

Nach 9/11 – Die Zukunft des Datenschutzes

*Max Mosing**

*dzt Strathclyde University, Glasgow, Scotland**
mosing@it-law.at*

Schlagworte: Datenschutz, Geschichte, richtlinienwidrige Datendefinition, Paradigmenwechsel, Datenhandel, ZMR, CCTV, Total Information Awareness, IPv6, e-CommunicationRL, Privacy

Abstract: Datenschutz ist ein gewichtiger Teil der Informationsgesellschaft: (Personenbezogene) Daten sind allgegenwärtig. Die Pflichten treffen den Staat gleichermaßen wie den nichtstaatlichen Datenverarbeiter. Zielt die e-CommunicationRL verstärkt auf den privaten Bereich ab, zeigen die Entwicklungen nach 9/11th, wie wichtig es ist, den Staat als Datenverarbeiter nicht aus den Augen zu verlieren (vgl idZ die mögl RL-widrigkeit des österr Datenbegriffs): Staatlicher Datenhandel, Videoüberwachung udgl. Die e-CommunicationRL scheint eine Ausdehnung des Anwendungsbereichs des Datenschutzrechts hin zum Recht auf Privatheit einzuläuten.

1. Vorbemerkungen

Ziel des vorliegenden Beitrages ist es, dass auf Basis der faktisch-gesellschaftlichen und legislativen Entwicklungen das Datenschutzrecht in einem (beinahe) globalen Zusammenhang gesehen wird: Durch das Spannen von weiten ([rechts]politischen) Bögen und das Aufstellen von sich daraus ergebenden Thesen soll der Beitrag als (aufgrund der Umfangsbeschränkung – kurze) Anregung dienen, den Datenschutz als (gewichtigen) Teil des großen Ganzen der Informationsgesellschaft zu sehen

2. Thesen

Datenschutzrecht ist ein „dankbares rechtstheoretisches Thema“: Erstens ist es auf einem Level der Abstraktheit angesiedelt, der nicht nur für den Laien schwer fassbar ist; die typische österr Frage „Für was brauch’ ma denn das?!“ wird in keinem juristischen Bereich öfters gestellt. Zwei-

* Ein Lebenslauf des Autors findet sich unter <http://www.it-law.at/papers/cv/mosing.pdf> (1.4.2003).

** Der Autor bedankt sich an dieser Stelle bei *Christina Sofokleous* für die Anregungen.

tens ist das Datenschutzrecht von einer solchen Komplexität und gleichzeitig von einer solchen Ubiquität, dass man leicht dazu hingerissen ist, (rechts)politische Stellungnahmen abzugeben.¹ Drittens ist es (größtenteils) „rechtstheoretisch“, weil das Datenschutzrecht trotz der unter zweitens erwähnten Umstände von unterdurchschnittlicher praktischer Relevanz zu sein scheint.

2.1. These: Niemand will (ernsthaft) Datenschutz

Francis Bacon sagte, „Knowledge, of itself, is power“. Diese Wahrheit wurde mit der Informationsgesellschaft zu einem „Information is power“² und durch die weltweite Vernetzung immer mehr zu einem „Data, of itself, is power“: Aus unbedeutenden Einzeldaten kann in Netzwerken (strukturierte) Information (über Einzelpersonen) gebildet werden, die durch Ausfilterung nach gewünschten Kriterien zu einem detaillierten Wissen von ungeahntem Ausmaß führen kann (Stichwort: „knowledge-based economies“):³ In den 60ern versprach ein US-Ice-Cream-Unternehmen Kunden an ihrem 18ten Geburtstag einen Gutschein für Ice-Cream und Tausende gaben ihre Daten bekannt; als der Vietnam-Krieg begann, nutzte das US-Militär die Daten zum Abgleich mit ihren Registrierungslisten. Oder: Vor dem II. Weltkrieg wurde in den Niederlanden eines der ersten staatlichen Register eingeführt, das ua die Religion jedes Bürgers verzeichnete; als die Deutschen einrückten, bedienten sie sich des Registers um die jüdische Bevölkerung zu identifizieren. Dennoch scheint niemand ernsthaft am Datenschutz interessiert zu sein:

- Die Wirtschaft sieht sich durch den Datenschutz in ihrer „Erwerbsfreiheit“ eingeschränkt: Daten können direkt⁴ und indirekt⁵ zu Geld gemacht werden; „Data, of itself, is money“.
- Der Konsument bzw Bürger hat meist den „Ich-Habe-Ja-Nichts-Zu-Verbergen-Zugang“ zum Datenschutz: Solange er einen Profit zu erhalten glaubt, ist er bereit, jegliche Daten bekannt zu geben. So hat ein bekannter österr Datenschützer vor einiger Zeit den Autor gefragt: „Was wollen Sie: Bequemlichkeit oder Datenschutz?!“ Der Konsument bzw

¹ Vgl ARGE DATEN – Österreichische Gesellschaft für Datenschutz: <http://www.ad.or.at/news/> (1.4.2003).

² Vgl *Ian J Lloyd*, *Information Technology Law*³ (Butterworths, 2000) xxxvii.

³ Bsp von *Suelette Dreyfus*, *Underground* (Random House Australia, 1997) <http://www.underground-book.com/chapters/lotef/privacy.html> (1.4.2003).

⁴ Von Adressen bis hin zu ausgearbeiteten Profilen zu fast allen erdenklichen Themen werden gehandelt.

⁵ Von dubiosen Spammern über riesige Handelsketten bis hin zur Politik werden Daten für Marketing, Produktentwicklung und andere Strategien genutzt.

Bürger scheint § 1 DSG 2000,⁶ der einzigartig ein Grundrecht mit unmittelbarer Drittwirkung normiert, nicht „zu würdigen“.

- Der (sicherheits)politische Zugang zum Datenschutz war und ist zweischneidig: Der „Programmparagraph“ § 1 DSG ist vorgegeben, auf der anderen Seite sind Auskunftspflichtgesetze⁷ zu beachten und den Sicherheitsbehörden, die nur ungern die durch den Datenschutz vorgegebenen Grenzen beachten (vgl §§ 6 ff DSG), (umfassende) Rechte gewährt.⁸ Das bringt, nach *Menasse*, eine „[...] Entwicklung, die zu unkontrollierbaren Polizeibefugnissen, zu Lauschangriff, und Rasterfahndung und bei der kleinsten Unruhe zur hysterischen Jagd auf Sündenböcke führt [...]“.⁹ Es ist daher nicht verwunderlich, dass nach dem EKIS¹⁰-Skandal anstatt des Überdenkens des Zugangs zu „staatlichen Daten“ zu einem immer breiteren Zugang kommt (vgl Punkt 2.4).¹¹

2.2. These: Österr Datenbegriff RL-widrig

Trotz der obgenannten „Beliebtheit“ wurde relativ früh erkannt, dass unterschiedliche Datenschutzstandards dem internen EU-Markt abträglich sein können und die DatenschutzRL¹² erlassen. Zentraler Begriff ist dabei „personenbezogenen Daten“, der in Art 2 lit a DatenschutzRL als „alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person““ definiert wird. Das österr DSG 2000 definiert „Daten“ bzw „personenbezogene Daten“ zwar in § 4 Z 1 leg cit richtlinienkonform doch schränkt es die Anwendbarkeit des Gesetzes in § 1 leg cit dadurch ein, dass nur die „Geheimhaltung der [...] personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht“ Gegenstand ist. Das Erfordernis findet sich in der DatenschutzRL nicht. Nach dem *Effet*

⁶ BG über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000) BGBl I 1999/165 idF BGBl I 2001/136.

⁷ BG vom 15. Mai 1987 über die Auskunftspflicht der Verwaltung des Bundes und eine Änderung des Bundesministeriengesetzes 1986 (Auskunftspflichtgesetz) BGBl 1987/287 idF BGBl I 1998/158 und Bundesgrundsatzgesetz vom 15. Mai 1987 über die Auskunftspflicht der Verwaltung der Länder und Gemeinden (Auskunftspflicht-Grundsatzgesetz) BGBl 1987/286 idF BGBl I 1998/158.

