

# **PRIVACY: EIN GRUNDRECHT MIT ABLAUFDATUM? INTERDISZIPLINÄRE BEITRÄGE ZUR GRUNDRECHTSDEBATTE**

**Walter Peissl**

*Institut für Technikfolgen-Abschätzung (ITA) der  
Österreichischen Akademie der Wissenschaften, Wien, Austria*

Im Spannungsfeld von technischer Entwicklung, politischen Rahmenbedingungen und gesellschaftlicher Relevanz analysiert die Technikfolgenabschätzung die interdependenten Beziehungen von Technik und Gesellschaft. Dieses Unterfangen benötigt eine interdisziplinäre Vorgangsweise. Kaum ein Gebiet ist von so dynamischer Entwicklung geprägt wie die Informations- und Kommunikationstechnologien. Sie durchdringen immer mehr Lebensbereiche und ermöglichen Arbeitserleichterung und erhöhte Bequemlichkeit ebenso wie zunehmende Überwachung und Kontrolle. Die Dynamik der technischen Entwicklung wurde in den vergangenen Jahren jedoch noch durch die Dynamik im politisch-rechtlichen Bereich überholt. In Folge der Attentate des 11. September 2001 wurde eine Reihe von Initiativen ergriffen, die mehr Sicherheit gewährleisten sollen. Der Preis dafür sind aber allzu oft Einschränkungen individueller Freiheiten.

Vor diesem Hintergrund beschäftigt sich das Institut für Technikfolgen-Abschätzung (ITA) der Österreichischen Akademie der Wissenschaften mit dem gesellschaftlichen Problemfeld „Schutz der Privatsphäre“. Ein wesentlicher Bestandteil der Arbeit ist, die Entwicklung des in Frage stehenden Grundrechts und dessen Bedrohung aus unterschiedlichen Perspektiven zu beleuchten. Im vorliegenden Buch werden die Beiträge der vom ITA zu diesem Zweck veranstalteten internationalen Konferenz „Privacy – Ein Grundrecht mit Ablaufdatum?“ vom 11. November 2002 in Wien dokumentiert. Die Konferenz bot WissenschaftlerInnen aus unterschiedlichen Bereichen sowie PraktikerInnen aus Politik und Zivilgesellschaft ein Forum zum Dialog.

Ausgangspunkt der hier dokumentierten Beschäftigung mit Privacy bildet eine philosophische Begründung des Wertes des Privaten für liberale Gesellschaften. *Herlinde Pauer-Studer* verdeutlicht, wie wichtig individuelle Freiheit und Autonomie für liberale Gesellschaften sind. Die klassische Unterscheidung von Öffentlichem und Privatem beruht für sie auf unterschiedlichen Prinzipien des Zusammenlebens. Die klar strukturierten, rechtsförmigen Beziehungsmuster sind typbildend für Beziehungen im öffentlichen Bereich, in Politik, Recht und Wirt-

schaft. Der private Bereich, die Familie, hingegen ist gekennzeichnet durch Verständnis, Liebe und Zuneigung. Diese Zweiteilung führt zu einer moralisch unterschiedlichen Bewertung der beiden Bereiche. Während im Öffentlichen Rechte, Gerechtigkeit und Reziprozität die moralischen Kategorien sind, ist das Private gekennzeichnet von Empathie, Großzügigkeit und Nachsicht. Diese traditionelle öffentlich-privat Unterscheidung ist wegen der geschlechtsspezifischen Konnotation umstritten: Das Private wird oft den Frauen, das Öffentliche den Männern zugeordnet. Dies mag mit ein Grund für die Benachteiligung von Frauen sein: „Wird die Familie per definitionem mit ‚höheren‘ Zielen als jenem der Gerechtigkeit assoziiert, so erscheinen Fragen nach der gerechten Arbeitsverteilung innerhalb der Familie geradezu als Ausdruck einer kleinlichen, einer moralisch niederen Gesinnung“ (Seite 19). Aus diesem Grund plädiert Pauer-Studer für eine Reformulierung der Kategorien des Privaten und des Öffentlichen. „Es geht um die Bestimmung von ‚öffentlich‘ und ‚privat‘ auf der Basis neutraler Rechtsbeziehungen zwischen Individuen einerseits und zwischen Individuen und staatlichen bzw. gesellschaftlichen Institutionen andererseits“ (Seite 19).

