‚Privacy Management in Progress' – Balanceakte zwischen Öffnung und Schließung personenbezogener Daten

Ulrike Hugl

Zusammenfassung

Datenschutzfragen betreffen uns alle und tangieren unterschiedlichste Bereiche unseres Alltags- wie Berufslebens. Datenschutz (Privacy) als Schutz der Privatsphäre wird vor dem Hintergrund unterschiedlicher wissenschaftlicher Disziplinen diskutiert und birgt technologische, soziale, ethische, ökonomische wie politische Implikationen. Neue technologische Entwicklungen und kostengünstige Überwachungsmöglichkeiten ermöglichen zunehmend ubiquitäre Datensammlungen und -verwendungen für den Staat wie für Unternehmen. Der Beitrag thematisiert zunächst aktuelle internationale wie nationale Datenschutzentwicklungen, individuelle Datenspuren und Fragen der Datensicherheit, gefolgt von rechtlichen Problemfeldern und wissenschaftlichen Datenschutztheorien und -ansätzen vor dem Hintergrund unterschiedlicher Disziplinen. Abschließend werden mögliche Handlungsstrategien sowie Fragen des Status quo für Einzelne wie Unternehmen diskutiert.

Einführung

Datenschutz zielt generell auf die Entscheidung eines Individuums, welche persönlichen Daten wann und wem zugänglich sein sollen. Der Schutz vor missbräuchlicher Datenverarbeitung durch Staat, Unternehmen und Privatpersonen steht im Vordergrund. Unterschiedliche Definitionen von Datenschutz fokussieren – je nach Blickwinkel – auf den Schutz der Privatsphäre, des Persönlichkeitsrechts bei der Verarbeitung von Daten, des Rechts auf informationelle Selbstbestimmung (Deutschland) sowie auf den Schutz vor Datenmissbrauch. Letzterer impliziert den Schutz vor unbefugter wirtschaftlicher oder technischer Einflussnahme auf die Unversehrtheit von Daten. Im engeren Sinn umfasst Datenschutz die Auslegung der rechtlichen Rahmenbedingungen des Schutzes der Privatsphäre inklusive der Verarbeitung und Weitergabe bzw. Verwertung von Daten. Gebräuchlich sind auch die Begriffe ‚Privacy' (Schutz der Privatsphäre), ‚Data Protection' (z.B. im europäischen Rechtsraum), ‚Data Privacy' und ‚Information Privacy'. In der Europäischen Union wird Datenschutz insbesondere als „Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten" (vgl. EU 24. Okt. 1995, Art. 1 Abs. 1) verstanden, im Europarat als Schutz des „Recht[s] auf einen Persönlichkeitsbereich […] bei der automatischen Verarbeitung personenbezogener Daten" (vgl. EU 28. Jan. 1981, Art. 1), in Liechtenstein und der Schweiz als „Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden" (vgl. DSG 19. Juni 1992, § 1; DSG 14. März 2002, Art. 1 Abs. 1). In Deutschland zielt das Bundesdatenschutzgesetz auf den Schutz einer Beeinträchtigung der Persönlichkeitsrechte des Einzelnen (vgl. BDSG 20. Dez.

1990, § 1 Abs. 1), in Österreich hingegen wird auf den „Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht“ fokussiert (vgl. DSG 2000, § 1 Abs. 1 Satz 1). Geht es um den spezifischen Schutz vor Datenverlust, Datendiebstahl oder Datenveränderung, wird von Informationssicherheit oder von Datensicherheit gesprochen.

Zum einen schreitet die technische Entwicklung immer rascher voran und der allgemeine Bedarf an Datensammlungen steigt an, zum anderen sind dementsprechende Diskussionen und vor allem die Umsetzung der Datenschutzgesetze nach wie vor deutlich im Hintertreffen. Diese Entwicklung führt zu stetig wachsenden Risiken für den Einzelnen, was sich unter anderem in den immer häufiger in den Medien bekannt werdenden Datenschutzvorfällen widerspiegelt.

Während die Datensparsamkeit ein Grundprinzip der aktuellen Datenschutzrichtlinie der Europäischen Union ist (vgl. EU 24. Okt. 1995, Art. 6 Z. 1 c), ist der Wunsch nach weniger Datensammlungen als unrealistisch zu betrachten: In einer Zeit geprägt von asynchronen Konflikten und allseits kommunizierten Bedrohungen der nationalen Sicherheit zielt der Staat offenbar verstärkt auf die Sammlung von Daten über Bürgerinnen und Bürger, dies um partiell im Bereich der Strafverfolgung technisch Schritt halten sowie politische Rahmenvereinbarungen auf EU- und internationaler Ebene erfüllen zu können. Der Aufbau von biometrischen Datenbanken, die Rasterfahndung, Passagierdatenbanken, die Vorratsdatenspeicherung (VDS) und der Ausbau der Kameraüberwachung an öffentlichen Plätzen, aber auch serviceorientierte Anwendungen wie Bürgerkarten, Gesundheitsinformations- oder eGovernment-Systeme sind nur einige Beispiele für das gesteigerte Engagement der staatlichen Sammlung personenbezogener Daten.

Doch nicht nur der Staat sammelt personenbezogene Daten: Abhängig von der Branche sind unterschiedliche Informationen über bestehende und potenzielle Kunden, deren Merkmale, Wünsche und Verhalten für ein Unternehmen von Bedeutung. Während staatliche Institutionen (z.B. in Form eines Datenschutzbeauftragten) einer gewissen Kontrolle unterliegen, agieren Unternehmen meist vorwiegend profitorientiert und eruieren immer wieder Möglichkeiten und Beweggründe, Graubereiche der Datenschutzgesetze auszuloten, um Wettbewerbsvorteile generieren zu können.

Entwicklungen, Überwachungskategorien und Datenspuren

Privacy International (PI), eine international tätige Menschenrechtsorganisation, führt laufend Studien zum Datenschutz, zur Überwachung und Einhaltung von Menschenrechten durch. Im Jänner 2011 wurde die neueste europäische Studie zu Datenschutzentwicklungen in 33 europäischen Staaten veröffentlicht (vgl. PI/EPIC/CMCS 2010): Die Analysekategorien reichen von der demokratischen Entwicklung und dem konkreten Datenschutzvollzug (gesetzlich) über ‚Data Sharing‘-Spezifika bis hin zu Fragen des Datenschutzes im Bereich des Finanzwesens, der Medizin und des Umgangs mit verschiedensten Überwachungstechnologien durch die Regierungen. Zusammenfassend wird für Europa Folgendes konstatiert (ebd., S. 11):

> „Europe is the world’s leader in privacy rights. But with leadership like this, we worry about the future. The Directive on Data Protection [Anmerkung: Richtlinie 95/46/EG] has been implemented across EU member states and beyond, but inconsistencies remain. Surveillance harmonisation that was once threatened is now in disarray. Yet there are so many loopholes and exemptions that it is increasingly challenging to get a full understanding of the privacy situations in European countries. The cloak of ‚national security‘ enshrouds many practices, minimises authorisation safeguards and prevents oversight.“

Im europäischen ‚Privacy Ranking‘ von PI finden sich Österreich und die Schweiz gemeinsam mit elf weiteren Staaten in der Kategorie ‚systematisches Scheitern von Schutzmaßnahmen‘, Deutschland wird mit ‚einige Sicherheiten, aber geschwächter Schutz‘ etwas besser bewertet. Im deutschsprachigen Raum werden dabei vorwiegend Fragen zur Speicherung von Kommunikationsdaten, Datenaustauschaktivitäten (Grenzüberwachung, DNA), der Einsatz von visuellen Überwachungssystemen sowie diverse weitere Aktivitäten der Regierungen, die den Datenschutz ihrer Bürger tangieren, urgiert (vgl. PI 2007).

