich auch gegen einen im Wesentlichen ökonomisch gestützten Code richten kann.

Einer der zentralen Grundsätze des Datenschutzrechts ist die Begrenzung der Datenverarbeitung auf das für einen bestimmten Erhebungszweck erforderliche Maß. Sind die personenbezogenen Daten nicht mehr erforderlich, so sind sie zu löschen: Verbindungsdaten nach § 6 Abs. 2 Satz 2 TDSV unverzüglich »spätestens am Tag nach Beendigung der Verbindung« und Nutzungsdaten nach § 6 Abs. 1 i.V. m. § 4 Abs. 4 Nr. 2 TDDSG unmittelbar nach Beendigung des Zugriffs bzw. der Nutzung. Im Unterschied zum TK-Datenschutzrecht lässt das TDDSG auch eine Sperrung genügen, wenn gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungspflichten einer Löschung entgegenstehen. Allerdings lässt das Datenschutzrecht von der Löschungspflicht Ausnahmen zu, insbesondere soweit die Verbindungs- bzw. Nutzungsdaten zu Abrechnungszwecken benötigt werden (§ 6 Abs. 4 TDDSG, § 6 Abs. 2 Satz 1 i.V.m. § 7 Abs. 1 TDDSG). »Soweit« bedeutet in diesem Zusammenhang, dass aus der Menge der Verbindungs- bzw. Nutzungsdaten nur die für die Abrechnung erforderlichen Daten verarbeitet werden dürfen, während die Restmenge wiederum »unverzüglich zu löschen« ist (§ 7 Abs. 3 Satz 2 TDSV). Entsprechendes ergibt sich für die Verarbeitung der Nutzungsdaten aus dem in § 6 Abs. 4 TDDSG verankerten Prinzip der Erforderlichkeit, das durch eine Verpflichtung zu entsprechenden technischen Vorkehrungen einer Löschung bzw. Sperrung flankiert wird (§ 4 Abs. 4 Nr. 2 TDDSG).

Für das Speichern der Abrechnungsdaten sieht das Datenschutzrecht Höchstspeicherfristen (Bizer DuD 2002, 302) vor, d.h. die Provider dürfen die personenbezogenen Abrechnungsdaten »zu Beweiszwecken für die Richtigkeit der berechneten Entgelte« unter Kürzung der Zielrufnummer um die letzten drei Ziffern bis Ablauf dieser Frist speichern (§ 7 Abs. 3 Satz 2, 3 TDSV). Als Ausnahme zu dieser Regel gilt, dass auf Verlangen des Kunden die Abrechnungsdaten mit Versendung der Rechnung zu löschen oder vollständig zu speichern sind (§ 7 Abs. 4 Satz 1 TDSV). Auf Betreiben der Sicherheitsbehörden wurde die Höchstspeicherfrist durch die TDSV vom 18. 12. 2000 (BGBl. I S. 740) von zunächst 80 Tagen auf sechs Monate verlängert (§ 7 Abs. 3 Satz 3 TDSV). In früheren Entwürfen war sogar eine Frist von einem Jahr vorgesehen. Die vom Verordnungsgeber zu dieser Regelung gelieferte Begründung, Vorstellungen aus der Praxis erforderten zur besseren Abrechnung eine verlängerte Speicherfrist, ist allerdings ein »Schimäre«. Tatsächlich sehen große TK-Provider schon aus Kostengründen keine Notwendigkeit von der Höchstspeicherfrist von 80 Tagen abzuweichen – auch wenn dies mit Rücksicht auf zahlungsunwillige Kunden nicht öffentlich kommuniziert wird.