Auf Basis eines autonomiebasierten politischen Liberalismus argumentiert Pauer-Studer im folgenden den Wert des Privaten für die persönliche Freiheit und Autonomie. Persönliche Freiheit ist in diesem Konzept neben der Gleichheit der zentrale Wert und wird dahingehend definiert, dass „Freiheit ... die Fähigkeit [bedeutet], eine autonome Person zu sein, d. h. autonom die Art und Form des Lebens, welches man führen will, zu bestimmen, sofern dies mit der Freiheit von anderen verträglich ist“ (Seite 20). Diese personale Autonomie ist die Basis für weitere Freiheiten, wie etwa politische Freiheit, Meinungs- und Pressefreiheit, Versammlungs- und Religionsfreiheit sowie die Freiheit der sexuellen Orientierung. Diese Freiheiten bedürfen rechtlicher Absicherung, was in den Grundrechtskatalogen europäischer Verfassungen zum Ausdruck kommt. In diesem Kontext von persönlicher Autonomie spielt Privatheit eine wesentliche Rolle: Sie ist sowohl Ausdruck als auch Voraussetzung. „Einem autonomiebasierten Liberalismus gilt der Wert der Privatheit als unverzichtbar“ (Seite 23).

In weiterer Folge zeigt Pauer-Studer, dass auch im Rahmen eines autonomiebasierten Liberalismus Begrenzungen von Privatheit und persönlicher Autonomie argumentiert werden können, ohne sich perfektionistischer Ansätze vom gesellschaftlich Guten und dessen Durchsetzung verpflichten zu müssen.

Wie bereits gezeigt, bedarf die persönliche Freiheit auch der rechtlichen Absicherung. Welche Rechte garantieren nun Privatheit? Wie sind sie entstanden und auf welchen Grundüberlegungen fußen sie? In seiner entwicklungsgeschichtlichen Darstellung der verschiedenen Wurzeln des grundrechtlichen Schutzes der Privatsphäre zeigt *Ewald Wiederin*, dass die Idee der Privatsphäre eine relativ neue Konzept darstellt. Die ersten Grundrechtskodifikationen beschränken sich auf

den Schutz von Wohnung und Briefgeheimnis. Zwei Grundrechte, deren Wurzeln in politischer Freiheit und Freiheit wirtschaftlicher Betätigung liegen. Erst viel später – Ende des 19. Jahrhunderts – trat der Wert der Privatsphäre in der juristischen Diskussion hervor. Bemerkenswert erscheint dabei, dass neben den allgemeinen sozio-ökonomischen Veränderungen, wie etwa der Auflösung der Hauswirtschaft, der Industrialisierung und der damit einhergehenden Ausdifferenzierung von unterschiedlichen Rollen, auch technische Entwicklungen eine nicht unwesentliche Rolle spielten: Warren und Brandeis (1890, 193) argumentierten in ihrem zentralen Aufsatz, dass Entwicklungen der Photographie es möglich gemacht hatten, Bilder intimster Situationen auf den Titelseiten der Zeitung zu platzieren und Fortschritte der Aufnahmetechnik es erlaubten, jedes Flüstern in die Öffentlichkeit zu tragen. Da gegen diese Entwicklungen das Zivilrecht versage, plädierten sie für eine generelle Anerkennung eines Rechts auf Privatheit, das das Recht, allein gelassen zu werden, beinhaltet. Obschon sich diese Ansicht nicht unmittelbar durchsetzte, kann sie als Ausgangspunkt der modernen Diskussion um eine rechtliche Absicherung der Privatheit gelten. Ein weiterer ganz wesentlicher Schritt war die Anerkennung der Privatsphäre in der Allgemeinen Erklärung der Menschenrechte 1948 und in weiterer Folge in der Europäischen Konvention zum Schutz der Grundfreiheiten und Menschenrechte (EMRK). „Im Unterschied zu den klassischen grundrechtlichen Gewährleistungen, die sich auf den Schutz ausgewählter Aspekte beschränkt hatten, räumt Art. 8 EMRK jeder Person einen umfassenden Schutz auf Achtung der Privatsphäre ein, der sowohl die sozialen als auch die räumlichen und die kommunikativen Aspekte auffängt und der in vielen Aspekten über die klassischen Gewährleistungen hinausgeht“ (Seite 49). Die dennoch möglichen Eingriffe in die Privatsphäre bedürfen nach Art. 8 Abs. 2 EMRK einer gesetzlichen Grundlage und sind nur insoweit zulässig, als sie für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl eines Landes, die Verteidigung der Ordnung und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig sind. Für Wiederin stellt diese Materialisierung des Grundrechtsschutzes „ohne Zweifel einen Fortschritt dar. Weil aber die Effizienz einer solchen materiellen Prüfung mit der Bereitschaft der Verfassungsgerichte steht und fällt, sich auf sie einzulassen, ist sie formellen Rechtfertigungsprozeduren nicht schlechterdings überlegen“ (Seite 51). Als Beleg führt er an, dass „Ermächtigungen zu staatlichen Überwachungsmaßnahmen in ganz Europa Prüfungen ihrer Verhältnismäßigkeit nahezu unbeschadet überstanden haben“ (ibid.).

