Zeitschrift für Datenrecht und Informationssicherheit

digma

www.digma.info 10. Jahrgang, Heft 4, Dezember 2010

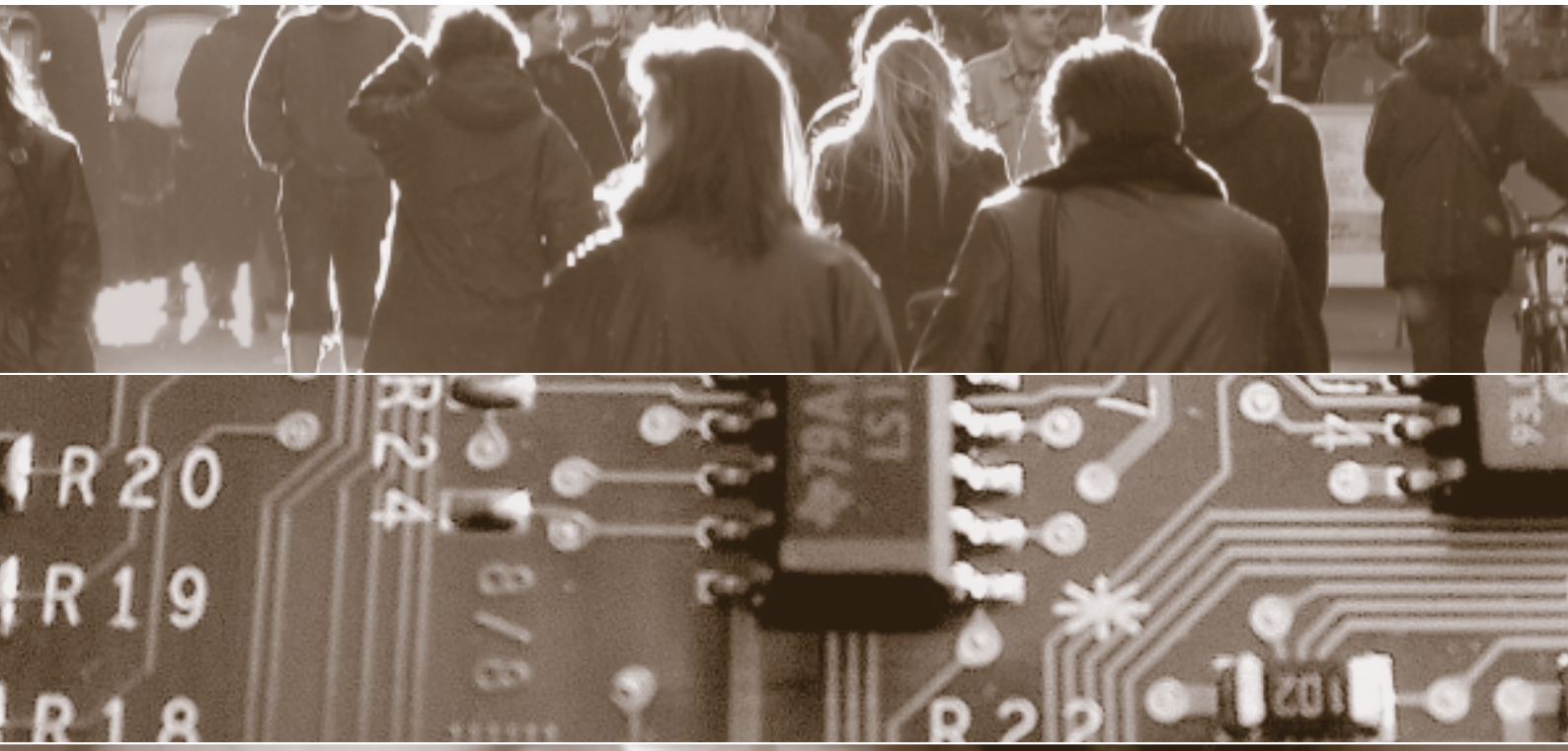
Schwerpunkt:

2001–2010

fokus: Datenschutzkonzept auf dem Prüfstand

fokus: Zehn Jahre IT Security: Was hat sich bewegt?

report: Häusliche Gewalt: Daten- oder Opferschutz?



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

Schulthess §

inhalt

fokus

Schwerpunkt:
2001–2010

Datenschutzkonzept auf dem Prüfstand

Das Konzept des öffentlich-rechtlichen Datenschutzes ist seit den 1980er-Jahren praktisch unverändert geblieben. Wie hat es sich angesichts der Herausforderungen des ersten Jahrzehnts (E-Themen, 9/11 und Sicherheit, Öffentlichkeitsprinzip und Schengen) bewährt? Wo liegen die Schwächen?