Entscheidend ist, dass mit der Verlängerung der Höchstspeicherfrist die

Menge der Verbindungsdaten, auf die die Sicherheitsbehörden im Rahmen ihrer Befugnisse auch rückwirkend zugreifen dürfen, erweitert werden. Die Auskunftsverpflichtung über bspw. TK-Verbindungsdaten beschränkt sich seit der Antiterrorgesetzgebung bei weitem nicht mehr nur auf die für Straftatverfolgung zuständigen Behörden (§ 100 g, h StPO). Nach § 8 Abs. 8 BVerfSchG, § 10 Abs. 3 MAD-Gesetz sowie § 2 Abs. 3 a BND-Gesetz sind nun auch die Nachrichtendienste befugt, allerdings unter den verfahrensrechtlichen Voraussetzungen des Artikel G-10-Gesetzes, von den Anbietern geschäftsmäßiger TK-Dienste und Teledienste Auskünfte über die TK-Verbindungsdaten und Teledienstnutzungsdaten einzuholen (Terrorismusbekämpfungsgesetz vom 9.1.2002, BGBl. I S. 361).

Eine der TDSV vergleichbare Regelung gilt nach dem Datenschutzrecht für Teledienste (§ 6 Abs. 7 TDDSG), die lediglich rechtstechnisch eine andere Konstruktion aufweist: Soweit für Zwecke der Abrechnung erforderlich darf der Provider Nutzungsdaten verarbeiten (§ 6 Abs. 4 Satz 1 TDDSG). Er hat sie folglich zu löschen, wenn sie für den Abrechungszweck nicht mehr benötigt werden. Nur wenn der Kunde einen Einzelnachweis für seine kostenpflichtigen Nutzungen verlangt, dann dürfen die Nutzungsdaten personenbezogen gespeichert werden (vgl. § 6 Abs. 6 TDDSG). Ist dies der Fall, dann gilt eine Höchstspeicherfrist, die nach der Gesetzesfassung vom 14.12.2001 (BGBl. I S. 3721) wie auch im TK-Datenschutzrecht von 80 Tagen auf sechs Monate verlängert worden ist.

Im Zuge der Verschärfung der Sicherheitsgesetze nach dem Terroranschlag vom 11. September 2001 in New York und Washington hat sich die Diskussion über die Umwandlung der Höchstspeicherfristen in Mindestspeicherpflichten bzw. in die Verpflichtung zur Vorratsspeicherung erheblich intensiviert. Einen ersten Vorschlag hat – soweit ersichtlich – die CDU/CSU-Opposition in einem Gesetzentwurf »zur Verbesserung der Bekämpfung von Straftaten der Organisierten Kriminalität und des Terrorismus« vom 29.8.2001 eingebracht (BT-Drs. 14/6834). Mit der Begründung, dass die Auskunft über Verbindungs- und Nutzungsdaten leer laufe, wenn diese Daten von den Providern gelöscht werden müssten, wird eine Ausweitung der Verordnungsermächtigung nach § 89 Abs. 1 Satz TKG auf »Mindestspeicherfristen« gefordert (BT-Drs. 14/6834, S. 7, 14).

Weitergehende Vorschläge enthielt der von den Ländern Bayern und Thüringen am 27.11.2001 eingebrachte Gesetzentwurf »zur Verbesserung des strafrechtlichen Instrumentariums für die Bekämpfung des Terrorismus und der Organisierten Kriminalität« (BR-Drs. 1014/01). Der Entwurf sah eine Ausweitung des § 89 Abs. 1 TKG auf die Vorratsspeicherung von TK-Daten nicht nur für »Zwecke der Strafverfolgung und der Gefahrenabwehr«, sondern auch für die »Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes sowie des Zollkriminalamtes« vor. Mit der Einbeziehung der Nachrichtendienste geht der Gesetzentwurf über die von der CDU/CSU-Bundestagsfraktion im Entschließungsantrag »Sicherheit 21« vom

9. 10. 2001 ursprünglich vorgesehene Beschränkung der Mindestfristen »zugunsten der Strafverfolgungsbehörden« deutlich hinaus (BT-Drs. 14/7065 (neu)).