In weiterer Folge zeigt Wiederin, dass auch der in der Menschenwürde wurzelnde Schutz der Privatsphäre Grenzen hat. Es ist also logisch, dass sich im Zuge der Digitalisierung „ein Recht entwickelt hat, auf das sich auch juristische Personen berufen können und das zwar einen Personenbezug, aber keinen Privat-

sphärenbezug verlangt: das Recht auf Datenschutz“ (Seite 53). Dies – so sein Resümee – weise auf einen „Trend in Richtung auf Informationskontrolle“ (Seite 55).

Wie dieses Recht auf Informationskontrolle in privatrechtlicher Hinsicht genutzt wird, welchen Veränderungen es im Laufe der Zeit unterworfen war, analysiert *Andreas Heldrich* in seinem Beitrag. Er spannt dabei den Bogen von der Begründung für die Abweisung von Geldentschädigungen für Beleidigungen am Ende des 19. Jahrhunderts in Deutschland bis hin zu der nunmehr vorherrschenden Rechtsansicht, dass der Persönlichkeitsschutz nicht mit dem Tod des Rechtsträgers ende, sondern vielmehr seine Persönlichkeitsrechte, insbesondere sein Name und sein Bild, auf die Erben übergehen (Seite 67). Diese doch sehr ausgeprägte Veränderung in der Einschätzung des Persönlichkeitsrechtes und der Auswirkungen bei Verletzung desselben fand in knapp hundert Jahren statt. Anhand markanter Gerichtsurteile zeichnet Heldrich diese Entwicklung nach. Wie zu erwarten, verlief diese Entwicklung im Spannungsfeld von prominenten Persönlichkeiten einerseits und kommerziellen Vermarktungsinteressen von Werbung und Presse andererseits. Am Anfang stand die Absicht von zwei Journalisten, Fotos des Leichnams des früheren Reichskanzlers Otto von Bismarck zu verkaufen. Dieser Fall machte deutlich, dass zu dieser Zeit keine entsprechende Regelung des Persönlichkeitsschutzes vorhanden war. Dies führte in weiterer Folge zum Recht am eigenen Bild, geregelt in den §§ 22 ff Kunsturhebergesetz (Seite 61).