Geschichten aus dem Wilden Westen

Der Datenschutz im privatrechtlichen Bereich steht damit an einem entscheidenden Punkt: Nur wenn Transparenz über die Datenbearbeitungen geschaffen wird, können die Konsumenten entscheiden, ob und wie sie ihre Datenschutzrechte einfordern wollen.

Weder Anonymität noch Radiergummi

Unsere Daten, die wir mehr oder weniger freiwillig im Web hinterlassen, sind zu einer Goldgrube geworden. Warum sind wir Nutzer schutzlos geblieben? Ein Rückblick auf zehn Jahre Datenschutz und Identitätsmanagement im Internet.

10 Jahre IT Security: Was hat sich bewegt?

Welche Voraussagen haben sich als richtig erwiesen und welche Schlussfolgerungen lassen sich den rückblickenden Beobachtungen entnehmen? Ein Streifzug durch zehn Jahre Angriff und Verteidigung.

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 99.00 (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

Häusliche Gewalt: Daten- oder Opferschutz?

Häusliche Gewalt ist ein Phänomen, welchem mit geeigneter Beratung begegnet werden kann. Die kantonalen Fachstellen könnten mit pro-aktiver Kontaktaufnahme eine Hemmschwelle überschreiten, verfügen aber oftmals nicht über genügende gesetzliche Grundlagen, um die notwendigen Informationen für die Kontaktaufnahme von anderen Behörden zu erhalten. Die Autorinnen zeigen auf, wie sich proaktive Beratung und Datenschutz vereinen lassen.

Security Management für IT-Dienstanbieter

On-demand-Anwendungen basieren auf einer Vielzahl von Diensten unterschiedlicher Anbieter und Funktion. Das EU-Forschungsprojekt PoSecCo will Dienstanbieter dabei unterstützen, die komplexen Anforderungen der beteiligten Akteure bezüglich Sicherheit und Compliance vollständig und effizient zu erfüllen sowie die resultierenden Implementierungen zu validieren.

Grundbuchdaten im Internet

Die Revision der eidgenössischen Grundbuchverordnung über das Grundbuch wird die Grundlage für die elektronische Erfassung und Publikation der Grundbuchdaten im Internet bilden. privatim fordert weitere Massnahmen, um die Risiken für die Persönlichkeitsrechte auf das erforderliche Mass zu minimieren.

Striptease

Ein Dialog über Doodle, über Belanglosigkeiten und Intimitäten in Facebook im Zeitalter des biometrischen Passes, der Cumuluskarte, der Mail-Kontrolle und der ungehemmten Fichierung.

Öffentlichkeit mit der Brechstange

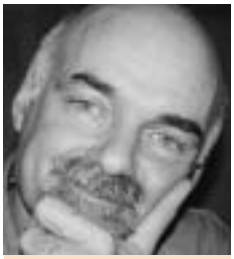
Wikileaks zerrt an die Öffentlichkeit, was die Urheber der Information geheim halten möchten. Julian Assange und Wikileaks sind für die einen Verräter, für die anderen Helden. Ist Öffentlichkeit nur um der Öffentlichkeit willen gut? Ist sie schlecht? Auf jeden Fall: Es wird für einen Urheber von Informationen deutlich schwieriger werden, die Interpretationshoheit für sich zu reservieren.

report

forum

Datenschutzkonzept auf dem Prüfstand

Datenschutz im öffentlich-rechtlichen Bereich und die Herausforderungen 2001–2010 im Spiegel von digma



Beat Rudin, Herausgeber beat.rudin@unibas.ch

Meldet sich der Gesetzgeber als Schrankensetzer ab, lastet der Grundrechtsschutz ganz auf dem Verhältnismässigkeitsprinzip.

Zehn Jahre hat digma den Datenschutz im öffentlich-rechtlichen Bereich nun begleitet – zehn Jahre, in denen sich das Konzept des öffentlich-rechtlichen Datenschutzes zu bewähren hatte. Hat es sich bewährt?