Die schon erwähnte Frage der nationalen Sicherheit bildet seit den Anschlägen auf das World Trade Center in New York am 11. September 2001 die vorrangige Argumentationslinie für die Einführung unterschiedlichster Überwachungsmaßnahmen westlicher Staaten. Was jedoch darf oder soll ein Staat für den Aufbau einer sogenannten Sicherheitsgesellschaft tun? Der Begriff Sicherheitsgesellschaft wird von Peter-Alexis Albrecht vor dem Hintergrund der Kriminologie und des Strafrechts aufgegriffen: Die Grundlagen wurden (vor allem in Deutschland) im Präventionsstaat der 1980er und 1990er Jahre gelegt; die Anschläge 2001 waren somit der Anlass und nicht der Grund für die „Entwicklung zur Sicherheitsgesellschaft“ (Albrecht 2010, S. 175). Als zentrale Wegbereiter sieht Albrecht staatliche Deregulierungsmaßnahmen, „ungezügelten Neoliberalismus“ (Ökonomieprinzip) sowie „moralisch-religiösen Fundamentalismus“ (ebd.) wie sie in vielen Staaten der westlichen Welt vorherrschen, und konstatiert, dass ‚Prävention‘ im Konnex gesellschaftlicher Transformationsprozesse mittlerweile „zum neuen Zauberwort“ avanciert sei (vgl. Steinke 16.08.2010). Als weitere Wegbereiter können zudem die rasante Entwicklung und sinkende Preise von Informations- und Kommunikationstechnologien, ebenso das starke Medienecho zum Ruf nach mehr Sicherheit von Staat und Bürgern genannt werden. Die beschriebene Ausgangslage im Sicherheitskonnex führt zu einem Teufelskreis, nämlich zu einem „Überdehnen und Ausreizen der Sicherheits- und Überwachungstechniken“ und „hat sein Gegenteil mitproduziert – die Menschen fühlen sich durch die gesteigerte Kontrolle, der sie unterliegen, mehr bedroht, als sie de facto sind, was auf der kollektiven Ebene wiederum verstärkte Sicherheitsbedürfnisse weckt usf.“ (Uhl 2008, S. 15).

Durch die aufgezeigte Entwicklung wurde in den letzten Jahren der Weg zum panoptischen Überwachungsstaat mit Registrierung und Kontrolle in verschiedensten gesellschaftlichen Bereichen bereitet. Als Michel Foucault 1973 auf Basis seiner Untersuchungen von einer „Gesellschaft, in der Panoptismus herrscht“ (Foucault 2002, S. 735) sprach, konnte er schwerlich voraussehen, welche analytischen Überwachungs- und Datenverwendungsmöglichkeiten im 21. Jahrhundert verwirklicht und noch möglich sein würden. Mittlerweile sind beispielsweise

Computernetzwerke, kryptometrische und biometrische Verfahren (z.B. Gesichts-, Iris-/Netzhaut-, Finger- und Handabdruck-, Stimm- und Körpergeruchs- sowie Körperbewegungserkennung, Atemgasanalyse zur nicht invasiven Diagnostik), Soziale Netzwerke, Blogs, Foren u.v.m. im Internet, Techniken des Profiling und Data Mining, Video-, Audio-, Briefverkehr-, Flugpassagier- und Arbeitsplatzüberwachung sowie ‚smarte' Kommunikations- und Logistikformen und medizinische Überwachung via Radio-Frequency Identification (RFID) omnipräsent und durchdringen zunehmend unsere Arbeits- und Alltagswelt. Alle genannten Möglichkeiten und *Überwachungskategorien* bergen auf der einen Seite Chancen, Erleichterungen und effizientes Arbeiten für den Staat, die Wirtschaft und den Einzelnen, auf der anderen Seite jedoch auch Gefahren des unerwünschten Verlusts der Privatsphäre und des Grundrechts auf Datenschutz, Risiken des Datenmissbrauchs und -diebstahls (bis hin zum Identitätsdiebstahl) sowie Gefahren durch eine unerwünschte Verknüpfung personenbezogener Daten.

Nutzer hinterlassen beispielsweise im Internet beim Surfen, Mailen, beim Umgang mit Sozialen Netzwerken und durch die Nutzung von Mobiltelefonen (mit GPS, Internetzugang usw.), beim Online-Einkauf und -Banking u.a.m. aktive oder passive (ohne Zutun des/der Betroffenen) *Datenspuren*, die wiederum vorwiegend von professionellen Datensammlern und sogenannten Informationsbrokern – beispielsweise nach Ort, Zeit, Partnern und Inhalten ‚kontextualisiert', verknüpft, personen- oder freundesgruppenbezogen – ausgewertet und verkauft werden. Als weit verbreitete Trackinginstrumente werden vorrangig *Cookies* eingesetzt. Cookies sind kleine Textdateien, die auf dem Endgerät eines Internetnutzers beim Aufruf einer Website angelegt werden. Individuelle Daten, die auf der Basis von Cookies gewonnen wurden, werden mit weiteren Daten zusammengeführt und mitunter an Interessierte versteigert. Ein Beispiel (vgl. Schaumann 29.04.2012): Ein Nutzer recherchiert ein seltenes, vorrangig berufsbedingtes Krankheitsbild und dessen kostspielige Behandlungsmöglichkeiten auf einer Website. Ein auf Tracking spezialisiertes Unternehmen bietet daraufhin den (virtuellen) Kontakt des Nutzers zum Verkauf für Anwaltskanzleien (Interesse an Klage gegen Arbeitgeber), Pharmaunternehmen (Medikamentenkauf) und Gesundheitsdienstleister (Behandlung, Therapie) an. Die zugrundeliegende automatisierte Versteigerung solcher Nutzerdaten geht dabei innerhalb von Bruchteilen von Sekunden via ‚data exchanges' vonstatten. *Data Mining* als eine weitere Technik nutzt kombinierte Zusammenhänge von individuellen Datenspuren durch automatisierte Unterstützung (systematisierte Auswertung durch Korrelation von Datenelementen) mit dem Ziel, neue, status-quo-beschreibende und/oder vorhersagende Muster und Regelmäßigkeiten in Datensätzen aufzufinden. Beim Instrument des *Profiling* werden individuelle oder gruppenbezogene Kundenprofile (Datenabbild des Kaufverhaltens), Nutzungsprofile von Websitebesuchen u.a. in spezifischen Kontexten eruiert. Kunden werden somit identifiziert, deren Informationen gesammelt und diese zur weiteren Ansprache und individualisierten Absatzinstrumenten genutzt, vorrangig für personalisierte Werbung via Newsletter, Mailings oder Recommendersysteme wie ‚Kunden, die dieses Produkt X gekauft haben, kauften auch …'. Durch das Bestreben nach möglichst detaillierten und vollständigen Profilen werden, ökonomisch betrachtet, „[…] vermeintliche Konkurrenten zu Anbietern und Kunden, indem sie ihre Datenbestände entgeltlich substituieren und so das eigene Portfolio verbessern"

(Hess/Schreiner 2012, S. 108). Daher bieten beispielsweise Online-Börsen wie BlueKai (siehe http://www.bluekai.com/) Profile von etwa 300 Millionen Nutzerinnen und Nutzern an – unterteilt nach 30.000 Merkmalen mit diversen Auswahlmöglichkeiten von beobachtetem Verhalten bis zu Absichtsprognosen von Nutzerinnen und Nutzern (ebd.; vgl. auch die oben erwähnten Versteigerungen).