Nach dem Gesetzesvorschlag Bayerns und Thüringens (BR-Drs. 1014/01) soll die Höhe der Mindestspeicherfrist durch eine Rechtsverordnung unter Berücksichtigung der berechtigten Interessen der Dienstanbieter, der Betroffenen sowie der Erfordernisse »effektiver Strafverfolgung und Gefahrenabwehr« sowie der »effektiven Erfüllung der gesetzlichen Aufgaben« der sonstigen Sicherheitsbehörden festgelegt werden. Eine vergleichbare Regelung sollte unter der Überschrift »Vorratsspeicherung« als neuer § 6 a in das TDDSG eingefügt werden. Im Bundesrat wurde der Vorschlag mit Beschluss vom 22. 3. 2002 zurückgewiesen und deshalb nicht in den Deutschen Bundestag eingebracht. Jedoch finden sich die Vorschläge der Sache nach in einem Beschluss des Bundesrates vom 31. 5. 2002 wieder, nachdem sich die Mehrheitsverhältnisse auf Grund der Wahlergebnisse in Sachsen-Anhalt zu Gunsten der CDU geführten Länder geändert hatten (BR-Drs. 275/02).

Dem Beschluss liegt ein von Niedersachsen am 27. 3. 2002 eingebrachter Entwurf eines »Gesetzes zur Verbesserung der Ermittlungsmaßnahmen wegen des Verdachts sexuellen Missbrauchs von Kindern und der Vollstreckung freiheitsentziehender Sanktionen« zugrunde, der jedoch durch die Mehrheit der CDU-geführten regierten Bundesländer erheblich ausgeweitet wurde und über die Verfolgung und Bekämpfung von Straftaten gegen die sexuelle Selbstbestimmung hinausgeht. Der Sache nach werden die Änderungen zu § 89 Abs. 1 TKG sowie § 6 a TDDSG aus dem Gesetzentwurf Bayerns und Thüringens vom 27. 11. 2001 (BR-Drs. 1014/01) wieder aufgegriffen. Gleichwohl ist bemerkenswert, dass wenige Tage nach dem Beschluss der »schwarzgelben« Mehrheit der Bundesvorstand der CDU Deutschlands in dem Version 2.0 »Chancen@Deutschland – Eine Internetstrategie für die Politik« vom 3. 6. 2002 »die von der Bundesregierung geplante generelle Verpflichtung von Providern zur Einhaltung von Mindestspeicherpflichten« als »aus rechtsstaatlichen wie auch wirtschaftlichen Gründen nicht tragbar« geißelte.

Auf europäischer Ebene spielt die Einführung von Mindestspeicherpflichten derzeit vor allem im Rahmen der Revision der EG-TK-Datenschutzrichtlinie 97/66/66 vom 15. 12. 1997 eine Rolle. Die Problemstellung zwischen den Interessen des Datenschutzes, der Wirtschaft und der Strafverfolgungsbehörden ist bereits in der Mitteilung der Kommission eEurope2002 über die »Schaffung einer sichereren Informationsgesellschaft ...« vom 26. 1. 2001 (KOM (2000) 890, S. 20 – 22) ausgebreitet. Nach Art. 6 Abs. 1 der noch geltenden TK-Datenschutzrichtlinie 97/66/EG sind die dort als Verkehrsdaten bezeichneten Verbindungsdaten »nach Beendigung der Verbindung ... zu löschen oder zu anonymisieren«. Ausnahmen sind nur zu festgelegten Zwecken, insbesondere zur Berechnung der Entgelte zulässig. Allerdings ermöglicht Art. 14 der Richtlinie bereits heute den Mitgliedstaaten, Ausnahmen zu Zwecken der inneren und äußeren Sicherheit, insbesondere zur »Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten« zu erlassen.