⁸ Vgl insb § 7 Abs 1 DSG, der eine Verarbeitung von Daten nur bei rechtlicher Befugnis (wohl nach der gesamten Rechtsordnung) UND Nichtverletzung der schutzwürdigen Geheimhaltungsinteressen zulässt.

⁹ *Robert Menasse*, Erklär mir Österreich (Suhrkamp, 2000) 13.

¹⁰ EKIS (= Elektronisches kriminalpolizeiliches Informationssystem): <http://www.bmi.gv.at/ekis/> (1.4.2003).

¹¹ Vgl *Karl Kollmann*, Eintrittskarte für Datenmissbrauch, <http://www.heise.de/tp/deutsch/inhalt/te/4320/1.html> (1.4.2003)

¹² RL 95/46 vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr AB L 1995/281, 31.

Utile ist bei staatlicher Datenverarbeitung der Anwendungsumfang der DatenschutzRL unmittelbar anzuwenden; bei Schäden, die durch nicht-staatliche Verarbeitung und durch den beschränkten Anwendungsbereich des G entstehen, kommt die Staatshaftung in Betracht.¹³

2.3. These: Paradigmenwechsel im Datenschutz nach 9/11: „Back to the Roots“

Das Datenschutzrecht ist eine relativ junge Disziplin, doch hat diese bereits mehrere Paradigmenwechsel durchlebt:

1970 wurde im deutschen Bundesland Hessen das weltweit erste DatenschutzG¹⁴ erlassen. Hintergrund war das in den 60igern begonnene Einrichten von staatlichen Rechenzentren. Die Angst vor der „Informationsmacht“ staatlicher „Supercomputer“ führte zur Überzeugung, dass Datenschutzrecht die Datenverarbeitung begleiten müsse, um die Machtbalance zwischen Bürgern und Staat zu gewährleisten, ohne den Nutzen der Datenverarbeitung a priori zu verunmöglichen: *George Orwell's* „Big Brother“¹⁵ und die Angst vor der Zentralisierung von Information.

In den 70ern wurde klar, dass vor allem die Vernetzung von Daten die Balance aus dem Gleichgewicht bringen könnte. Das Datenschutzrecht zielte auf die Regelung des staatlichen Netzwerkes, der „Big Family“, ab.

In den 90ern wurde auch der „Little Sister“ – den privaten Datenverarbeitern – eine verstärkte Beachtung zgedacht. In Österreich wurde schon mit dem § 1 DSG 1978¹⁶ normiert, dass *jedermann* gegenüber *jedermann* Anspruch auf Datenschutz hat.

Für die „Little Sister“ sind Kundendaten zu einem wertvollen Gut geworden, das für Marketing und „Customer Relationship Management“ eingesetzt wird. Die Daten sind den Unternehmen auch bares Geld wert: Loyalty Cards (Kundenkarten) gewähren Rabatte und Geschenke im Gegenzug zur Preisgabe nicht unbeachtlicher Daten. Auch in diesem Bereich brachte die Vernetzung Gefahren, wie die „nectar card“¹⁷ im Vereinigten

¹³ Vgl allg *Öhlinger/Potacs*, Gemeinschaftsrecht und staatliches Recht: Die Anwendung des Europarechts im innerstaatlichen Bereich² (Orac, 2001).

¹⁴ LG vom 7.10.1970, Datenschutzgesetz, GVBl I 1970/41.

¹⁵ *George Orwell*, 1984 (*Harcourt Brace Jovanovich*, 1949).

¹⁶ Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten (Datenschutzgesetz – DSG) BGBl 1978/565.

¹⁷ Der Supermarkt *Sainsbury's* gibt gemeinsam mit *Barclaycard*, der führenden Kreditkarte in den UK, *Debenhams*, einem führenden Warenhaus, und *British Petrol* (BP) eine gemeinsame Kundenkarte („nectar card“) aus.