Auch die *Vorratsdatenspeicherung (VDS)* als derzeit umfassendste Überwachungsmaßnahme im europäischen Raum – ebenfalls auf politischer Ebene vor dem Hintergrund der nationalen Sicherheit auf Basis der Terroranschläge von New York, Madrid und London argumentiert – sorgt für massive Datenschutzbedenken. Mit der EU-Richtlinie 2006/24/EG (vgl. EU 15. März 2006) sind alle Mitgliedsstaaten mit insgesamt etwa 400 Millionen Bürgerinnen und Bürgern aufgefordert, die Richtlinie innerstaatlich umzusetzen und Kommunikationsverbindungsdaten ihrer Bürgerschaft für mindestens sechs (bis 24) Monate zu registrieren. Davon betroffen sind Telefongespräche, Multimedia- und Kurzmitteilungen (MMS, SMS), die Internet-Telefonie sowie sämtlicher Internetverkehr (Protokolle einschließlich E-Mail). Bei Telefongesprächen sind die Teilnehmer, deren Nummern, der Zeitpunkt, die Dauer und die Standortdaten bereitzustellen. Inhalte von Telefonaten werden zwar nicht gespeichert, allerdings lassen sich durchaus Rückschlüsse über andere Daten ziehen (z.B. durch die Verknüpfung mit Geodaten oder durch Kontakte zu einschlägigen Hotlines oder Nummern wie jene von Telefonseelsorgen, psychosozialen Diensten, der AIDS-Hilfe, von Selbsthilfegruppen bei bestimmten Krankheiten, den Anonymen Alkoholikern, bestimmten Anwälten, Ärzten, Journalisten etc.). Die VDS bildet insofern ein EU-weites Novum, als personenbezogene Daten von Bürgern ‚präventiv', das heißt ohne Anfangsverdacht und konkrete Gefahr, für einen Zugriff von Ermittlungsbehörden im Bedarfsfall ‚bevorratet' werden. Summa summarum: Jede Bürgerin, jeder Bürger avanciert zur/zum Verdächtigen im Überwachungsstaat. In Österreich ist die Richtlinie seit dem 1. April 2012 umgesetzt (6 Monate Speicherung) – in Deutschland, der Tschechischen Republik und in Rumänien war dies ebenso, die entsprechenden Gesetze wurden jedoch von den jeweiligen staatlichen Verfassungsgerichtshöfen für rechtswidrig erklärt (in Ungarn wird ein Urteil für Mitte 2012 erwartet). Auch in Österreich wurde Mitte Juni 2012 eine Klage (siehe www.verfassungsklage.at) eingereicht, ebenso besteht eine Ankündigung der Kärntner Landesregierung, die österreichische Umsetzung vom Verfassungsgerichtshof prüfen zu lassen. Das deutsche Bundesverfassungsgericht erklärte in seinem Urteil im März 2010 das seit 2008 geltende Gesetz für verfassungswidrig: Es seien insbesondere keine konkreten Maßnahmen zur Datensicherheit vorgesehen, zusätzlich die Hürden für staatliche Zugriffe auf die betreffenden Daten zu niedrig (vgl. BVerfG 2. März 2010). Die VDS ist – über die Frage der nationalen Verfassungswidrigkeit hinaus – nach Meinung vieler Rechtsexperten auch weder mit der Europäischen Menschenrechtskonvention (vgl. Europarat 4. Nov. 1950) noch mit der EU-Grundrechtscharta (vgl. EU 7. Dez. 2000, Art. 8: Anerkennung des Rechts auf den Schutz personenbezogener Daten) vereinbar. Mittlerweile ist absehbar, dass die derzeitige EU-Richtlinie zur VDS überarbeitet werden wird. Nichtsdestoweniger müssen Staaten, welche die Richtlinie aktuell nicht umsetzen (Deutschland ringt derzeit um eine neue nationale Regelung), mit Millionenklagen vor dem Europäischen Gerichtshof rechnen.

Bei der VDS gelten, neben den schon genannten, verschiedene Datenschutzaspekte als bedenklich: Als Beispiel zunächst die Frage von *Berufs- und Schweigepflichten* von beispielsweise Anwälten, Journalisten und Seelsorgern in Österreich. Betroffene werden ohne eine grundlegende Veränderung ihres Kommunikationsverhaltens keinen Vertraulichkeitsschutz für ihre Klienten, Patienten, Informanten, Zeugen usw. gewährleisten können. Zunächst diskutierte Ausnahmen für solche Geheimnisträger haben sich als technisch nicht durchführbar erwiesen. Bei Journalisten und Anwälten wird die Wahrscheinlichkeit sehr hoch sein, dass Verbindungsdaten im Zusammenhang mit Ermittlungen gegen Dritte verwendet werden. Die größte Gefahr bildet hierbei wohl auch der Interpretationsspielraum von Ermittlern bei der Einschätzung aller verknüpften Daten (Kontakte via Telefonie, Geodaten usw.) einer Person mit ihrem dokumentierten Kommunikationsverhalten in Beruf und Freizeit im Bevorratungszeitraum. Durch die VDS werden Betroffene zum Schutz ihrer Klientel faktisch in Richtung derselben konspirativen Verhaltensweisen gedrängt, wie sie von Mitgliedern der organisierten Kriminalität, Berufsverbrechern, Geheimdienstmitarbeitern usw. angewandt werden. Verschiedene Interessenvertretungen betroffener Berufsgruppen haben mittlerweile Empfehlungen zum Umgang mit ihren Klienten, Patienten usw. ausgesprochen. Dazu zählen beispielsweise ein Zurück zum postalischen Versand von Unterlagen sowie persönliche Treffen anstelle von E-Mails und Telefonaten. Die VDS birgt jedoch noch eine weitere Gefahr: Sie öffnet Tür und Tor für Anschwärzungen und Manipulationen. Auf der Basis der VDS reicht es aus, beispielsweise einem unliebsamen Unternehmer eine Software unterzuschieben, die auf einschlägigen, für Ermittlungsbehörden sensiblen oder unzulässigen Websites surft, und anonym Anzeige zu erstatten. Am Beispiel des bayrischen Politikers Malte Spitz (Grüne) wird en detail aufgezeigt, welche Datenspuren im Rahmen der VDS die Handynutzung hinterlässt (vgl. Biermann 24. Feb. 2011): Er musste jedoch, um seine gespeicherten Daten im Zeitraum von August 2009 bis Februar 2010 zu erhalten, die Deutsche Telekom klagen. Sein Mobiltelefon hatte im genannten Zeitraum mehr als 35.000 Mal Informationen geliefert. Die Abfolge und Analyse der Daten ergeben ein beeindruckendes Bild über seine Vorlieben, Gewohnheiten und sein Verhalten. Es kann eruiert werden, wann er wo ist, welche Verkehrsmittel er nutzt (Flug, Bahn oder Auto), wann er am besten erreichbar ist und wann nicht, ob er lieber SMS verschickt oder lieber telefoniert, wann er in welchem Biergarten sitzt usw. ZEIT ONLINE (ebd.) hat die VDS-Daten zudem mit frei im Internet verfügbaren Informationen aus Twitter, Blogeinträgen und von Websites (z.B. Termine auf der Website seiner Partei) verknüpft. Ermittlungsbehörden würden noch über wesentlich mehr Daten verfügen, nämlich die Daten seiner Kontakte, also Personen, mit denen er telefoniert, denen er SMS gesandt und die er getroffen hat usw.[1] Der Fall von Malte Spitz hat jedenfalls erstmals einer breiten Öffentlichkeit aufgezeigt, in welcher Tiefe Aspekte des Lebens eines Bürgers (Lebensumstände wie Geschäftsbeziehungen) mit Hilfe von VDS-Daten eruiert werden können. Von politischer Seite (EU) wird, trotz Datenschutzbeden-

[1] Downloadmöglichkeit der gelisteten VDS-Daten unter https://spreadsheets.google.com/ccc?key=0An0YnoiCbFHGdGp3WnJkbE4xWTdDTVV0ZDlQeWZmSXc&hl=en_GB&authkey=COCjw-kG sowie einer interaktiven Karte seiner Bewegungsdaten nach Datum und genauer Uhrzeit unter http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten.

ken sowie aktueller Gutachten, welche der VDS geringen bis keinen Nutzen (z.B. bezüglich islamischen Terrors und auch sonstiger Verbrechensbekämpfung) attestieren (vgl. z.B. Albrecht 2011), an der VDS festgehalten. Zudem werden EU-Projekte wie INDECT (http://www.indect-project.eu/) unter Beteiligung von Forschungsgruppen und Unternehmen aus Österreich, Deutschland und anderen Staaten umgesetzt (Fördersumme etwa 11 Millionen Euro). INDECT erforscht Überwachungstechnologien (z.B. Kleinstdrohnen mit Überwachungskameras) in ihrer Kombination und mit entsprechendem Datenabgleich aus verschiedenen Quellen wie Blogs, Foren, Sozialen Netzwerken, polizeilichen Datenbanken, öffentlichen Kameras u.v.m. – kombiniert mit automatischer Personenidentifizierung via Gesichtserkennung. Zielsetzung soll insbesondere die Abwehr terroristischer Gefahren und schwerer Verbrechen sein. VDR-Daten würden die Datenkombinationsmöglichkeiten des von INDECT anvisierten Überwachungssystems noch erweitern.