Während der Kommissionsvorschlag zur Richtlinie »über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation« vom 12.6.2000 noch bei dieser Regelung blieb (Art. 15 Abs. 1 KOM (2000) 385), wurde diese Linie spätestens seit dem Frühjahr 2001 von einigen Mitgliedstaaten im Rat der Europäischen Union zu Gunsten einer Regelung der Vorratsspeicherung (»data retention«) aufgeweicht. Insbesondere die Bundesregierung bat die EU-Kommission im Rahmen der Regelung des Art. 6 zu prüfen, »ob und ggf. welche Harmonisierungsmaßnahmen erforderlich sind, um den notwendigen Bedürfnissen der Strafverfolgungsbehörden Rechnung zu tragen« (12.12.2001, Dok. 15104/01 ADD 1). Dem Vorschlag des Rates die Ausnahmebestimmung zur strikten Löschungspflicht durch eine Regelung in Art. 15 Abs. 1 des Entwurfes (jetzt Art. 14) aufzuweichen, stimmte das Europaparlament in zweiter Lesung am 30.5.2002 mit einer Ergänzung grundsätzlich zu. Nun soll unter der Voraussetzung einer engeren Grundrechtsbindung eine Aufbewahrung der Verbindungsdaten »während einer begrenzten Zeit gemäß den allgemeinen Grundsätzen des Gemeinschaftsrechts« zulässig sein (Europaparlament vom 30.5.2002, P5-TAPROV (2002) 0261 – PE 319.107).[16]

3. Fazit

Der Ausgangspunkt der Überlegungen war die Regulierung der technischen Infrastruktur des Internets (der Code) und seine Auswirkungen auf den Datenschutz. Dem Gesetzgeber ist es mit dem Prinzip der datenvermeidenden Technikgestaltung sowie weiteren flankierenden Instrumenten gelungen, die informationelle Selbstbestimmung als eine Zielvorgabe der technischen Entwicklung zu implementieren und auf diese Weise einen Paradigmenwechsel im Verhältnis von Technik und Datenschutzrecht einzuleiten. Allerdings gilt – wie die Beispiele zeigen –, dass der Gesetzgeber die Regulierung des Codes längst auch für Zwecke der Inneren Sicherheit instrumentalisiert hat. Die Perspektiven des Datenschutzes liegen in der Förderung einer datensparsamen Technikgestaltung als Bestandteil des Systemdatenschutzes, gleichwohl werden die Gestaltungsräume angesichts des zunehmenden Datenhungers der Sicherheitsbehörden auf die personenbezogenen Daten elektronischer Kommunikation immer enger. Es bleibt die Förderung von Konzepten des technisch unterstützten Selbstdatenschutzes, für den es wiederum eines ungehinderten Zugangs zu sicheren Kryptographieverfahren bedarf, für den sich Alfred Büllesbach vor (Büllesbach 1999, 458) und hinter den Kulissen mit Nachdruck eingesetzt hat.

Alfred Büllesbach hat die (zumindest) partiell bestehenden Interessenkonvergenzen zwischen der Wirtschaft einerseits und den Bürgerrechten für Datenschutz und Datensicherheit als Voraussetzungen einer sich entwickelnden Informationsgesellschaft frühzeitig erkannt und als Herausforderung auch seiner eigenen Tätigkeit angenommen. Als Datenschutzpolitiker wird Alfred

Büllesbach angesichts der Herausforderungen an ein modernes Datenschutzrecht mehr denn je gefordert sein: Wer verbindet schon Erfahrungen aus dem Leben eines Wissenschaftlers und akademischen Lehrers mit denen eines Landesdatenschutzbeauftragten und schließlich den Herausforderungen und Visionen als Datenschutzbeauftragter eines großen internationalen Konzerns? Nur ein Datenschutzpolitiker wie Alfred Büllesbach.