Erst nach dem zweiten Weltkrieg gelang der „eigentliche Durchbruch zu einer gewinnbringenden Vermarktung von Persönlichkeitsrechten“ (Seite 62). Diese wiederum steht in Konflikt mit dem ebenfalls grundrechtlich abgesicherten Recht auf Pressefreiheit. Eine weiteres Problem sieht Heldrich in der unterschiedlichen Höhe der zugesprochenen Ersatzleistungen. Wenn für die Veröffentlichung von Bildern im Gebet der Prinzessin Caroline von Monaco 100.000 Euro zugesprochen werden, die Entschädigungen bei Vergewaltigung aber nur bei etwa 5.000 Euro liegen, kann man sich trotzdem „des Eindrucks nicht ganz erwehren, dass die Gerichte hier mit zweierlei Maß messen. Persönlichkeitsverletzungen bei der Verfolgung kommerzieller Interessen durch die Medien wiegen offenbar schwerer als Verletzungen von körperlicher und seelischer Integrität im allgemeinen gesellschaftlichen Zusammenleben“ (Seite 65 f). Dass dies nicht einer Bevorzugung von Prominenten, sondern einer „nicht mehr zeitgemäßen Sichtweise bei der Schadensfeststellung“ geschuldet sei, belegt Heldrich mit der Feststellung, dass die Ökonomisierung unseres Denkens und Handelns einen Grad erreicht habe, der unsere Persönlichkeit verändert hat (Seite 66) und dass erlittenes Leid, wie bei einem Gesundheitsschaden, einer Vergewaltigung etc. in der Tat auch etwas anderes sei als entgangener Gewinn bei der Vermarktung fremder Persönlichkeitsinteressen (ibid.).

Der abschließende Hinweis Heldrichs, dass es in unserer Rechtsordnung dennoch möglich ist, der Kommerzialisierung von Persönlichkeit („Ich-AG“) gewisse Grenzen zu setzen, führt zurück zur Forderung Pauer-Studers, dass „Gesellschaften ..., wenn sie Wert auf Autonomie legen, nicht unbeschränkt Privatheitsverletzungen der Bürgerinnen und Bürger gegen sich selbst zulassen [können]. Denn dies bleibt nicht ohne Folgen für die betroffenen Individuen und den Stellenwert des Rechts auf Privatheit insgesamt“ (Seite 29).

Obwohl unterschiedliche nationale Datenschutzregelungen in die jeweiligen kulturellen und rechtspolitischen Kontexte eingepasst sind, stellt sich bei näherer Analyse heraus, dass die derzeitigen Regelungen mehr Gemeinsamkeiten aufweisen, als auf den ersten Blick anzunehmen wäre. Die Entwicklung der gemeinsamen Grundsätze, der „Fair Information Principles (FIPS)“, zeichnet *Colin Bennett* in seinem Beitrag nach. Die Prinzipien von

- Verantwortung,
  - Zweckbestimmung und Ausschließlichkeit,
  - Zustimmungsverpflichtung,
  - Minimierung von Datenspeicherung in Bezug auf Datenmenge und Speicherdauer,
  - Aktualität, Vollständigkeit und Richtigkeit,
  - Gewährleistung entsprechender technischer Sicherheit,
  - Offenheit und schließlich der
  - Zugang der Datensubjekte zu ihren Daten einschließlich der Möglichkeit zu Richtigstellung, Löschung und Widerspruch zur Datenverwendung
- finden tatsächlich ihren Niederschlag in vielen nationalen wie auch internationalen Regelungen.

Sie dienen in unterschiedlichsten Arenen als Grundlage für jene Aushandlungsprozesse, die allen Privacy-Regimen zugrunde liegen. Als erste internationale Organisation nahm sich der Europarat des Themas an und verabschiedete 1980 die „Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (Treaty 108)“ (Council of Europe (CoE) 1981). In der Zeit von Jänner 1981 bis Dezember 2001 haben 33 der 41 Mitgliedsstaaten des Europarates die Konvention unterzeichnet, 25 haben sie auch ratifiziert (Seite 75). Nahezu zeitgleich wurden die ökonomischen Auswirkungen unterschiedlicher Datenschutzpolitiken auf transatlantische Handelsbeziehungen thematisiert. Die Arena dazu bildet die Organisation für Zusammenarbeit und Entwicklung (OECD). In langen Verhandlungen wurden die „Guidelines on the Protection of Personal Privacy and Transborder Flows of Personal Data“ (OECD 1980) entwickelt. Ihnen folgten 1992 die Guidelines on „Security of Information Systems“ (OECD 1992) und 1997 die „Guidelines for Cryptography Policy“ (OECD 1997). Mit dem Aufkommen des e-Commerce in den 1990er Jahren veränderte sich auch die Sicht-