Behörden wie Unternehmen haben sich auch laufend die Frage nach der *Datensicherheit* (von VDS- und anderen Daten) zu stellen. Das Umsetzen klarer gesetzlicher Vorgaben in Geschäftsprozessen und der Aufbau der notwendigen technischen Infrastrukturen benötigt zum einen klare Rahmenbedingungen und zum anderen erhebliche Zeitressourcen – dasselbe gilt auch für den Aufbau entsprechender ‚Awareness' bei den Mitarbeitern. Bezüglich der VDS trifft dies in besonderem Maße die durchführenden Provider. *Anonymous*, ein offenes Kollektiv von wechselnden Internetaktivisten ohne Anführer und kontrollierende Instanz, hat jedenfalls jüngst mit großem Medienecho aufgezeigt, dass Behörden, staatsnahe Institutionen, Parteien u.a. durchaus erhebliche Mängel bezüglich ihrer Datensicherheit aufweisen. Einige Beispiele: In Österreich wurde die GIS (Gebühren Info Service) gehackt (etwa 100.000 Kontonummern und 211.700 Datensätze waren unverschlüsselt auf einem Server gespeichert), es erfolgten Angriffe auf Parteiseiten, es wurden 25.000 Daten von Polizisten online gestellt und 600.000 Daten von Versicherten der Tiroler Gebietskrankenkasse kamen unter die Verfügungsgewalt der Gruppe. Um für die Privatsphäre der Bürgerinnen und Bürger (und gegen die VDS) zu sensibilisieren, wurde aktuell die Veröffentlichung von brisanten E-Mails von Politikern angekündigt.

Rechtliche Problemfelder und Datenschutzkonzepte

Um die Bürger zu schützen und ihr Interesse an der Geheimhaltung ihrer personenbezogenen Daten zu wahren, sehen die EU-Richtlinie (vgl. EU 24. Okt. 1995, Art. 10) und nationale Datenschutzgesetze (vgl. z.B. DSG 2000, § 26; BDSG 20. Dez. 1990, § 6) ein *Auskunftsrecht* Betroffener vor. Ein Kritikpunkt an der gültigen Rechtslage ist jedoch die Tatsache, dass dieses Auskunftsrecht von den Betroffenen erst dann in Anspruch genommen werden kann, wenn die Datensammlung und somit auch deren Betreiber einem/einer Betroffenen auch bekannt sind. Dies tritt im schlimmsten Fall erst dann ein, wenn bereits ein Schaden entstanden ist. Außerdem ist anzumerken, dass Bürger allgemein nur schwer Zugang zu Verwaltungswissen haben und zudem die Qualität etwaiger Auskünfte – auch vor dem Hintergrund niedriger Strafrahmen bzw. Verwaltungsstrafbestimmungen sowie der Notwendigkeit einer zivilrechtlichen Einforderung samt Prozessrisiko seitens der Betroffenen – zu wünschen übrig lässt. Entsprechende

Auskünfte sind nur in 13% der Fälle korrekt (vgl. Reichmann 2004, S. 757). Eine mögliche Anforderung an die nächste Generation von Datenschutznormen bzw. die nächste EU-Richtlinie wäre die Umkehrung dieses schwer auszuübenden Auskunftsrechts hin zu einer *aktiven Informationspflicht* der Betroffenen durch den Betreiber einer Datensammlung: Werden personenbezogene Daten gesammelt, gekauft oder in einer anderen Form verarbeitet, so müssten die Betroffenen aktiv durch den Betreiber der Datensammlung informiert werden. Somit wären einzelne Bürger in der Situation, nicht nur reaktiv zu wissen, wo personenbezogene Daten über sie gespeichert werden, sie wären auch erstmals in der Lage, von ihrem Recht auf Privatsphäre und Datenschutz aktiv Gebrauch zu machen.

Eine weitere vorgeschlagene Änderung des Datenschutzgesetzes könnte man auch als einen Paradigmenwechsel in Hinblick auf die damit verbundenen Privacy-Theorien sehen: Die EU-Richtlinie, das österreichische und andere nationale Datenschutzgesetze unterteilen Daten in verschiedene *Abstufungen der Schutzwürdigkeit* (z.B. im DSG 2000 in indirekt personenbezogene, personenbezogene und sensible/besonders schutzwürdige Daten). Dies entspricht der Herangehensweise der Sphärentheorie, die ebenfalls zwischen mehreren Sphären der Schutzwürdigkeit unterscheidet. Bei näherer Betrachtung der Möglichkeiten der modernen Datenverarbeitung und -verknüpfung offenbart sich allerdings die Unzulänglichkeit dieses Ansatzes: Auch einzelne, nicht als schutzwürdig betrachtete Daten können durch Kombination zur Bildung von Profilen und somit zu direkt personenbezogenen Informationen führen. Grundsätzlich empfehlenswert wäre also eine Erweiterung des als schützenswert zu betrachtenden Datenbereichs, nämlich den Grundannahmen der Mosaiktheorie (Egger 1990) folgend. Diese geht davon aus, dass – gleich einem Bild aus vielen kleinen Mosaiksteinen – aus Daten in Verbindung mit anderen Daten ein mehr oder weniger genaues Profil eines Menschen entstehen kann. In einer Zeit, in der die Datenverarbeitung gegenüber der reinen Datenerfassung zunehmend an Bedeutung gewinnt (vgl. Tichy/Peissl 2001, S. 8), scheint ein reiner Schutz von sensiblen oder personenbezogenen ‚Einzeldaten' – wie derzeit rechtlich verankert – nicht mehr ausreichend, um sich gegen eine Profilbildung wehren und sein Interesse am Schutz seiner personenbezogenen Daten wahren zu können.

In den letzten Jahren werden neben diversen Privacy-Theorien auch weitere Aspekte im Rahmen des wissenschaftlichen Diskurses thematisiert: Beispielsweise spricht Solove (2008) von Privacy als „issue of global concern" (S. 2) und konstatiert, dass „[…] the discourse has ranged from popular writers to journalists to experts in law, philosophy, psychology, sociology, literature, economics, and countless other fields" (S. 4). Er unterscheidet vier zentrale Gruppen von Aktivitäten, welche als Ausgangspunkt für Datenschutzprobleme gelten können: „information collection" (surveillance, interrogation), „information processing" (aggregation, identification, insecurity, secondary use, exclusion), „information dissemination" (breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, distortion) und „invasion" (intrusion, decisional interference) (Solove 2007, S. 758). Andere Forschungslinien fokussieren (insbesondere in den Bereichen Marketing und Online Social Networks) beispielsweise auf Online Privacy oder auf psychosoziale Faktoren wie Überzeugungen und Persönlichkeit (vgl. z.B. Hugl 2011; Krasnova/Veltri 2010; Hugl 2010; Lipton 2010).

