Zeitschrift für Datenrecht und Informationssicherheit

digma

www.digma.info 11. Jahrgang, Heft 2, Juni 2011

Schwerpunkt:

Location Based Services

fokus: Datenschutz in ortsbasierten Diensten
fokus: Location Privacy in RFID-Systemen
report: Offene Deklaration von Web Analytics



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth

Schulthess §

inhalt

fokus

Schwerpunkt:
Location Based Services

auftakt
Menschliches Versagen
von Michael Waidner Seite 49

Wo war wer wann? Ihr Smartphone weiss es
von Günter Karjoth Seite 52

Datenschutz in ortsbasierten Diensten
von Martin Werner Seite 54

Datenschutzgerechte ortsbasierte Dienste
von Jan Zibuschka und Eleny Kosta Seite 60

zwischentakt
Um Dimensionen brisanter: Facebooks Gesichtserkennung
von Beat Rudin Seite 65

Datenschutz durch Selbstregulierung?
von Kurt Pärli Seite 66

Location Privacy in RFID-Systemen
von Christian Wachsmann und Ahmad-Reza Sadeghi Seite 70

Schutz von Lieferketten mit RFID-Tags
von Erik-Oliver Blass und Refik Molva Seite 76

agenda Seite 79

Datenschutz in ortsbasierten Diensten

Ortsbasierte Dienste ermöglichen eine Nutzung von Mobiltelefonen als persönliche Informationsquelle und helfen dabei, die für eine Person relevante Information aus der Datenflut des Internets herauszufiltern. Der Autor erklärt die Probleme von ortsbasierten Diensten und erläutert mögliche Lösungsansätze.

Datenschutzgerechte ortsbasierte Dienste

Bei vielen ortsbasierten Diensten besteht die Gefahr, dass die Diensteanbieter exzessiven Zugang zu den personenbezogenen Daten über die Nutzer erhalten. Wie können ortsbasierte Dienste rechts- und datenschutzkonform gestaltet werden?

Location Privacy in RFID-Systemen

RFID-Systeme ermöglichen die automatische drahtlose Identifikation von Objekten und stellen eine allgegenwärtige Technologie mit zahlreichen Anwendungsmöglichkeiten dar. Welches sind die Sicherheits- und Datenschutzanforderungen an solche Anwendungen?

Schutz von Lieferketten mit RFID-Tags

Das Einschleusen von Fälschungen stellt heute eine grosse Gefahr für Warenlieferketten dar. Das System «Tracker» setzt einfache RFID-Tags als Ersatz für herkömmliche Barcodes ein, um Lieferketten gegen eingeschleuste Fälschungen abzusichern und ausserdem neugierige Mitbewerber davon abzuhalten, die eigene Warenlieferkette auszuspähen.

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer J. Schweizer, Dr. Günter Karjoth

Redaktion: Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

Zustelladresse: Redaktion digma, per Adr. Datenschutzbeauftragter des Kantons Basel-Stadt, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, Fax +41 (0)61 201 16 41, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 131.00 (inkl. Versandspesen), Einzelheft: CHF 42.00

Anzeigenmarketing: Publicitas Publimag AG, Mürtschenstrasse 39, Postfach, CH-8010 Zürich
Tel. +41 (0)44 250 31 31, Fax +41 (0)44 250 31 32, www.publimag.ch, service.zh@publimag.ch

Herstellung: Schulthess Juristische Medien AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 99, Fax +41 (0)44 200 29 98, www.schulthess.com, zs.verlag@schulthess.com

Offene Deklaration von Web Analytics

Website-Betreiber sammeln und analysieren eine Fülle an Daten, ohne dies offen zu deklarieren. Datenschutz-Gütesiegel wie EuroPriSe erhöhen die Transparenz beim Einsatz von Web Analytics.

Häusliche Gewalt

StPO und OHG regelten die Mitteilung von Name und Adresse von Opfern an eine Beratungsstelle abschliessend und damit bleibe für kantonales Recht kein Raum, kritisieren Kettiger/Schwander einen in digma 2010.4 erschienenen Artikel von Glockengiesser/Stämpfli. Stimmt nicht ganz, wenden die beiden Autorinnen des ersten Beitrages ein, und weisen darauf hin, dass in Fällen von häuslicher Gewalt ausserhalb des Geltungsbereichs der StPO durchaus kantonaler Regelungsspielraum und -bedarf besteht.