weise auf das Privacy-Problem. Während in den 1970er Jahren die Angst vor dem Großen Bruder Staat und seinen zentralistischen Großrechenanlagen im Vordergrund der Diskussion standen und dementsprechend große Anstrengungen bezüglich legislativer Aktivitäten erfolgten, wurde – wohl auch der technischen Entwicklung mit Miniaturisierung und Vernetzung wegen – deutlich, dass nur ein Maßnahmenbündel aus gesetzlichem Rahmen, Selbstregulationsmechanismen, Privacy Enhancing Technologies und Bewusstseinsbildung notwendig ist. Insbesondere interessant erscheint die veränderte Einschätzung wonach Datenschutz weniger ein Handelshemmnis darstellt, als vielmehr eine notwendige Bedingung dafür ist, dass KonsumentInnen öffentliche Netzwerke für geschäftliche Transaktionen nutzen (Seite 78). Da die OECD Guidelines keinerlei bindenden Charakter haben, blieb eine unübersichtliche und heterogene Landschaft an Datenschutzregelungen bestehen. Dies wurde zunehmend als Hemmnis für den zu gestaltenden gemeinsamen Markt in der Europäischen Union erkannt, was nicht unwesentlich zur weiteren Entwicklung beitrug. „Data protection had ceased to be merely a human rights issue; it was also intrinsically linked to the operation of international trade. The result was by far the most influential international policy instrument to date: the Directive on Personal Data with Regard to the Processing of Personal Data and on the Free Movement of such Data (Europäische Union 1995)“ (Seite 78 f). Die EU-Datenschutzrichtlinie stellt in der Tat einen wesentlichen Durchbruch dar. Sie harmonisiert nicht nur die Datenschutzgesetzgebung in der EU, sie entfaltet auch Außenwirkungen, indem sie den Export von Daten an ein angemessenes Schutzniveau bindet. Dies führte zum so genannten „Safe Harbour“-Abkommen zwischen den USA und der EU, in dem sich US-amerikanische Firmen, die mit Partnern in der EU personenbezogene Daten austauschen wollen, freiwillig den Grundsätzen der Richtlinie unterwerfen. Die Überprüfung der Einhaltung dieses Abkommens ist jedoch immer wieder Gegenstand von Diskussionen, weswegen öfters auch alternative Modelle diskutiert werden. Ein Weg wäre, die internationalen Standardisierungsgremien und ihre Methoden der Zertifizierung zu nutzen. Ob dies allerdings tatsächlich jemals der Fall sein wird, kann nicht prognostiziert werden (Seite 84).

Aus einer wesentlich weiteren Perspektive nähert sich *David Lyon* dem Problem. Seiner Ansicht nach, ist eine ausschließlich der Privatheit geschuldete Aufmerksamkeit zu eng. Ohne die Wichtigkeit von Privacy zu unterschätzen meint er dennoch: „It’s just that to focus on privacy alone seriously misses the mark of current challenges of surveillance“ (Seite 91). Was sind nun die zentralen Herausforderungen? Sie liegen in den gesellschaftlichen Veränderungen, die einerseits durch technische Entwicklungen wie durchsuchbare Datenbanken und deren Vernetzung erleichtert, aber auch durch die politischen Folgen der Attentate des 11. September beschleunigt wurden. Am Beispiel der amerikanischen Total