Im Folgenden werden einige Datenschutzansätze (vorwiegend aus dem deutschsprachigen Raum) vorgestellt:

Die für das Zivilrecht entwickelte *Sphärentheorie* (auch Schichtentheorie) wurde von Hubmann (1953) erstmals publiziert und geht davon aus, dass identitäts- bzw. den Eigenwert des Menschen bestimmende Daten in unterschiedlich empfindliche Bereiche eingeteilt werden können. In einem kreisförmigen Schichtenmodell sind mehrere, unterschiedlich sensible und somit schutzwürdige Sphären angeordnet, wobei die „schützenswerteste" Sphäre den Mittelpunkt des Modells darstellt. Hubmann geht dabei von einer Dreiteilung in Individual-, Privat- und Geheimsphäre aus (ebd., S. 269). Den innersten (absolut geschützten Bereich) stellt die Geheim- oder Intimsphäre dar, definiert als „[…] Handlungen, Äußerungen und Gedanken, von denen niemand oder höchstens ein genau beschränkter Kreis von Vertrauten Kenntnis nehmen soll, an denen also ein Geheimhaltungsinteresse besteht" (ebd., S. 270). Die der relativ geschützten Privatsphäre zugehörigen Daten sind dagegen nur einem bestimmten (bzw. unbestimmten, aber beschränkten) Personenkreis ohne Weiteres zugänglich, sollen aber darüber hinausgehenden Kreisen sowie der breiten Öffentlichkeit entzogen werden. Die rechtlich ungeschützte Individualsphäre schließlich beinhaltet beispielsweise den Namen, die Ehre und das Recht am eigenen Bild (ebd., S. 270).

Verschiedene Autoren (Jäggi 1960; Scholler 1967; Habermas 1990) erweiterten das Modell um eine weitere Sphäre: die „Sozialsphäre". Die „Sozialsphäre" ist ein zwischen Privat- und Öffentlichkeitssphäre angesiedelter Bereich, der alle Daten umfasst, die „[…] zwar jedermann erlaubterweise wahrnehmen kann, die aber nicht Gegenstand eines besonderen Kundgebungswillens sind" (Jäggi 1960, S. 133a). Seidel (1972) wiederum schlägt fünf Schichten vor: die Geheim-, Intim-, Vertrauens-, Sozial- und Öffentlichkeitssphäre. Der gemeinsame Nenner der verschiedenen Autoren bleibt jedoch die eingangs erwähnte Unterscheidung zwischen einer absolut geschützten Sphäre und mehreren Bereichen mit mehr oder weniger ausgeprägter Zugriffsmöglichkeit. Rechtliche Anwendung fand die Sphärentheorie erstmals im sogenannten Mikrozensus-Urteil des Deutschen Bundesverfassungsgerichtshofes aus dem Jahre 1969 (vgl. Theißen 2009), bis dieser Ansatz 1983 vom Ansatz eines Selbstbestimmungsrechts über personenbezogene Daten abgelöst wurde.

Hauptkritikpunkte an der Sphärentheorie sind vor allem die unpräzise und somit unzureichende Abgrenzung der einzelnen Sphären (vgl. z.B. Rohlf 1980) sowie die Schwierigkeit, klare Grenzlinien für die (zulässigen) Zugriffssektoren von öffentlichen Institutionen zu ziehen (vgl. z.B. Egger 1990). Ein weiterer Problempunkt ergibt sich auch aus der Relativität und Subjektivität der Privatsphäre, also der unterschiedlichen Auffassung ein und derselben Information durch verschiedene Personen (vgl. z.B. Steinmüller et al. 1971; Tichy/Peissl 2001). Daraus ergibt sich die grundsätzliche Frage „[…] wer dazu bemächtigt ist, festzulegen, welche Daten sensibel sind und welche nicht" (Egger 1990). Des Weiteren können sich nach diesem Ansatz auch durchaus praktische Probleme durch die Möglichkeiten der Datenverknüpfung ergeben: öffentliche Daten könnten durch eine Kombination mit ‚privaten' oder weiteren ‚öffentlichen' Daten zu Informationen werden, die eine Person wiederum als ‚privat' einstufen würde (vgl. z.B. Böckenförde 2003).

An die genannten Kritikpunkte der Sphärentheorie, im Speziellen dem Gefahrenpotential der Datenverknüpfung, versucht die *Mosaiktheorie* anzuknüpfen. Dabei wird davon ausgegangen, dass – analog zu Mosaiksteinchen, die zusammengesetzt schließlich ein Bild ergeben – „[…] voneinander unabhängige, scheinbar harmlose Daten ein genaues Persönlichkeitsprofil ergeben, wenn sie miteinander verknüpft werden" (Egger 1990, S. 57). Daraus ergibt sich in Erweiterung der Sphärentheorie eine klare Anforderung, nicht nur „[…] Daten aus ‚sensiblen' Sphären zu schützen – wie immer diese definiert werden […]" (Tichy/Peissl 2001, S. 8), sondern alle Daten, die zur Bildung eines Persönlichkeitsprofils genutzt werden können. Aufgrund der zunehmenden Bedeutung der Datenverarbeitung gegenüber der reinen Datenerfassung ist es für einzelne Bürger kaum noch nachvollziehbar, wer welche Daten übermittelt bzw. verarbeitet. So „[…] entzieht sich das eigene ‚virtuelle' Bild weitgehend der eigenen Steuerung, womit zwangsläufig schutzwürdige Interessen verletzt werden" (ebd.). Praktische Probleme bei der Mosaiktheorie entstehen demnach durch sukzessive (neue) Datenverknüpfungen und daraus resultierenden neuen Zugriffsberechtigungen auf schützenswerte Daten. Ein weiteres Problem kann der jeweilige Informationssicherheitslevel (Sicherheit der Systeme bzw. Daten) verschiedener Datenhalter bilden. Generell steigen die gesammelten Datenmengen kontinuierlich, was auch ihre Kombinationsmöglichkeiten erhöht und die Schwierigkeit der Überprüfung von Profilbildungen mit sich bringt.

Nach den Grundannahmen der *Rollentheorie* besitzt eine Person nicht eine einheitliche Persönlichkeit (vgl. z.B. Dammann et al. 1992), sondern ist in einer Gesellschaft immer Träger verschiedener, voneinander unterscheidbarer Rollen – abhängig davon, in welcher gesellschaftlichen Situation sie sich gerade befindet. Je nach Situation und somit auch Rolle hinterlässt diese Person bestimmte Datenspuren – als Schüler/in beispielsweise Schuldaten, als Steuerzahler/in Einkommensdaten oder als Patient/in Gesundheitsdaten (vgl. Steinmüller 1984, S. 150). Entgegen den Annahmen der Sphärentheorie wird keine Trennung in verschiedene Bereiche abgestufter Schutzwürdigkeit vorgenommen. Vielmehr geht man davon aus, dass die Privatsphäre sich aus vielen unterschiedlichen Bildern aus diesen Rollen zusammensetzt. Somit ergibt sich eine grundsätzliche Schutzwürdigkeit aller Daten einer Person sowie eine Selbstverantwortung, welche dieser Daten wem preisgegeben werden (vgl. Tichy/Peissl 2001, S. 8). Der Unterschied zur Sphärentheorie und verschiedensten anderen Ansätzen (wie beispielsweise dem „right to be left alone") kann wie folgt festgehalten werden:

> „Privatheit manifestiert sich demgemäß nicht im Rückzug aus der Öffentlichkeit in einen abgeschlossenen ‚Innenraum', einen ‚Fürsichbereich', sondern als Ergebnis einer rollenspezifischen und folglich begrenzten Informationsweitergabe, als ‚situativ unterschiedlicher Bereich von Nichtinformationen'." (Amelung 2002, S. 23; zit. n. Mallmann 1976, S. 39)

Datenschutz wird nach der Rollentheorie dann tangiert, „[…] wenn Informationen aus einem Lebensbereich [einer Rolle] mit denen eines anderen Lebensbereiches zusammengeführt werden" (Petersen 2000, S. 12). Egger folgend kommt dem Datenschutz im Rahmen der Rollentheorie der Zweck zu, „die Zusammenführung der einzelnen Bilder zu verhindern und die Beibehaltung der verschiedenen Bilder zu sichern" (Egger 1990, S. 59). Müller (1975, S. 107)

wiederum notiert kurz und bündig: „Datenschutz ist hiernach die überlegte Zuweisung von Informationen".