Raserei auf der Strasse

Wer mit seinem Auto auf der Strasse zu schnell unterwegs ist, riskiert, geblitzt zu werden. Höchste Zeit, dass das Strassenverkehrsgesetz geändert und die Höchstgeschwindigkeit abgeschafft werden. Eine abwegige Argumentation? Mitnichten, wenn man die Reaktion auf ein Bundesverwaltungsgerichtsurteil zu einer anderen «Raserei auf der Strasse» hört …

report

Transparenz im Internet
Offene Deklaration von Web Analytics
von Darius Zumstein, Aleksandar Drobnjak und Andreas Meier — Seite 80

Follow-up: Häusliche Gewalt
Häusliche Gewalt: Vom Bund geregelt
von Daniel Kettiger und Marianne Schwander — Seite 86

Follow-up: Häusliche Gewalt
Häusliche Gewalt: Es darf diskutiert werden
von Iris Glockengiesser und Sandra Stämpfli — Seite 90

Transfer
Smartphones als Virenschleuder?
von Roland Portmann — Seite 92

forum

privatim
Aus den Datenschutzbehörden
von Sandra Stämpfli — Seite 94

schlusstakt
Raserei auf der Strasse
von Bruno Baeriswyl — Seite 96

cartoon
von Reto Fontana

Datenschutz durch Selbstregulierung?

Auslegeordnung, Probleme und Regulierungsperspektiven bei Location Based Services



Prof. (FH) Dr. iur. Kurt Pärli, Leiter Zentrum für Sozialrecht, Zürcher Hochschule für angewandte Wissenschaften, Winterthur, und Privatdozent für Arbeits- und Sozialversicherungsrecht, Universität Sankt Gallen. kurt.paerli@zhaw.ch

Schranken der Datenbearbeitung und Stärkung der Durchsetzungsrechte braucht es vor allem dort, wo missbräuchliche Datenbearbeitung die Betroffenen in ihrer Existenz bedroht.

Die potenziellen Anwendungsfelder für Location Based Services sind praktisch unbegrenzt. Wie bei jeder technischen Innovation finden sich Stimmen, die euphorisch wirtschaftliche, individuelle und gesellschaftliche positive Aspekte betonen. Aus datenschutzrechtlicher Perspektive überwiegen kritische Töne[1]. Insbesondere wird gefragt, ob die bestehenden Regulierungsansätze im Datenschutzrecht den Anforderungen gerecht werden, die sich durch die rasante Entwicklung bei den Informations- und Kommunikationstechnologien ergeben[2].

Location Based Services bilden lediglich eine der zahlreichen Herausforderungen, mit denen sich Datenschutzrecht konfrontiert sieht. Eine grundlegende Reform des – gerade erst revidierten – Datenschutzgesetzes muss einerseits die Durchsetzung der datenschutzrechtlichen Prinzipien erleichtern und andererseits den ökonomischen und technologischen Rahmenbedingungen vermehrt Beachtung schenken[3]. Die nachfolgenden Ausführungen gehen u.a. der Frage nach, ob spezifische gesetzliche Regelungen für Location Based Services notwendig sind oder ob (regulierte) Selbstregulierung eine Alternative darstellt.

Heutiger Rechtsrahmen für Location Based Services

In rechtlicher Hinsicht sind bei Location Based Services je nach Technologie sowohl das Fernmeldegesetz (FMG) wie das Datenschutzgesetz (DSG) zu beachten. Das FMG regelt die fernmeldetechnische Übertragung von Informationen umfassend, insbesondere ist auch der Mobilfunkt erfasst[4]. Nach Art. 45b FMG ist die Bearbeitung von Standortdaten über Abrechnungszwecke hinaus nur zulässig, wenn die betroffene Person in die Bearbeitung ausdrücklich einwilligt.