Information Awareness Initiative zeigt er auf, wie sehr sich Überwachung bereits integriert hat, und vor allem, was geplant ist. Öffentliche und private Datenbanken werden integriert, Informationen aus unterschiedlichsten Kontexten zusammengeführt und zur Erstellung von Profilen genutzt. Diese sehr weit reichenden Aktivitäten in den USA führen nach Lyon dazu, dass „[t]he surveillance state expanded to become the surveillance society“ (Seite 95). Die besondere Problematik liegt darin, dass durch die vorgegebenen Kriterien eine soziale Diskriminierung von Bevölkerungsgruppen entsteht, die völlig vom Verwertungsinteresse der überwachenden und Daten sammelnden Organisation abhängen. Die Definition der Selektionskriterien und damit auch die Zuschreibung von Eigenschaften ist dem Einfluss der Datensubjekte völlig entzogen. Damit bestimmen andere, welche Teilaspekte einer realen Persönlichkeit Teil der elektronischen Persönlichkeit werden und welche Teile davon, mit welcher Gewichtung, in die Bewertung dieser elektronischen Persönlichkeit eingehen. Die Überwachungssituation hat sich auch deshalb geändert, weil durch die automationsunterstützte Überwachung flächendeckende und permanente Überwachung möglich wurde. Früher hat sich Überwachung meist auf spezielle Daten oder besondere Aktivitäten bezogen. Heute verlieren alle Datensubjekte ihre Unschuld „... and we all enter a more ‚fishbowl‘ like world where our business is open to the scrutiny of others“ (Seite 97). Überwachung findet demgemäß nicht mehr statt, weil jemand etwas Abweichendes getan hat, sondern alle hinterlassen bei alltäglichen Verrichtungen elektronische Spuren, die sich zur Überwachung eignen. Durch die so generierten Profile wird Bevorzugung und Ausschluss von Leistungen möglich. Diese aus dem Marketing bekannten Prozesse werden zunehmend auf staatliche Sicherungsaufgaben übertragen, was zur Diskriminierung ganzer Bevölkerungsgruppen führen kann.

Es sind aber nicht nur die neuen Technologien, die für diese Entwicklung verantwortlich sind. Gesellschaftliche Trends, die Garland (2001, zit. Seite 100) die „new culture of crime control“ nennt, sind zumindest ebenso wichtig. Garland konstatiert eine Veränderung in den Erklärungsmustern für Kriminalität. Während früher die Wurzeln von Kriminalität oft in sozialen Lebensbedingungen gesehen wurden, und ein wesentliches Ziel die Umerziehung und Re-Integration von Straftätern war, beherrschen nun neue Ansätze die Diskussion. Darin wird vor allem Wert darauf gelegt, in verschiedenen sozialen Situationen die Möglichkeiten für kriminelle Handlungen zu minimieren. Parallel dazu hat sich auch die Einstellung Straftätern gegenüber geändert: Sie verdienen ihre Strafe und können nicht erwarten verstanden zu werden. Insgesamt eine eher ökonomisch orientierte, denn soziale Sichtweise. In diesem Sinne ist auch zu verstehen, dass Sicherheit zu einer Ware wird, für die bezahlt werden muss. Im Sinne effizienter Abläufe passen die neuen Überwachungstechnologien perfekt in dieses Szenario.

Wie bereits weiter oben ausgeführt, ist es in der internationalen Privacy-Diskussion mittlerweile Konsens, dass nur ein Bündel von Maßnahmen den Bedrohungen der Privatheit gerecht werden kann. Ein junger, aber wichtiger Zweig dabei ist „Datenschutz durch Technik“. Ein wesentlicher Akteur in dieser Arena ist *John Borking*. In seinem Beitrag stellt er grundlegende Anforderungen an technischen Datenschutz dar. Basierend auf den anerkannten Prinzipien, wie sie auch Bennett in seinem Paper dargestellt hat, erläutert Borking wie diese Prinzipien in technische Systeme integriert werden können und stellt dabei die einzelnen Schritte detailliert dar. Die beschriebene Vorgangsweise reicht von der Risikoanalyse über die „Privacy Impact Analysis (PIA)“ bis zum Einsatz eines Privacy Diagnostic Tools (PDT) und führt weiter zur Vorstellung von Privacy Enhancing Technologies (PET). Ein wesentlicher Ansatz hierbei ist der „Identity Protector“. Dabei wird ein informationstechnisches System derart gestaltet, dass personenbezogene Daten von Nutzungsdaten getrennt werden, sodass eine Zuordnung nur nach bestimmten Regeln und unter Zuhilfenahme des Identity Protectors möglich ist. Die zentralen Strategien bei der Entwicklung von PETs sind erstens die Verhinderung von Identifikation unter Berücksichtigung des Aufwandes, der getrieben werden muss, um bestehende Sicherheitsschranken zu überwinden; und zweitens die Verhinderung unrechtmäßiger Datenverarbeitung. Die allgemeinen Grundlagen illustriert Borking anschließend anhand eines realisierten Spitalsverwaltungssystems. Besonders interessant ist hierbei, dass die Kosten für die datenschutzfreundliche Variante nur ein Prozent höher lagen als bei der Gestaltung eines herkömmlichen Systems (Seite 129). Es zeigt sich, dass bei frühzeitiger Integration der PET-Ideen das Kostenargument nicht zur Abwehr von Datenschutzanliegen taugt.