Ein Vorteil der Rollentheorie liegt in der Relativität des Begriffs Privatsphäre und dem subjektiven Empfinden von Schutzwürdigkeit. Erhebliche Probleme ergeben sich aber beispielsweise aus der grundlegenden Definition eines Rollenbegriffes[2], der Definition der Rolle des Einzelnen dem Staat gegenüber[3] oder aus Faktoren, auf die Bürger keinen Einfluss haben (z.B. Ermessensentscheidungen von Behörden) (vgl. Vogelsang 1987, S. 138). Des Weiteren ist die erwähnte Selbstbestimmung der Datenweitergabe nicht in allen Bereichen des menschlichen Lebens möglich – die Berufung auf eine subjektiv empfundene Privatheit kann im Umgang mit öffentlichen Behörden durchaus ernste Sanktionen und Konsequenzen nach sich ziehen (vgl. z.B. Egger 1990). Somit erscheint die Rollentheorie nur wenig praktikabel und ist für eine exakte Bestimmung der persönlichen Schutzbereiche ungeeignet (vgl. Petersen 2000, S. 13).

Das *Recht auf informationelle Selbstbestimmung* (Deutschland) bedeutet das Recht einer Person, grundsätzlich selbst über die Preisgabe und Verwendung ihrer personenbezogenen Daten zu bestimmen. Jede Person soll also selbst bestimmen können, wie viele und welche Daten sie an andere weitergeben will (vgl. z.B. Pawlikowsky 1985). Dieses Recht wurde erstmals von Luhmann (1965) im rechtswissenschaftlichen Diskurs erwähnt und fand durch Steinmüller et al. (1971) in einem Gutachten seinen Niederschlag im Bereich des Datenschutzes. Das Konzept stieß anfangs auf Ablehnung, dies änderte sich allerdings, als es 1983 im Zuge der Grundsatzentscheidung zum Volkszählungsurteil erstmals vom deutschen Bundesverfassungsgericht anerkannt wurde. Wie bereits erwähnt, hatte sich die Judikative vom Mikrozensus-Urteil 1969 an den Grundgedanken der Sphärentheorie orientiert. War der Gegenstand des Verfahrens ursprünglich nur die Überprüfung der Verfassungsmäßigkeit des Volkszählungsgesetzes gewesen, ging das deutsche Bundesverfassungsgericht weit darüber hinaus und nahm die Entscheidung zum Anlass, allgemeine Grundsätze für die moderne Daten- und Informationsverarbeitung aufzustellen (vgl. Petersen 2000, S. 7).

> „Damit wird die Freiheit auf Selbstdarstellung realisiert, die davon ausgeht, daß jede/r mündige BürgerIn ein Recht auf Individualität hat. Als eigene Persönlichkeit soll jeder Mensch auf seine soziale Umwelt so einwirken können, daß er das Verhalten der Mitmenschen in Bezug auf seine Person beeinflusst. Das kann er aber nur, wenn er selbst bestimmt, welche Informationen über ihn existieren sollen. Dazu benötigt er das Recht auf informationelle Selbstbestimmung." (Egger 1990)

---

[2] Nach Ansicht der Autorin bezieht sich Vogelsang (1987) hier auf unklare Definitionen verschiedener möglicher Rollen, ebenso auf die Unklarheit der Gesamtheit der einer bestimmten Rolle gesellschaftlich zugewiesenen kulturellen Modelle.

[3] Nach Ansicht der Autorin bezieht sich Vogelsang (1987) hier auf die Frage von Spiel- und Handlungsräumen für den Einzelnen.

Dieser Ansatz kann als Weiterentwicklung der Rollentheorie aufgefasst werden, da dieser ebenfalls nicht daten-, sondern verarbeitungsorientiert ist und die persönlichen Lebensbereiche nicht in verschiedene Zonen der Schutzwürdigkeit einteilt, sondern die Schutzwürdigkeit von Informationen vom Verwendungszusammenhang abhängig macht (Egger 1990, S. 57).

Schon Steinmüller et al. (1971) erkannten eine Schwachstelle des Ansatzes der informationellen Selbstbestimmung: Existierten bei der Sphärentheorie Abgrenzungsschwierigkeiten hinsichtlich der einzelnen Sphären, so besteht die Schwierigkeit beim Recht auf informationelle Selbstbestimmung in der Beurteilung der Zulässigkeit eines Eingriffs in den geschützten Bereich. Eine genaue Definition von Rechtsgründen, die einen Informationseingriff rechtfertigen, sei bislang noch nicht präzise gelungen (vgl. Riepl 1994, S. 27) bzw. erscheint undurchführbar, da alle möglichen Fälle von vornherein bekannt sein müssten (vgl. z.B. Egger 1990). So bleiben Generalklauseln bestehen, mit der latenten Gefahr (wie auch bei der Sphärentheorie), „daß das R.i.S. [Recht auf informationelle Selbstbestimmung, Anm.] lediglich als quasi normativer Obersatz mißbraucht wird, um das im konkreten Fall wünschenswerte Ergebnis zu erhalten“ (Deutsch 1998, S. 81).

Neben den eben genannten Konzepten bestehen unterschiedliche weitere Privacy-Ansätze vor dem Hintergrund verschiedener Disziplinen. Erstmals ist die internationale wissenschaftliche Privacy-Diskussion zum Ende des 19. Jahrhunderts aufgekommen. Warren und Brandeis (1890) als bekannte Vertreter eines ersten Diskurses beanstandeten die damaligen aktuellen Entwicklungen, nämlich die Erfindung der Fotografie sowie das Aufkommen des Sensationsjournalismus. Sie definierten Privacy als eines der wichtigsten Menschenrechte (‚the right to privacy‘). Darauf aufkommend erfolgten erste öffentliche Diskussionen zur Frage des Rechts, alleine gelassen zu werden. Das Konzept des ‚right to be let alone‘ wurde in der Vergangenheit oftmals als zu vage (vgl. z.B. Solove 2002; Schoeman 1984; Allen 1988) bzw. als Widerspruch zur Grundidee einer ‚offenen Gesellschaft‘ (vgl. Brin 1998) kritisiert. Seit der zweiten Hälfte des 20. Jahrhunderts entwickelten sich einige weitere Theorien und Konzepte. Einer Systematisierung von Solove (2002) folgend finden sich dem erwähnten ‚right to be let alone‘ beispielsweise auch Ansätze wie ‚limited access to the self‘, ‚privacy as secrecy‘ (Geheimhaltung von Informationen), ‚control over personal information‘ (Oberhoheit über eigene Daten und Informationen und eigene Entscheidung über Weitergabe), ‚privacy as personality‘ sowie ‚privacy as intimacy‘, auf welche hier aus Platzgründen nicht näher eingegangen werden kann. Gleich ist allen diesen Konzepten, dass sie nur auf einen spezifischen Ausschnitt unseres Lebens, also z.B. auf Persönlichkeit, Intimität, Identität, Geheimhaltung oder Kontrolle über Information fokussieren (eine spezifische Analyse unterschiedlicher Konzepte findet sich z.B. in Kemp/Moore 2007). Um solche eindimensionalen Konzepte zu überwinden, werden zunehmend mehrdimensionale Ansätze diskutiert, welche verschiedene Dimensionen (physische, interaktionale, psychische, informationelle, soziale usw.) sowie Theorien kombiniert berücksichtigen (vgl. z.B. Burgoon et al. 1989; DeCew 1997; Laufer and Wolfe 1977; Detailliertes zu diesen Ansätzen: Hugl 2010). Solove (2002) kritisiert an diesen multidimensionalen (sogenannten Cluster-)Konzepten allerdings, dass sie zwar mehrere Ansätze kombinieren, nichtsdestoweniger „[…] still curcumscribe privacy based on the boundaries of each of the clustered conceptions“ (S. 1126), sich also nach wie vor zu sehr an traditionellen Konzepten anlehnen. In

seinem ‚pragmatic approach' empfiehlt er eine Berücksichtigung des jeweiligen Kontexts bzw. der Situation des Nutzers/der Nutzerin (z.B. spezifische Anwendung einer bestimmten Technologie wie das Eingeben von Privacy-Settings auf einer eCommerce-Website), einer datenschutzrelevanten Situation sowie konkrete Praktiken (social practices) des Umgangs mit Datenschutzfragen zu berücksichtigen (ebd., S. 1154).