1 Vergleichbares ließe sich auch für den technischen Schutz des Urheberrechts beschreiben und präzisieren.
2 »Chatten nur unter Pseudonym« wäre also eine »soziale Norm«, »Ohne SSL-Verschlüsselung übermittelt kein Kunde seine Kreditkartennummer« ein Beispiel für eine Steuerung durch den Markt. »Nutzerdaten sind unverzüglich nach Ende der Verbindung zu löschen« ein Beispiel für staatliche Regulierung.
3 »Der Anspruch einer neuen materiellen Rationalität ist also nicht prinzipiengeleitet, sondern dynamisch. In täglicher kommunikativer Herstellung verlangt er die Gestaltung der neuen Technologien nach den Werten Gerechtigkeit, Solidarität und Freiheit ...« (Büllesbach 1986, S. 280).
4 Siehe hierzu Artikel 29 Data Protection Working Group Party, Opinion 2/2002 on the use of unique identifier in telecommunication terminal equipments: the example of Ipv6, Working Paper 48, Adopted on 30. May 2002.
5 5,8 Millionen DM laut Bundesministerium für Wirtschaft und Technologie, PM vom 31.1.2001 »AN.ON – BMWi fördert Projekt zur Stärkung von Anonymität im Internet«.
6 »http://www.datenschutzzentrum.de/projekte/anon/index.htm« sowie »http://www.inf.tu-dresden.de/~hf2/anon/«.
7 Auf P3P verweist im übrigen auch Lessig 1999, 160 f.; dt.: 2001, 283. Näher »http://www.w3.org/P3P/«.
8 »Zu Recht verweigert der Verbraucher, Bürger und Kunde personenbezogene Daten, wenn er nicht gleichzeitig auf einen adäquaten Schutz vertrauen kann. Unternehmen, die diese Herausforderung nicht annehmen, werden deshalb auf dem Markt auf Dauer nicht existieren können« (Büllesbach 1993, S. 80)
9 59% very bzw. 25% somewhat concerned.
10 So wird bspw. die Frage aufgeworfen, welchen haftungsrechtlichen Verbindlichkeitsgrad ein Gütesiegel gegenüber dem Kunden haben kann (Dahm, DuD 2002).
11 Der im Rahmen von ILETS erstellte Anforderungskatalog an Service Provider der TK ist identisch mit dem aus der Ratsentschließung 96/C 329/01 vom 17.1.1995 über die rechtmäßige Überwachung des Fernmeldeverkehrs (EG Abl. C 329/1 vom 4.11.1996).
12 Siehe »http://www.etsi.org/technicalactiv/li.html.«
13 Concerning Problems of Criminal Procedure Law Connected with Information Technology, Appendix 11 f.
14 So später auch die Begründung zu 9 Abs. 4 BVerfSchG: »Die Erkenntnisse ... berühren nähere Umstände der Kommunikation zwischen Personen, die dem Schutz des Grundrechts aus Art. 10 GG unterliegen«, BT-Drs. 14/7386 (neu) S. 40; Ebenso Antrag Niedersachsen BR-Drs. 275/02, S. 5. Stellenweise wurde auf § 161 ff. sowie §§ 100 a, 100 b StPO Abs. 1 Nr. 1 b) StPO zurückgegriffen.
15 Der beschlossene Entwurf wurde in zahlreichen Punkten auf der Grundlage der Beschlüsse des Rechtsauschusses verschärft.
16 Die Maßnahmen müssen »in einer demokratischen Gesellschaft« notwendig, angemessen und verhältnismäßig sein.. Alle genannten Maßnahmen – und damit auch die Datenspeicherung – müssen »den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich des in Artikel 6 Absatz 1 und 2 des Vertrages über die Europäische Union niedergelegten Grundsätzen entsprechen« (Abänderung 46).

Literatur

Bäumler, H. (DuD 2002): Marktwirtschaftlicher Datenschutz, Audit und Gütesiegel à la Schleswig-Holstein, DuD 2002, 325 ff.

Bizer, J. (1999 a): Datenschutz durch Technikgestaltung, in: H. Bäumler / A. v. Mutius (Hrsg.), Datenschutzgesetze der Dritten Generation, Neuwied 1999, S. 28 ff.

Bizer., J. (Bizer 1999 b): Nachfrage nach Sicherheit. Privater Vertraulichkeitsschutz und staatliche Sicherheitspolitik in der Telekommunikation, in: J. Bizer / H.-J. Koch (Hrsg.), Sicherheit, Vielfalt, Solidarität, ein neues Paradigma des Verfassungsrechts? Symposium zum 65. Geburtstag Erhard Denningers am 20. 6. 1997, Baden-Baden 1998, S. 29 ff.

Bizer, J. (2000): Kommentierung § 3 TDDSG in: A. Roßnagel, (Hrsg.), Recht der Multimediadienste, Loseblatt 2000.