Vielmehr deutet sich damit ein Weg an, der auch von NutzervertreterInnen als viel versprechend angesehen wird. Der Ökonomisierung personenbezogener Daten kann nur mit der Ökonomisierung des Datenschutzes (Seite 150) begegnet werden. Die Frage, der *Thilo Weichert* in seinem Beitrag nachgeht, ist nun, wie diese Ökonomisierung des Datenschutzes am erfolgsversprechendsten realisiert werden könnte. Der Wunsch der KonsumentInnen nach mehr Datenschutz konnte sich bisher marktmäßig noch nicht durchsetzen. Die deshalb geforderte Regulierung des Marktes bedarf aber handlungsfähiger und unabhängiger Aufsichtsbehörden. Der zentrale Ansatz sollte darin bestehen, den KonsumentInnen mehr Marktmacht zu geben. Um dies zu erreichen, steht an erster Stelle die Forderung nach mehr Transparenz: Ebenso wie der Produzent von Lebensmitteln verpflichtet ist, sämtliche Inhaltstoffe seiner Waren offenzulegen, muss die Bank, das Versicherungsunternehmen oder der Versandhändler verpflichtet werden, präzise anzugeben, welche Informationen er über die KundInnen sammelt und wie er diese verarbeitet (Seite 148 f). Weiters sollte von der grundsätzlich anonymen Kundenbezie-

hung ausgegangen werden und ein generelles Datenerhebungsverbot eingeführt werden. Ausnahmen bedürften dann der ausdrücklichen Zustimmung der KonsumentInnen. Unternehmen, die eine nicht genehmigte Datenverarbeitung durchführen, müssten dann mit Schadenersatzforderungen aber auch mit Ansprüchen aus ungerechtfertigter Bereicherung rechnen. Damit wäre eine wesentliche Forderung erfüllt: Die möglicherweise zu erwartenden Kosten für Datenschutzverletzungen würden wesentlich höher werden und Datenschutzverletzungen würden durch das ökonomische Kalkül damit unattraktiver. Eine andere Schiene in der Ökonomisierung des Datenschutzes stellt die positive Kommunikation von Datenschutz als Qualitätsmerkmal dar. Dazu bedarf es einiger Orientierungshilfen für die KonsumentInnen. Ein Beispiel dafür können Datenschutz-Audits und Gütesiegel sein. Bei den Gütesiegeln sollte jedoch darauf geachtet werden, dass es nicht zu einer Inflation an Gütesiegeln kommt (Peissl 2003).

Im abschließenden Beitrag gibt *Walter Peissl* einen Überblick über Privacy in Österreich. Ausgangspunkt dabei ist die Einschätzung der Problemlage aus Sicht der Technikfolgenabschätzung. Sowohl technische Entwicklungen als auch – nach dem 11. September 2001 besonders stark – politisch-gesellschaftliche Entwicklungen üben Einfluss auf die Privatsphäre aus. Vor dem Hintergrund der legislativen Entwicklungen der letzten Jahre wird dabei untersucht, ob ein Mehr an Überwachung auch tatsächlich zu einem Mehr an Sicherheit führt. Darüber hinaus werden aber auch andere Bedrohungen der Privatsphäre in der Informationsgesellschaft ausgemacht. In einem ersten Schritt ist zu klären, in welchen wirtschaftlich-gesellschaftlichen Zusammenhängen die dichtesten Datenspuren anfallen, welche Akteure über die größten Datenbestände mit hoher Datentiefe verfügen und welche Anwendungen die Privatsphäre bedrohen. War in den Anfängen der Datenschutzdiskussion vor allem der alles wissen und speichern wollende Staat die Hauptbedrohung für den Einzelnen, so hat sich mittlerweile auch im privaten Bereich ein nicht zu unterschätzendes Interesse für personenbezogene Daten entwickelt. Neben den Finanzdienstleistern und Versicherungsunternehmen sind es vor allem die Unternehmen der Telekommunikationsbranche, die durch die Art der Dienstleistung umfangreiches Wissen über ihre KundInnen generieren. Aus den unterschiedlichen Bedrohungsszenarien werden Vermeidungsstrategien abgeleitet und Handlungsempfehlungen gegeben. Eine hervorragende Rolle nimmt dabei die Datenvermeidung ein. Sie ist und bleibt ein wesentlicher Bestandteil modernen Datenschutzes. Zu prüfen ist jedoch, inwieweit der Einzelne überhaupt in der Lage ist, die Empfehlungen umzusetzen. Es zeigt sich, dass man auf individueller Ebene sehr schnell an Grenzen stößt und die Empfehlungen schwer umsetzbar sind. Deshalb ist auch in Zukunft neben der individuellen Verantwortung gesetzliche Rahmensetzung notwendig.