Fazit

Individuelle Schutzanforderungen hinsichtlich personenbezogener Daten sind subjektiv zu bewerten. Mögliche Handlungsstrategien bewegen sich demnach auf einem Kontinuum zwischen ‚extremem Datenexhibitionismus' und ‚absoluter Datenvorsicht'. Ein Beispiel: Der US-Journalismusprofessor Jeff Jarvis (2011) twitterte über seine Prostataerkrankung, seine dadurch eingeschränkten sexuellen Möglichkeiten, ebenso über Windeln, die er nach einer Operation tragen musste. Er sieht sich als „public man", dementsprechend sei sein Leben wie ein offenes Buch und Privatsphäre etwas für Egoisten, da Krankheitsdaten beispielsweise der Wissenschaft helfen könnten, neue Behandlungsmöglichkeiten zu entwickeln. Grundsätzlich sei das Problem nicht die Information oder die Technik, sondern wie diese genutzt wird. Hans Gerhard Zeger von der österreichischen ARGE Daten (www.argedaten.at) sieht das naturgemäß konträr und rät zur Datenvorsicht: „Es sind nicht die Daten selbst problematisch, sondern ihre Bewertung" (Geets 30.03.2012). Um auf das Beispiel der Krankheitsdaten zurückzukommen: Zum einen zeigen aktuelle Entwicklungen, dass beispielsweise Anbieter von Lebensversicherungen, Arbeitgeber, Informationsbroker, Google u.a.m. an solchen Daten großes Interesse haben. Des Weiteren besteht die Gefahr, dass falsche oder als problematisch zu wertende Daten über eine Person nachteilig verarbeitet und deren Speicherung in Datenbanken erfolgt – eine Löschung bzw. Berichtigung zu erlangen scheint (z.B. auch durch Cloud-Computing-Anwendungen) nahezu unmöglich geworden zu sein. Ein weiteres diesbezügliches Problem sind unterschiedliche Datenkombinationspfade, welche für den Einzelnen – beispielsweise nach einem Verkauf an diverse Anbieter – nicht mehr nachvollziehbar sind.

Somit stellt sich die Frage nach der Möglichkeit einer Schließung (Nicht-Freigabe) unserer individuellen Daten. Durch unterschiedliche Technologienutzungen im Alltags- wie Berufsleben (Smartphones, Soziale Netzwerke usw.) sind wir Opfer unserer eigenen Bequemlichkeit geworden. Datensammlungen wie deren Kombinationen werden künftighin zunehmen. Datenschutzgesetze, meist aufgrund politischer Kompromisse zustande gekommen, hinken den technologischen Entwicklungen hinterher. Die Mündigkeit und Überlegtheit einer Person sollte zu ‚Self-Awareness' über den aktuellen Stand der technologischen Entwicklungen und Möglichkeiten führen. Erst aus dieser Kenntnis und Selbstverantwortung heraus kann der Einzelne – je nach subjektiver Positionierung auf dem eingangs erwähnten Kontinuum zwischen ‚Datenexhibitionismus' und ‚Datenvorsicht' – individuelle Verhaltensänderungen ableiten. Mögliche und einfach zu realisierende Maßnahmen wären beispielsweise die Nutzung von Sicherheitstools (Verschlüsselung u.a.), die Verhinderung von Datenspionage auf dem Mobiltelefon, die Nutzung sicherer Passwörter u.v.m. Neben der individuellen Awareness sind auch Unternehmen aufgefordert, ihre kritischen Daten vor Missbrauch zu schützen. Eine aktuelle Studie

(Symantec, 31.10.2011) untersuchte das Interesse zur Teilnahme an staatlichen ‚Critical Infrastructure Protection'-Programmen für Banken, Versicherungen, Energieversorger (z.B. Gas-, Telefon-, Internet-, Elektrizitäts-, Wasserversorger), Massentransportanbieter (z.B. Bahn), pharmazeutische Unternehmen u.a. sowie deren aktuell eingeschätzte Sicherheitslage. Das Ergebnis: Weitgehende Schutzmaßnahmen (dies trifft vor allem den Schutz kritischer Daten vor Cyberangriffen) sind aufgrund von Personal- und Budgetmangel hintangestellt – es wird vorrangig situativ auf aktuelle Bedrohungen reagiert. Nur etwa ein Fünftel der betroffenen Unternehmen beteiligt sich an entsprechenden Schutzprogrammen. Demnach werden Schutzprogramme kaum längerfristig und umfassend wahrgenommen.

Datenschutz ist mittlerweile „[…] ein großes schwarzes Loch, das nur noch Energie frisst", so die provokante Aussage des Münsteraner Informatikrechtlers Thomas Hoeren anlässlich des 11. Datenschutzkongresses im Mai 2010 in Berlin. Wir scheinen uns hin zu einer ‚Post Privacy'-Ära zu bewegen: Der individuelle Wert der Privatsphäre ändert sich durch neuere gesellschaftliche Strömungen (besonders die junge Generation fungiert als Treiber), unsere Bemühungen, individuelle oder Unternehmensdaten zu schützen, werden zunehmend aufwändiger, ebenso entstehen dem Einzelnen hohe (Opportunitäts-)Kosten wie Beweisprobleme bei der Durchsetzung seiner Rechte.

Literatur

Albrecht, Hans-Jörg (2011): *Schutzlücken durch Wegfall der Vorratsdatenspeicherung?* (2. Fassung). München: Max-Planck-Institut für ausländisches und internationales Strafrecht.

Albrecht, Peter-Alexis (2010): *Der Weg in die Sicherheitsgesellschaft. Auf der Suche nach staatskritischen Absolutheitsregeln.* Berlin: BWV.

Allen, Anita L. (1988): *Uneasy Access: Privacy for Woman in a Free Society.* Totowa, NJ: Rowman & Littlefield.

Amelung, Ulrich (2002): *Der Schutz der Privatheit im Zivilrecht.* Tübingen: Mohr Siebeck.

BDSG (20. Dez. 1990): *Bundesdatenschutzgesetz* (Deutschland) (Stand 2006).

Biermann, Kai (24.02.2011): *Was Vorratsdaten über uns verraten*. Hamburg: ZEIT ONLINE. Abgerufen unter: www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz [Stand vom 20.07.2012].

Böckenförde, Thomas (2003): *Die Ermittlung im Netz.* Tübingen: Mohr Siebeck.

Brin, David (1998): *The Transparent Society: Will Technology Force Us To Choose Between Privacy and Freedom.* Reading, MA: Addison-Wesley.

Burgoon, Judee K.; Parrot, Roxanne; Lepoire, Beth A.; Kelley, Douglas L.; Walther, Joseph B. & Perry, Denise (1989): Maintaining and Restoring Privacy through Communication in Different Types of Relationship. *Journal of Social and Personal Relationships,* 6 (2), pp. 131–158.

BVerfG (2. März 2010): *Urteil des Bundesverfassungsgerichts* (Deutschland), 1 BvR 256/08, Absätze 1 bis 345.

Dammann, Ulrich; Karhausen, Mark & Müller, Paul (1992): *Datenbanken und Datenschutz. Soziale Probleme.* Frankfurt: Campus.

DeCew, Judith (1997): *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca: Cornell University Press.