Das DSG – entstanden vor dem Hintergrund von Befürchtungen, die bestehenden Persönlichkeitsschutzinstrumente vermöchten angesichts der technologischen Innovationen im Bereich elektronischer Datenbearbeitung nicht angemessenen Schutz zu gewähren – definiert in Art. 3 lit. e DSG den Begriff des Bearbeitens von Personendaten. Unter «bearbeiten» ist jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren zu verstehen, das DSG ist insoweit technologieneutral. Bei den durch Location Based Services gewonnenen Daten besteht eine Problematik darin, dass ein Personenbezug oft erst durch die Zusammenführung verschiedener Daten geschaffen wird, die isoliert betrachtet noch keine Personendaten sind. Soweit ein Personenbezug der Daten vorliegt, finden die Datenbearbeitungsgrundsätze des DSG wie die Bearbeitung nach Treu und Glauben, die Zweckbindung, Verhältnismässigkeit, Richtigkeit und Datensicherheit Anwendung[5].

Auch nach dem DSG ist die Datenbearbeitung zulässig, wenn die betroffene Person in die Bearbeitung ausdrücklich einwilligt (Art. 6 Abs. 2 lit. b, Art. 13 Abs. 1, Art. 17 Abs. 2 lit. c, Art. 19 Abs. 1 lit. b DSG). Wenn private Anbieter von Location Based Services besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeiten oder regelmässig Personendaten an Dritte weitergeben, müssen sie zudem ihre Datensammlung beim Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) anmelden (Art. 11a Abs. 3 lit. a und lit. b DSG).

Sofern und soweit Location Based Services in Arbeitsverhältnissen eingesetzt werden, sind einschlägige arbeitsrechtliche Persönlichkeits- und Gesundheitsvorschriften zu beachten (Art. 328 OR, Art. 6 Arbeitsgesetz und Art. 26 Verordnung 3 zum Arbeitsgesetz). In BGE 130 II 425 hat das Bundesgericht entschieden, dass ein GPS-Einsatz nur für die Kontrolle des Arbeitszeitmanagements zulässig sei, wobei die Informationen nicht in Echtzeit, sondern nur nachträg-

lich, durch Vergleich mit den Arbeitsrapporten ausgewertet werden dürfe[6].

Datenschutzrecht basiert auf dem Grundrecht der informationellen Selbstbestimmung; die Bearbeitung von Personendaten soll die Autonomie der Lebensgestaltung der betroffenen Personen gewährleisten. Auf diesem Hintergrund basieren die Durchsetzungsmechanismen des Datenschutzgesetzes, die auf das Prinzip des «Selbstdatenschutzes» und der individualrechtlichen Klagen gegen Datenschutzverletzungen abstützen (Auskunftsrecht nach Art. 8–10 DSG, Klagen bei Persönlichkeitsverletzungen, Art. 15 DSG, Ansprüche bei Datenschutzverletzungen durch Bundesorgane, Art. 25 DSG).

Nimmt man die Anzahl der Gerichtsentscheide zu individualrechtlichen Klagen gegen Datenschutzverletzung als Indikator für die Wirksamkeit des Datenschutzrechts, ist das Ergebnis ernüchternd: Trotz der beträchtlichen Anzahl an Datenschutzverletzungen – man denke nur an das häufig nicht eingehaltene Zweckbindungs- und Transparenzgebot – sind kaum datenschutzrechtliche Entscheide bekannt, die Klagen von Individuen betreffen[7]. Das kann verschiedene Ursachen haben. Längst nicht jede Datenschutzverletzung führt bei den betroffenen Personen zu schweren Nachteilen. Zudem wirken Verfahrenshürden abschreckend (Beweisprobleme, Kostenrisiken, fehlender Schaden oder schwierig zu beweisende Kausalität zwischen der Datenschutzverletzung und dem Schaden). Darüber hinaus besteht das eminent praktische Problem, dass bei einem gerichtlichen Vorgehen gegen eine Datenschutzverletzung genau die Information (erneut) zum Thema gemacht werden muss, die von der betroffenen Person gerade hätte geheim gehalten werden wollen.

Fehlt es an der praktischen Wirksamkeit des individualrechtlichen Datenschutzes, ist die Rolle der Aufsichtsbehörden umso wichtiger. Die Durchsetzungsmöglichkeiten des im Anwendungsbereich des DSG zuständigen EDÖB sind indes beschränkt. Er nimmt lediglich eine Beratungs- und Informationsfunktion wahr und kann gegenüber Privaten oder dem zuständigen Bundesorgan Empfehlungen abgeben und gerichtlich sanktionieren lassen (Art. 27–30 DSG). De lege ferenda werden für den EDÖB verschärfte Sanktionsmöglichkeiten (substanzielle Bussen), mehr personelle Ressourcen und Kompetenzen für rechtlich verbindliche konkrete Handlungsanweisungen gefordert[8].