Königreich (fiktiv) zeigen soll:¹⁸ Ein Kunde von *Sainsbury's* kauft täglich 2 Flaschen Wein und tankt wöchentlich bei BP überdurchschnittlich viel Benzin; aufgrund der Daten von *Debenhams* ist anzunehmen, dass der Betroffene zwei Wohnsitze in einigen Kilometern Entfernung hat. Als der Betroffene seinen Kreditrahmen bei der *Barclaycard* erweitern will, wird er ohne Erklärung abgelehnt; tatsächlich war dem Kreditkartenunternehmen das Risiko der Verunfallung im betrunkenen Zustand mit dem PKW zwischen den Wohnsitzen zu groß.

Nach dem Anschlag vom 11.9.2001 auf das *World Trade Center* (WTC) und nach der anfänglichen Blendung durch die „Global Coalition Against Terrorism“¹⁹ besonnen sich Datenschützer zu einem „back to the roots“: Der Datenschutz wollte primär die „Informationsmacht“ des Staates kontrollieren.

2.4. These: Threats – der Staat: Datenhandel, CCTV und Awareness

Nach der Volkszählung 2001²⁰ und der Errichtung eines Zentralen Melderegisters (ZMR)²¹ wurde eine „Support-Unit ZMR“ ins Leben gerufen, welcher die Vermarktung der Meldedaten zukommt:²² Sog „Businesspartner“ können ins ZMR Einsicht nehmen. Auch wenn nach § 16a Abs 5 MeldeG²³ eine „[...] Abfrage im konkreten Fall nur für die glaubhaft gemachten Zwecke erfolgen darf [...]“, soll die „Support-Unit“ als Wirtschaftseinheit die bereits erzielten Einnahmen im Jahr 2002 von rund 700.000 € steigern, was die Angst des „Ausverkaufs des Datenschutzes“ schürt.²⁴ Dieses Bsp zeigt, dass es nicht nur eines (EKIS-)Skandals bedarf, um „staatliche Daten“ in „ungeahnten Händen“ zu finden. Dieses Faktum sollte mE dazu führen, die steigende Datenerfassung im täglichen Leben mit Argusaugen zu verfolgen: e-Bürgerkarte, e-Government und die (präventive) Überwachung. Vor dem Hintergrund der internationalen

¹⁸ Vgl <http://www.sainsburys.co.uk>; <http://www.sainsburys.co.uk>; <http://www.barclaycard.co.uk>; <http://www.debenhams.com>; <http://www.bpplus.com>; <http://www.nectar.com> (alle: 1.4.2003).

¹⁹ Vgl Diplomacy and the Global Coalition Against Terrorism, <http://www.state.gov/coalition> (1.4.2003).

²⁰ Vgl <http://www.statistik.at/gz/vz.shtml> (1.4.2003).

²¹ Vgl <http://zmr.bmi.gv.at> (1.4.2003).

²² V BMI über die Bestimmung der Support-Unit Zentrales Melderegister (ZMR) als Organisationseinheit, bei der die Flexibilisierungsklausel zur Anwendung gelangt BGBl II 2003/20.

²³ BG über das polizeiliche Meldewesen (Meldegesetz 1991 – MeldeG) BGBl 1992/9 idF BGBl I 2001/98.

²⁴ [Http://futurezone.orf.at](http://futurezone.orf.at), Streit um kommerzielle Meldedatennutzung, vom 7.2.2003.

Rechtsinstrumente²⁵ zum Schutz des Privatlebens ist vor allem das Aufkommen von staatlichen (und privaten)²⁶ CCTVs (Closed Circuit TV – Videoüberwachung) zu beachten; am 17.2.2003 wurde im Innenstadtbereich von London ein System in Betrieb genommen, das gleichzeitig Mautsünder anhand der Nummerntafeln, aber auch Kriminelle durch Gesichtserkennung (Biometrie) identifizieren kann.²⁷ Im Herbst zuvor hat sich BMfl *Strasser* ebendort über CCTVs informiert und plant eine Aufstockung der bereits 160.000 in Ö im Einsatz befindlichen Kameras²⁸ – auch wenn die Rechtslage idZ zumindest unklar ist.²⁹ Welche Auswirkungen eine flächendeckende Videoüberwachung hat, zeigt *Orewell's* allgegenwärtiger „tele-screen“.