Deutsch, Markus (1998): *Die heimliche Erhebung von Informationen und deren Aufbewahrung durch die Polizei.* Heidelberg: C.F. Müller.

DSG (14. März 2002): *Datenschutzgesetz* (Schweiz).

DSG (19. Juni 1992): *Bundesgesetz über den Datenschutz* (Liechtenstein) (Stand 2006).

DSG (2000): *Datenschutzgesetz* (Österreich) (Stand 2011).

Egger, Edeltraud (1990): *Datenschutz versus Informationsfreiheit: Verwaltungstechnische und verwaltungspolitische Implikationen neuer Informationstechnologien.* Oldenburg, Wien.

EU (07.12.2000): *Charta der Grundrechte der Europäischen Union* (angepasste Fassung vom 12.12.2007).

EU (15.03.2006): *Richtlinie 2006/24/EG* des Europäischen Parlaments und des Rates.

EU (24.10.1995): *Richtlinie 95/46/EG* des Europäischen Parlaments und des Rates.

EU (28.01.1981): *Europäische Datenschutzkonvention*.

Europarat (4. November 1950): *Europäische Menschenrechtskonvention* (Konvention zum Schutze der Menschenrechte und Grundfreiheiten), zuletzt geändert durch Protokoll Nr. 14 vom 13.05.2004 m.W.v. 01.06.2010.

Foucault, Michel (2002): Die Wahrheit und die juristischen Formen. In: Defert, Daniel & Ewald, François (Hrsg.): *Schriften in vier Bänden. Dits et Ecrits (Bd. 2: 1970–1975).* Frankfurt am Main: Suhrkamp.

Geets, Siobhán (30.03.2012): *Öffentliche Debatten über Prostataleiden und volle Windeln*. Wien: Die Presse.

Habermas, Jürgen (1990 [1962]): *Strukturwandel der Öffentlichkeit.* Frankfurt am Main: Suhrkamp.

Hess, Thomas & Schreiner, Michel (2012): Ökonomie der Privatsphäre. *Datenschutz und Datensicherheit – DuD,* 36 (2), S. 105–109.

Hubmann, Heinrich (1953): *Das Persönlichkeitsrecht.* Köln, Graz: Böhlau.

Hugl, Ulrike (2010): Approaching the Value of Privacy: Review of theoretical privacy concepts and aspects of privacy management (paper no. 248). In: Library, A.E. (Ed.): *Proceedings of the 16th Americas Conference on Information Systems (AMCIS) (12–15 August)*. Lima.

Hugl, Ulrike (2011): Reviewing Person's Value of Privacy of Online Social Networking. *Internet Research,* 21 (4), S. 384–407.

Jäggi, Peter (1960): Fragen des privatrechtlichen Schutzes der Persönlichkeit. *Zeitschrift für Schweizerisches Recht,* 79 (II), S. 133a–141a.

Jarvis, Jeff (2011): *Public Parts.* New York: Simon & Schuster.

Kemp, Randal & Moore, Adam D. (2007): Privacy. *Library Hi Tech,* 25 (1), S. 58–78.

Krasnova, Hanna & Veltri, Natasha F. (2010): Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA. *43rd Hawaii International Conference on System Sciences (HICSS) (5–8 Jan.).* Koloa, Hawaii, IEEE.

Laufer, Robert S. & Wolfe, Maxine (1977): Privacy as a Concept and a Social Issue: A Multidimensional Development Theory. *Journal of Social Issues,* 33 (3), S. 22–42.

Lipton, Jacqueline D. (2010): Mapping Online Privacy. *Northwestern University Law Review,* 104 (2), *Paper no. 09–24*.

Luhmann, Niklas (1965): *Grundrechte als Institution.* Berlin: Duncker & Humblot.

Mallmann, Christoph (1976): *Datenschutz in Verwaltungs-Informationssystemen.* Oldenburg, München.

Müller, Paul J. (1975): *Funktionen des Datenschutzes aus sozialer Sicht.* DVR.

Pawlikowsky, Gerhart J. (1985): *Daten, Macht und Sicherheit – Über den Umgang mit Daten und Systemen.* Wien: Österreichischer Wirtschaftsverlag.

Petersen, Stefanie (2000): *Grenzen des Verrechtlichungsgebotes im Datenschutz.* Münster u.a.: Lit-Verlag.

PI (Ed.) (2007): *Surveillance Monitor 2007 – International Country Rankings.* London: Privacy International (PI).

PI/EPIC/CMCS (Ed.) (2010): *European Privacy and Human Rights (EPHR) 2010.* London: Privacy International (PI), Electronic Privacy Information Center (EPIC), Center for Media and Communications Studies (CMCS).

Reichmann, Gerhard (2004): Das Auskunftsrecht nach dem Datenschutzgesetz 2000 – Eine Fallstudie. *ZfV – Zeitschrift für Verwaltung,* 1529 (04), S. 752–757.

Riepl, Frank (1994): *Informationelle Selbstbestimmung im Strafverfahren.* Tübingen: Mohr Siebeck.

Rohlf, Dietwalt (1980): *Der grundrechtliche Schutz der Privatsphäre. Zugleich ein Beitrag zur Dogmatik des Art. 2 Abs. 1 GG.* Berlin: Duncker & Humblot.

Schaumann, Philipp (29.04.2012): Werden unsere Surf-Daten verkauft? *66. Newsletter sicherheitskultur.at*.

Schoeman, Ferdinand D. (1984): Privacy: Philosophical Dimensions of the Literature. In: Schoeman, Ferdinand D. (Ed.) *Philosophical Dimensions of Privacy. An Anthology.* Cambridge: Cambridge University Press.

Scholler, Heinrich (1967): *Person und Öffentlichkeit.* München: Beck.

Seidel, Ulrich (1972): *Datenbanken und Persönlichkeitsrecht unter besonderer Berücksichtigung der amerikanischen Computer Privacy.* Köln: Schmidt.

Solove, Daniel J. (2002): Conceptualizing Privacy. *California Law Review,* 90, S. 1087–1156.

Solove, Daniel J. (2007): ‚I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review,* 44, pp. 745–772.

Solove, Daniel J. (2008): Understanding Privacy. *GWU Legal Studies Research Paper No. 420 (Harvard University Press)*, S. 1–24.

Steinke, Ronen (16.08.2010): Der Wunsch nach Härte (Interview mit Peter-Alexis Albrecht). Berlin: *taz.de*.

Steinmüller, Wilhelm (1984): *Datenschutz. ADV-Recht. ADV-Recht I: Automatisierte Datenverarbeitung.* München: Goldmann.

Steinmüller, Wilhelm; Lutterbeck, Bernd; Mallmann, Christoph; Harbort, U.; Kolb, G. & Schneider, J. (1971): *Grundfragen des Datenschutzes – Gutachten im Auftrag des Bundesministeriums des Inneren.* Bonn: BT-Drucksachen VI/3826.

Symantec (31.10.2011): *Symantec Critical Infrastructure Protection Survey. Global Findings.* Mountain View, CA: Symantec.

Theißen, Sascha (2009): *Risiken informations- und kommunikationstechnischer (IKT) Implantate im Hinblick auf Datenschutz und Datensicherheit:* Karlsruhe: Univ.-Verl. Karlsruhe.

Tichy, Gunther & Peissl, Walter (2001): *Beeinträchtigung der Privatsphäre in der Informationsgesellschaft*. ITA-manu:script, S. 1–19.

Uhl, Florian (2008): Überwachen. In: Sperl, Gerfried & Steiner, Michael (Eds.): *Watching you. Kontrolle, Datenhandel, Überwachung.* Graz: Leykam.

Vogelsang, Klaus (1987): *Grundrecht auf informationelle Selbstbestimmung?* Baden-Baden: Nomos.

Warren, Samuel D. & Brandeis, Louis D. (1890): The Right to Privacy. *Harvard Law Review,* 4 (5), S. 193–220.