Selbstregulierung als Ausweg aus der Datenschutzrechtskrise?

Seit mehreren Jahren wird die Debatte um ein der technologischen Entwicklung und den Bedrohungen für den Schutz der Persönlichkeit angepasstes Datenschutzrecht durch Vorschläge zur Selbstregulierung angereichert. Fokussiert wird dabei die «regulierte Selbstregulierung», die zwischen den Polen rein privater Selbstregulierung und klassischer staatlicher Steuerung über Ge- und Verbote anzusiedeln ist[9]. Bei «regulierter Selbstregulierung» definiert der Staat Regulierungsziele und den rechtlichen Rahmen, innerhalb dessen ein Ziel realisiert werden soll. Die Umsetzung und Konkretisierung dieses Regelungsziels wird danach betroffenen und beteiligten Privaten überlassen[10].

Der Personenbezug wird oft erst durch die Zusammenführung verschiedener Daten geschaffen, die isoliert betrachtet noch keine Personendaten sind.

Im revidierten DSG sind erste Ansätze solcher Selbstregulierungskonzepte enthalten. In Art. 11 DSG ist ein freiwilliges Zertifizierungsverfahren vorgesehen. Wer nach dem in der Verordnung und in einer Richtlinie beschriebenen Verfahren ein solches «Datenschutzgütesiegel» erhält, wird von der Pflicht der Registrierung in die Datensammlung des EDÖB befreit (Art. 11a Abs. 5 lit. f DSG)[11]. Keine Anmeldung muss weiter vornehmen, wer in seinem Betrieb einen Datenschutzbeauftragten bezeichnet hat, der unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und ein Verzeichnis der Datensammlungen führt (Art. 11 Abs. 5 lit. e DSG)[12].

Diese ersten Selbstregulierungsansätze im DSG werden in der schweizerischen Lehre als zu wenig weit gehend kritisiert[13]. Andere Stimmen

Kurz&bündig

Bei Location Based Services sind je nach Anwendungsbereich und bei vorhandenem Personenbezug sowohl die Schranken des Fernmeldegesetzes (FMG) wie das Datenschutzgesetz (DSG) zu beachten. Die Durchsetzung datenschutzrechtlicher Grundprinzipien (Rechtmässige Beschaffung, Transparenz, Zweckbindung, Datensicherheit, Verhältnismässigkeit und Einwilligung) erweist sich in der Praxis – nicht nur, aber auch bei Location Based Services – als utopisch. Die mit der Personenortung einhergehenden Datenschutzprobleme werden regelmässig als Indikator für eine eigentliche Datenschutzkrise wahrgenommen. Als Ausweg werden Konzepte «regulierter Selbstregulierung», eine Stärkung der datenschutzrechtlichen Aufsicht und die Verbesserung der individualrechtlichen Durchsetzungsrechte gefordert. Besonders notwendig ist die Verbesserung des Persönlichkeitsschutzes in den Bereichen Arbeit, Miete, Versicherung und Gesundheit. Hier kann die Missachtung der Datenbearbeitungsgrundsätze für die Betroffenen existenziell bedrohende Auswirkungen haben.

zweifeln grundsätzlich am Nutzen jeder Zertifizierung. Bei einer Datenschutzzertifizierung würden lediglich die organisatorischen und technischen Voraussetzungen für ein Datenschutzmanagement überprüft, nicht kontrolliert würde indes, ob der Datenschutz im fraglichen Betrieb tatsächlich eingehalten werde[14]. Für eine fundierte Aussage über die Wirkung dieser Instrumente ist es noch zu früh. Erfahrungen in den USA und anderswo zeigen, dass eine allzu optimistische Einschätzung des Potenzials der (regulierten) Selbstregulierung im Bereich Datenschutz fehl am Platz ist[15]. Zu beachten gilt auch, dass Datenschutz-Selbstregulierung unerwünschte Nebeneffekte nach sich ziehen kann. So berichtet eine Studie aus Grossbritannien über die Bildung kartellartiger Strukturen als Folge des Zusammenwirkens von Unternehmen zum Zwecke der Datenschutz-Selbstregulierung[16].