IdZ sei auf die nach dem 9/11th gestartete „Information Awareness“ hingewiesen: US-Behörden wurden mit der Überwachung der Infrastruktur (ua den Kommunikationsnetzen) beschäftigt (zB Department of Homeland Security, Terrorist Threat Integration Center [TTIC] und va die DARPA Information Awareness Office [IAO]).³⁰ Der US-Senat hat dem Pentagon-Project „Total Information Awareness (TIA)“ schließlich das Budget von US\$ 240 Mio nicht gewährt,³¹ doch könnte gefragt werden, warum man sich eigentlich dem Parlament „unterwerfen“ wollte, wenn man Identisches durch die Geheimdienste bewerkstelligen kann. Auch die EU steht der Überwachung nicht nach: Die „European Network and Information Security Agency“ erhält € 33 Mio bereitgestellt.³²

2.5. These: Führen neue Technologien zu weiterem Paradigmenwechsel?!

„The problem, however, is not so much technology. The TCP/IP [...] are essentially neutral.“³³ *Lessig* zeigte aber auf, dass der Code das eigent-

²⁵ Vgl *Europ Kommission, Art 29 – Datenschutzgruppe*, Arbeitsdokument zum Thema Verarbeitung personenbezogener Daten aus der Videoüberwachung 11750/02/DE, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp67_de.pdf (1.4.2003).

²⁶ Während nach Art 3 Abs 2 DatenschutzRL die RL weder auf den Bereich der öffentlichen Sicherheit noch auf ausschließlich persönliche oder familiäre Tätigkeiten Anwendung findet, ist das beim DSG sehr wohl der Fall (vgl zu privaten Zwecken aber § 45 DSG).

²⁷ *Heise online-Newsticker*, Verkehrsüberwachung mit integrierter Gesichtserkennung, <http://www.heise.de/newsticker/data/wst-10.02.03-002> (1.4.2003).

²⁸ In den UK wird man täglich 200 Mal von CCTV erfasst: *Lloyd*, *Information Technology Law*³, 35.

²⁹ <http://futurezone.orf.at>, 160.000 Kameras überwachen Österreich, vom 15.1.2003.

³⁰ Vgl *Sciencia Est Potentia*, <http://kai.iks-jena.de/miniwahr/tias-iao.html> (1.4.2003).

³¹ <http://futurezone.orf.at/futurezone.orf?read=detail&id=141800> (1.4.2003).

³² Vgl http://europa.eu.int/information_society/eeurope/index_en.htm (1.4.2003).

³³ *Lloyd*, *Information Technology Law*³, 32.

liche Gesetz im Internet ist,³⁴ und selbst die Wertneutralität des TCP/IP hat sich seit IPv6 (lebenslang und uU mit geographischen Angaben) verdünnt.³⁵ Technik ist nicht mehr (datenschutzrechtlich) wertneutral. Der Gesetzgeber muss auf Erscheinungen, wie Spamming,³⁶ Protokollierung von Log-files, Cookies, Web-bugs, location based services (LBS) udgl reagieren.³⁷ Auf EU-Ebene geschah das zT mit der e-CommunicationRL.³⁸ Die e-CommunicationRL soll gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft gewährleisten (Art 1 der RL). Doch das Recht auf Privatsphäre (Privacy: „the right to be left alone“)³⁹ ist ähnlich wie der Schutzzumfang der Datenschutz-Ge⁴⁰ in den Mitgliedsstaaten uneinheitlich; weiters ist es gerade im Bereich der elektronischen Kommunikation geradezu unmöglich, Daten mit von Daten ohne Personenbezug zu unterscheiden.⁴¹ Das könnte ein Grund sein, warum die e-CommunicationRL sich vom Personenbezug weg- und zu einem generellen Schutz der Privacy hinzubewegen scheint (vgl Definitionen in Art 2 der RL, die nur von „Daten“ sprechen; iZm Cookies udgl spricht Art 5 Abs 3 der RL nur von „Informationen“).⁴² Ob sich daraus ein genereller Trend zur Vereinheitlichung der Rechte auf Privatheit durch DatenschutzGe entwickeln wird, bleibt abzuwarten.