Wie die Beiträge dieses Bandes zeigen, ist das Grundrecht auf Privatsphäre aus unterschiedlichen Wurzeln entstanden, hat sich im Laufe der Zeit verändert und unterliegt auch weiterhin mannigfachen Einflüssen. Dass Individuen Rückzugsmöglichkeiten benötigen und dass liberale Gesellschaften ohne gesicherte Freiräume für ihre Mitglieder ihr Wesen verändern, kann ebenso gezeigt werden, wie Möglichkeiten den Bedrohungen positiv entgegenzutreten. Aus der Position eines technischen Determinismus müsste aufgrund der hohen Dynamik in den Bereichen Informations- und Kommunikationstechnologien und Biotechnologie dem Grundrecht auf Privatsphäre wohl ein baldiges Ablaufdatum zugeschrieben werden. Da aber technische Innovationen nicht einer technischen Eigenlogik allein entspringen, sondern durch den gesellschaftlichen Kontext mitgeformt werden, liegt es auch an EntscheidungsträgerInnen in Wissenschaft, Politik und Wirtschaft sowie bei VertreterInnen der Zivilgesellschaft, ob das Grundrecht auf Privatsphäre tatsächlich ein Ablaufdatum hat. Dieses Buch soll ein Beitrag zu dieser gesellschaftlich notwendigen Diskussion sein.

## LITERATUR

- Council of Europe (CoE), 1981, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108)*, Strasbourg.
- Europäische Union, 1995, Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, *Amtsblatt nr. L 281 23/11/1995*, 31–50 <[http://europa.eu.int/eur-lex/de/lif/dat/1995/de\\_395L0046.html](http://europa.eu.int/eur-lex/de/lif/dat/1995/de_395L0046.html)>.
- Garland, D., 2001, *The Culture of Control: Crime and Social Order in Contemporary Society*, Chicago: University of Chicago Press.
- OECD, 1980, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 23 September 1980 <[http://www.oecd.org/document/20/0,2340,en\\_2649\\_33703\\_15589524\\_1\\_1\\_1\\_37409,00.html](http://www.oecd.org/document/20/0,2340,en_2649_33703_15589524_1_1_1_37409,00.html)>.
- OECD, 1992, *Guidelines for the Security of Information Systems*, Paris: <[http://www.oecd.org/document/19/0,2340,en\\_2649\\_34255\\_1815059\\_119820\\_1\\_1\\_37409,00.html](http://www.oecd.org/document/19/0,2340,en_2649_34255_1815059_119820_1_1_37409,00.html)>.
- OECD, 1997, *Guidelines for Cryptography Policy*, Paris: <[http://www.oecd.org/document/11/0,2340,en\\_2649\\_34255\\_1814731\\_119820\\_1\\_1\\_37409,00.html](http://www.oecd.org/document/11/0,2340,en_2649_34255_1814731_119820_1_1_37409,00.html)>.
- Peissl, W., 2003, E-commerce: Nutzungsbarrieren aus KonsumentInnensicht, in: Mayer, G. (Hg.): *Konsumentenpolitisches Jahrbuch 2000-2001*, Wien, 9–34.
- Warren, S. D., Brandeis, L. D., 1890, The Right to Privacy, *Harvard Law Review IV (5)*, 193 ff.