Bessere Regulierung – und am richtigen Ort

Die Defizite und Grenzen des heutigen Datenschutzrechts sind seit längerer Zeit erkannt. Bald werden Location Based Services nicht mehr aus unserem Alltag wegzudenken sein. Die Praxis der entsprechenden Datentransfers kontrastiert scharf mit datenschutzrechtlichen Kernprinzipien wie dem der Einwilligung der betroffenen Person, der Transparenz, dem Zweckbindungsgebot sowie dem Gebot der verhältnismässigen Datenbearbeitung[17].

Fussnoten

1 Rolf. H. Weber/Annette Willi, IT-Sicherheit und Recht, Zürich, 2006, 253; siehe auch: Eidg. Datenschutzbeauftragter, Geolokalisierung per Handy, Quelle: <http://www.edoeb.admin.ch/dokumentation/00445/00471/01695/index.html?lang=de> (Zugriff: 21.4.2011).

2 «Mit rostiger Flinte unterwegs in virtuellen Welten?» betitelt der Autor Stephan Brunner seine Rundschau zum Stand und den Perspektiven des Datenschutzrechts im Lichte aktueller und künftiger technologischer Herausforderungen, siehe: Stephan Brunner, Mit rostiger Flinte unterwegs in virtuellen Welten?, Jusletter 4. April 2011.

3 Brunner (Fn. 2), Rz 51–65; Beat Rudin, Datenschutz in der Schweiz – Herausforderungen und Perspektiven, in: Datenschutzbeauftragter des Kantons Zürich (Hrsg.), Herausforderung Datenschutz – 10 Jahre Datenschutzgesetz – eine Zwischenbilanz, Zürich, Basel, Genf, 2005, 80 ff.

4 Urs Gasser, Rechtliche Aspekte des M-Commerce, SZW 2002, 18.

5 Stéphane Bondallaz, La protection des personnes et leurs données dans les télécommunacations, Zürich 2007, N 1440; zum Verhältnis FMG und DSG siehe auch Gasser (Fn. 4), 19; Daniel Kettiger, Rechtliche Rahmenbedingungen für Location Sharing Systeme in der Schweiz, Jusletter 9. August 2010, Rz 27.

6 Zur Kritik an dieser Entscheidung (und vor allem an der Interpretation durch die Medien) siehe Amédéo Wermelinger, GPS-Überwachung von Mitarbeitenden, digma 2005, 96 ff.

7 Siehe die Übersicht zu datenschutzrechtlichen Urteilen 1994–2003: Rolf H. Weber, Rechtsprechung zum Datenschutz – Rückblick auf zehn Jahre Rechtsprechung im Datenschutzbereich, digma 2003, 76–78.

8 Siehe dazu Brunner (Fn. 2), Rz 53.

9 Zur Selbstregulierung siehe grundsätzlich Arnold Marti, Selbstregulierung anstelle staatlicher Gesetzgebung?, ZBl 2000, 562 ff.

10 Zur Selbstregulierung im Bereich Datenschutz siehe grundsätzlich: Talidou Zoi, Regulierte Selbstregulierung im Bereich des Datenschutzes, Frankfurt a.Main, 2005; Sven Polenz, RFID-Techniken und Datenschutzrecht – Perspektiven der Regulierung, Chemnitz, 2009; Lukas Fässler, Datenschutz durch Selbstregulierung, Vortrag anlässlich der Veranstaltung des Schweizer Forums für Kommunikationsrecht SF am 27. Oktober 2003 in Zürich, <http://www.fsdz.ch/publikationen/faessler/Fachvortrag%20SF%20Kommunikationsforum%20-%20Datenschutz%20durch%20Selbstregulierung%20-%2027-10-2003.pdf> (Zugriff: 25.4.2011).

11 Das Zertifizierungsverfahren ist in der Verordnung über die Datenschutzzertifizierung (VDSZ, SR 235.13) geregelt und wird in Richtlinien des EDÖB weiter konkretisiert; siehe dazu Caroline Gloor Scheidegger, Datenschutzzertifizierung: Stand der Dinge, digma 2010, 74–75.