Bizer, J. (DuD 2002): Höchstspeicherfristen, DuD 2002, 302.

Bizer, J. / Petri, T. B. (DuD 2000): Kompetenzrechtliche Fragen des Datenschutz-Audits, DuD 2000, S. 97 ff.

Bogonikolos (1999): Development of Surveillance Technology and Risk of Abuse of Economic Information, Part 1/4, The Perception of Economic Risks Arising from the Potential Vulnerability of Electronic Commercial Media to Interception, Interim Study, Working Document for the STOA Panel, Luxemburg, May 1999, PE 1678.184/Int.St./part _.

Borking, J. (DuD 1998): Einsatz datenschutzfreundlicher Technologien in der Praxis, DuD 1998, S. 636 ff.

Borking, J. (DuD 2001): Privacy-Enhancing Technologies, Darf es ein Bitchen weniger sein?, DuD 2001, 607-615

Büllesbach, A. (1993): Das Unternehmen in der Informationsgesellschaft, in: Wilhelm, R. (Hrsg.), Information – Technik – Recht: Rechtsgüterschutz in der Informationsgesellschaft, Darmstadt 1993, S. 69 ff.

Büllesbach, A. (RDV 1997): Datenschutz und Datensicherheit als Qualitäts- und Wettbewerbsfaktor, RDV 1997, S. 239 ff.

Büllesbach, A. (1998): Vernetztes Denken für eine gerechte Gesellschaftsordnung, in: Gesellschaft für Rechts- und Verwaltungsinformatik e.V. (Hrsg.), Kommunikationstechnische Vernetzung: Rechtsprobleme – Kontrollchancen – Klienteninteressen, Darmstadt 1986, S. 263

Büllesbach, A. (1999): Datenschutz als prozessorientierter Wettbewerbsbestandteil, in: Müller, G./Stapf, K.-H. (Hrsg.), Mehrseitige Sicherheit in der Kommunikationstechnik: Bd. 2, Erwartung, Akzeptanz, Nutzung, Bonn 1999, S. 431 ff.

Büllesbach, A. (2002): Premium Privacy in: H. Bäumler / A. von Mutius (Hrsg.), Datenschutz als Wettbewerbsvorteil, Wiesbaden 2002, S. 45 ff.

Bundesregierung (2001): Rechtliche Zulässigkeit von so genannten IMSI-Catchern, Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der FDP, BT-Drs. 14/6885.

Burkert, H. (1997): Privacy-Enhancing Technologies: Typology, Critique, Vision, in: Agre, P.E./ Rotenberg, M. (Eds.), Tecnology and Privacy: The New Landscape, , Messachusetts 1997, S. 125 ff.

BUB 2001: Bundesverband deutscher Banken. Blitz Demoskopie Nr. 11, April 2001.

Cavoukian, A. / Gurski, M. / Mulligan, D. / Schwartz, A. (DuD 2000): P3P und Datenschutz, DuD 2000, S. 475 ff.

Cranor, L. F. (DuD 2000): Platform for Privacy Preferences – P3P, DuD 2000, 479.

Der Spiegel (32/2001): Wahre Wunderbox, Heft 33/2001 vom 13. 8. 2001, S. 54 f.

Enquete-Kommission, Zukunft der Medien in Wirtschaft und Gesellschaft, Deutschlands Weg in die Informationsgesellschaft, Schlussbericht, BT-Drs. 13/11004.

Enzmann, M. / Schulze, G. (2002, 115): Die DASIT-Lösung in: Ronagel 2002, S. 107 ff.

Forschungsrat (1995): Rat für Forschung, Technologie und Innovation: Informationsgesellschaft, Chancen, Innovationen und Herausforderungen, Feststellungen und Empfehlungen, hrsg. vom Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie (BMBF), Bonn 1995.

Fox, D. (DuD 1997): IMSI-Catcher, DuD 1997, 539.

Fox, D. (DuD 2002): Der IMSI-Catcher, DuD 2002, S. 212 ff.