³⁴ Lawrence Lessig, Code and Other Laws of Cyberspace (Basic Books, 2000).

³⁵ Vgl *Europ Kommission, Art 29 – Datenschutzgruppe*, Stellungnahme 2/2002 über die Verwendung eindeutiger Kennungen bei Telekommunikationsendeinrichtungen: das Beispiel IPv6, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp61_de.pdf (1.4.2003).

³⁶ Vgl zu Details *Max W. Mosing*, Spamming: Werbung bzw Massensendung per elektronischer Post, in: *IT-LAW.AT* (Hrsg), e-Mail (Manz, im Druck).

³⁷ Vgl zuletzt: *Dietmar Jahnel*, Spamming, Cookies, Web-Logs, LBS und die Datenschutzrichtlinie für elektronische Kommunikation, wbl 2003, 108.

³⁸ RL 2002/58/EG vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) ABI 2002 L 201, 37.

³⁹ *Lloyd*, Information Technology Law³, 36, legt dar, dass es weder in Scotland noch in England ein Recht auf Privacy gibt.

⁴⁰ Vgl Punkt 2.2 und die Definition des sec 1 para 1 UK Data Protection Act 1998, die nur Daten lebender (ecce!) Personen umfasst.

⁴¹ Vgl *Max W. Mosing*, Cookies and Log Files: The „Transparent Internet User“ or Data Protection on the Internet in the EU?!, <http://www.it-law.at> (1.4.2003).

⁴² Vgl *Mosing*, Cookies, <http://www.it-law.at>; aA *Jahnel*, wbl 2003, 108.

2.6. Evaluierung – Die Illusion des Privaten

Nach *David Lyon* ist unsere Kontrollmöglichkeit (iSd informational self-determination) seit der Ubiquität der Computerisierung nicht nur eingeschränkt, sondern uns faktisch entzogen – es bleibt nur die Illusion des Privaten.⁴³ Das zeigt die Wichtigkeit des Datenschutzes in der Informationsgesellschaft, in der Daten allgegenwärtig sind.

Das Datenschutzrecht ist nie „zur Ruhe“ gekommen: Obschon ein Paradigmenwechsel (Schutz vor dem Staat hin zum Schutz vor privaten Datenverarbeitern) stattgefunden hat, zeigen die Maßnahmen nach dem 11.9.2001 (WTC-Anschlag), dass die Bewahrung der Machtbalance zwischen Staat und Bürger für den Datenschutz zentral bleibt: Die Vermarktung von ZMR-Daten, der staatliche Einsatz⁴⁴ von CCTVs und Initiativen zur Überwachung des Kommunikationsverkehrs müssen mit Argusaugen verfolgt werden – sobald Geheimdienste im Spiel sind, scheint das allerdings lächerlich.

Auf den ersten Blick rein technische Entwicklungen beinhalten vielfach datenschutzrechtliche Aspekte: IPv6, aber auch Digital Right Management Systeme⁴⁵ sind im Lichte des Datenschutzes zu bewerten.

Alles in allem: Datenschutz darf nicht zur Illusion werden!

⁴³ Vgl *David Lyon*, Surveillance in Information Societies: Before and After September 11 2001, http://www.qsilver.queensu.ca/sociology/Surveillance/narrative_report.htm (1.4.2003).

⁴⁴ Der private Einsatz von CCTV ist im Lichte des DSGVO (noch) näher zu untersuchen.

⁴⁵ Vgl *Alexander Dix*, Digitales Urheberrechts-Management (DRM) und Datenschutz, <http://www.brandenburg.de/land/lfdbbg/empfehl/vortrag/drm.pdf> (1.4.2003).