12 Auch dies stellt eine Form der Selbstregulierung dar.

13 Fässler (Fn. 10), 19.

14 David Rosenthal, in: Rosenthal/Jöhri, Handkommentar zum Datenschutzgesetz, Zürich, Basel, Genf 2008, N 1, N 13 ff. zu Art. 11 DSG.

15 Alexander Rossnagel, Regulierung und Selbstregulierung im Datenschutz, in: Kubicek et al. (Hrsg.), Global@home – Informations- und Dienstleistungsstrukturen der Zukunft, Jahrbuch Telekommunikation und Gesellschaft 2000, Band 8, Heidelberg, 2000, 385–391.

16 Wolfgang Schulz/Thorsten Held, Regulierte Selbstregulierung als Form modernen Regierens. Arbeitspapiere des Hans-Bredow-Instituts Nr. 10, Hamburg, 2002, C-15, 97 (Quelle: <http://www.hans-bredow-institut.de/webfm_send/53>; Zugriff 25.4.2011); Joachim Jacob/Helmut Heil, Datenschutz im Spannungsfeld von staatlicher Kontrolle und Selbstregulierung, in: Bizer et al. (Hrsg.) Freundesgabe für Büllesbach Alfred, Stuttgart 2002, 213–223.

17 Rudin (Fn. 3), 74 f.; Bruno Baeriswyl, Geschichten aus dem Wilden Westen. Der Datenschutz im privatrechtlichen Bereich geht seine eigenen Wege: Der Grundrechtsschutz bleibt auf der Strecke, digma 2010, 140 ff.

18 Die Ergebnisse der Evaluation werden im Verlaufe dieses Jahres erwartet.

19 Brunner (Fn. 2), Rz. 41–45; Rudin (Fn. 3), 85–86.

20 Brunner (Fn. 2), Rz. 56 ff.

21 Brunner (Fn. 2), Rz. 26 ff.; Marie-Theres Tinnefeld, Einbrüche der Privatheit im digitalen Netz – Grundprobleme und technologische Ansätze des Grundrechtsschutzes, Jusletter 1. September 2010.

22 Brunner (Fn. 2), Rz. 26.

23 Bundesgesetz vom 8. Oktober 2004 über genetische Untersuchungen beim Menschen (GUMG), SR 810.12.

24 Zu den arbeits- und versicherungsrechtlich relevanten Bestimmungen des GUMG siehe Kurt Pärli, Die arbeits- und versicherungsrechtlichen Bestimmungen des Bundesgesetzes über genetische Untersuchungen (GUMG), AJP 2007, 79–88.

Die Wirksamkeit des DSG wird zurzeit evaluiert. Teil der Evaluation bildet auch, ob sich der technologieneutrale Ansatz des DSG bewährt hat[18]. In der Lehre wird angeregt, die Technologieneutralität zu überwinden und durch Regulierung von Architekturen die technische Ausgestaltung von Systemen von Anfang an datenschutzmässig in die richtige Richtung zu lenken. Der Gesetzgeber kann hier steuernd einwirken und die Kosten-Nutzen-Rechnung solcher Innovationen beeinflussen[19]. Solche Konzepte verdienen eine nähere Prüfung. Wie weit hier auch Formen regulierter Selbstregulierung Platz finden sollen, kann offenbleiben. Zu vermeiden sind Selbstregulierungsleerläufe, die für die Datenbearbeiter lediglich unnötigen administrativen Aufwand bedeuten und den von der Datenbearbeitung betroffenen Personen bestenfalls Datenschutzkonformität vorgaukeln. Weiter ist bei regulierter Selbstregulierung zu beachten, dass die Normsetzung nicht nur den Produkteherstellern oder den Wirtschaftsverbänden überlassen wird, sondern vielmehr der Einbezug von Konsumenten-, Arbeitnehmer-, Versicherten oder Patientenorganisationen zwingend vorgeschrieben wird.

Die Defizite des heutigen Datenschutzrechts bestehen schwergewichtig in der Rechtsdurchsetzung. Vorschläge zur Verbesserung liegen vor: Stärkung der datenschutzrechtlichen Aufsicht (u.a. mit härteren Sanktionsmöglichkeiten) und Verbesserung der individualrechtlichen Durchsetzungsmöglichkeiten durch Verbandsklagerechte[20].