Golembiewski, C. (2002): Das Datenschutzaudit in Schleswig-Holstein, in: H. Bäumler/ v. Mutius (Hrsg.), Datenschutz als Wettbewerbsvorteil, Wiesbaden 2002, S. 107 ff.

Greß, Sebastian (DuD 2001): Das Datenschutzprojekt P3P, DuD 2001, 144 ff.

Grimm, R. / Löhndorf, N./ Scholz, P. (DuD 1999, 272): Datenschutz in Telediensten (DASIT), DuD 1999, S. 272 ff.

IBM (1999): Multi-National Consumer Privacy Survey, October 1999.

Konferenz (1997): 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Erforderlichkeit datenschutzfreundlicher Technologien, Entschließung vom 23./24. 10. 1997, DuD 1997, S. 735.

Lessig, L. (1999): Code and other Laws of Cyberspace, New York 1999 (dt.: Code und andere Gesetze des Cyberspace, Berlin 2001.

Löwenau-Iqbal, G. (DuD 2001): Der Einsatz des IMSI-Catchers zur Überwachung von Handys, DuD 2001, S. 578.

Opaschowski (2001): Der gläserne Konsument, B.A.T Forschungsinstitut 2001.

Opaschowski (DuD 2001): Datenschutz quo vadis ? DuD 2001, S. 678 ff.

Pernice, I. (DuD 2002): Die Telekommunikationsüberwachungsverordung (TKÜV), DuD 2002, 207 ff.

Petri, T. B. (2002): Zielvereinbarungen im Datenschutzrecht, in: H. Bäumler/ v. Mutius (Hrsg.), Datenschutz als Wettbewerbsvorteil, Wiesbaden 2002, S. 142 ff.

Podlech, A. (DVR 1972/73): Verfassungsrechtliche Probleme öffentlicher Informationssysteme, DVR 1972/73, S. 149 ff.

Pütz, S. (DuD 1997): Zur Sicherheit digitaler Mobilfunksysteme. Nachweisbare Authentikation am Beispiel von UMTS, DuD 1997, S. 321 ff.

Pütz, S. / Schmitz, R. / Martin, T. (DuD 2001): Security Mechanismen in UMTS, DuD 2001, S. 623 ff.
Registratiekamer (1995): Privacy-Enhancing Technologie. The path to anonymity Vol. I und Vol. II 1995.
Rieß, J. (2001): Selbstregulierung und E-Business-Politik – Die Sicht der Wirtschaft, TA-Datenbanknachrichten Nr. 4, 10. Jg Dezember 2001, S. 65 ff.
Roßnagel, A. (1993): Rechtswissenschaftliche Folgenforschung 1993.
Roßnagel, A. (2002 a): Marktwirtschaftlicher Datenschutz im Datenschutzrecht der Zukunft, Wiesbaden 2002, S. 115 ff.
Roßnagel, A. (2002 b): Datenschutz beim Online-Einkauf, Wiesbaden 2002.
Schaar, P./Stutz, U. (DuD 2002): Datenschutz-Gütesiegel für Online-Dienstleistungen, DuD 2002, S. 330 ff.
Simonis, H. (2002): Datenschutz als Standortvorteil für das Land Schleswig-Holstein, in: H. Bäumler/v.Mutius (Hrsg.), Datenschutz als Wettbewerbsvorteil, Wiesbaden 2002, S. 224.
Statewatch (DuD 1997): EU and FBI launch global surveillance system, DuD 1997, S. 346 ff.
Steinmüller, W. / Lutterbeck, B. / Mallmann, C. u.a. (1973): Grundfragen des Datenschutzes, Gutachten, BT-Drs. 6/3826.
The Pew Internet & American Life Project (2000): Trust and privacy online. Why americans want to rewrite the rules, August 2000.
Wedde, P. / Schröder (2001): Quid ! Das Gütesiegel für Qualität im betrieblichen Datenschutz, Frankurt am Main 2001.
Wenning, R. / Köhntopp, M. (DuD 2001): P3P im europäischen Rahmen, DuD 2001, S. 139 ff.