Verschiedene Autoren weisen darauf hin, dass im Datenschutzrecht nicht nur ein Ausbau, sondern auch und vor allem eine Verwesentlichung der Datenschutzrechte ansteht[21]. Die Rede ist von einem «Post-Privacy-Zeitalter» und davon, dass sich der Charakter der Privatsphäre im Lichte der omnipräsenten Online-Dienste wandle[22]. Ob allerdings künftiges Datenschutzrecht einem behaupteten oder herbeigeredeten grundlegend neuen Verständnis von Privatsphäre entsprechen muss, bedarf fundierter Analyse und einer breiten gesellschaftlichen Diskussion.

Geschützt werden soll die Persönlichkeit vor Datenbearbeitung dort, wo dies einem gesellschaftlichen Konsens entspricht; vordinglich dort, wo die Missachtung datenschutzrechtlicher Grundsätze die betroffenen Personen in ihrer beruflichen und sozialen Existenz gefährdet. Besonders heikel sind die Bereiche Arbeit, Miete, Gesundheit, Versicherung: Hier braucht es klare gesetzliche Schranken des Zulässigen und eine effiziente Rechtsdurchsetzung durch Beweislasterleichterungen und wirksame Sanktionen.

Solche Schranken der zulässigen Datenbearbeitung und prozessuale Regelungen zur erleichterten Durchsetzung persönlichkeitsrechtlicher Ansprüche müssen nicht unbedingt (nur) im DSG verankert werden. Als Beispiel kann das Bundesgesetz über genetische Untersuchungen beim Menschen (GUMG)[23] aufgeführt werden. Das GUMG enthält für den Umgang mit genetischer Information in Arbeits- und Versicherungsverhältnissen strenge Nachfrage- und Verwertungsverbote und beschränkt deshalb die zulässige Bearbeitung von Daten, die genetische Informationen enthalten[24].

Soweit die Gefährdung der Persönlichkeitsrechte durch Datenbearbeitung im Arbeitsverhältnis erfolgt, können auch normative Bestimmungen in Gesamtarbeitsverträgen ein Mittel darstellen, um eine sinnvolle Begrenzung der Beschaffung und insbesondere auch der Verwertung von Arbeitnehmerpersonendaten vorzunehmen. Eine bessere Rechtsdurchsetzung im Bereich des arbeitsrechtlichen Datenschutzes liesse sich weiter durch eine Beweislasterleichterung bei Klagen wegen Verletzung von Art. 328 und 328b OR realisieren. Zu prüfen ist auch, ob Pönalentschädigungen, wie sie bei missbräuchlicher Kündigung vorgesehen sind, ein adäquates Mittel zur Stärkung des Datenschutzrechts wären. Vermehrt in die Pflicht zu nehmen sind zudem die Vollzugsorgane des Arbeitsgesetzes. Im bereits erwähnten GPS-Fall BGE 130 II 425 wandte sich ein Mitarbeiter des Unternehmens an die kantonalen Arbeitsschutzbehörden, die in der Folge die Entfernung des Lokalisierungssystems vom Dienstwagen anordneten. Es kann an dieser Stelle nicht verschwiegen werden, dass – ähnlich wie im Bereich des Datenschutzes – auch beim Arbeitsschutz ein Vollzugsdefizit besteht. Dies soll die verantwortlichen Akteure in der Verwaltung, der Politik und der Justiz nicht daran hindern, die grundrechtliche Schutzpflicht im Bereich Daten- und Persönlichkeitsschutz ernst zu nehmen und je in ihrem Kompetenzbereich ihre Verantwortung wahrzunehmen. ■

Schranken der Datenbearbeitung und prozessuale Regelungen zur erleichterten Durchsetzung persönlichkeitsrechtlicher Ansprüche müssen nicht unbedingt (nur) im DSG verankert werden.

Zeitschrift für Datenrecht und Informationssicherheit
digma
www.digma.info
erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 131.00** (inkl. Versandkosten)

Name Vorname

Firma

Strasse

PLZ Ort Land

Datum Unterschrift

Bitte senden Sie Ihre Bestellung an:
Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich
Telefon +41 44 200 29 19
Telefax +41 44 200 29 18
E-Mail: zs.verlag@schulthess.com
Homepage: www.schulthess.com

Schulthess §