Folge-Rechtsetzung zum Bundesdatenschutzgesetz

Als die erste digma-Nummer erschien, war der Bund in den letzten Zügen der gesetzgeberischen Umsetzung des 1993 in Kraft getretenen Datenschutzgesetzes[1]. Art. 38 Abs. 3 DSG-Bund in der ursprünglichen Fassung erlaubte dem Bund, bestehende Datensammlung mit besonders schützenswerten Personendaten oder mit Persönlichkeitsprofilen noch während fünf Jahren nach Inkrafttreten dieses Gesetzes benützen, ohne dass die Voraussetzungen von Art. 17 Abs. 2 DSG-Bund erfüllt sind, d.h. ohne dass ein Gesetz im formellen Sinn die Bearbeitung ausdrücklich vorsieht. Weil die Fünfjahresfrist, die am 30. Juni 1998 ablaufen sollte, nicht ausreichte, wurde mit Bundesbeschluss vom 26. Juni 1998[2] die Frist bis 31. Dezember 2000 verlängert. In der Folge wurden die nötigen formellen Gesetzesbestimmungen in drei Schritten geschaffen:

- In einem ersten Paket wurden mit Bundesbeschlüssen vom 18. Juni 1999 die Grundlagen für verschiedene Personenregister im Polizeibereich geschaffen[3].
- In einem zweiten Paket wurden mit Bundesgesetz vom 24. März 2000[4] gesetzliche Bestimmungen für verschiedenste Datenbearbeitungen aus allen Departementen geschaffen. Gleichzeitig wurde ein Bundesgesetz über die Bearbeitung von Personendaten im Eidgenössischen Departement für auswärtige Angelegenheiten[5] erlassen, weil die meisten im EDA geführten Personendatensammlungen sich vorher mehrheitlich bloss auf Verordnungsbasis stützten.
- Ein drittes Paket schliesslich betraf Datenbearbeitungen im Sozialversicherungsbereich: Mit Bundesbeschlüssen vom 23. Juni 2000[6] wurden – bereits auch mit Blick auf die allgemeinen Regelungen im ATSG, die zur gleichen Zeit im Parlament beraten wurden – zehn Gesetze geändert.

Verankerung des Grundrechts auf Datenschutz in der Bundesverfassung

Auch im «Überbau», im Verfassungsrecht, tat sich etwas: Das Bundesgericht hatte das Recht auf informationelle Selbstbestimmung als ungeschriebenes verfassungsmässiges Recht, als Teilgehalt der Persönlichen Freiheit, anerkannt. Es hat dabei zwar den vom deutschen Bundesverfassungsgericht[7] geprägten Begriff übernommen[8], allerdings ohne zu sagen, was es darunter versteht. Im Rahmen der Nachführung der Bundesverfassung wurde die Persönliche Freiheit «auseinandergerupft»: Einzelne Aspekte ihres bisherigen Inhalts wurden selbständig gewährleistet (Recht auf Leben, Verbot der Folter, Achtung des Privat- und Familienlebens, der Wohnung sowie des Brief-, Post- und Fernmeldeverkehrs), aber gleichzeitig auch die persönliche Freiheit – offenbar nur noch mit einem reduzierten Schutzbereich – garantiert (Art. 10 Abs. 2 BV). Selbständig verfassungsrechtlich garantiert wird seither auch das Grundrecht auf Datenschutz – aber mit einer missglückten Formulierung, indem das Grundrecht bloss Schutz vor Missbrauch der persönlichen Daten (Art. 13 Abs. 2 BV) bieten soll. Gemeint ist aber «etwas viel Grundsätzlicheres»[9]; treffender umschreibt es die EU-Charta der Grundrechte: «(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. (3) Die Einhaltung dieser

Vorschriften wird von einer unabhängigen Stelle überwacht.»

Rechtsetzung in den Kantonen

Weil dem Bund keine umfassende Datenschutz-Rechtsetzungskompetenz zukommt, sind die Kantone berechtigt und verpflichtet, eigene Datenschutzgesetze zu erlassen[10]. Als die erste digma-Nummer erschien, hatten erst siebzehn der sechsundzwanzig Kantone ein formelles Datenschutzgesetz (mindestens beschlossen):

- 1981: Genf (nur für automatisiertes Datenbearbeiten), Waadt;
- 1982: Neuenburg;
- 1984: Wallis;
- 1986: Bern, Jura;
- 1987: Tessin, Thurgau;
- 1990: Luzern;
- 1991: Basel-Landschaft;
- 1992: Basel-Stadt;
- 1993: Zürich;
- 1994: Uri, Schaffhausen, Freiburg;
- 2000: Zug und Appenzell Innerrhoden.

In den ersten beiden digma-Jahren kamen vier weitere Kantone hinzu:

- 2001: Solothurn, Appenzell Ausserrhoden;
- 2002: Graubünden und Glarus.

Bloss fragmentarische allgemeine gesetzliche Bestimmungen (einige wenige Artikel in ihren Staatsverwaltungsgesetzen) besassen weiterhin zwei Kantone:

- St. Gallen[11] und Obwalden.

Keine formellen Datenschutzgesetze, sondern bloss generell-abstrakte Regelungen unterhalb der Gesetzesstufe konnten zwei Kantone aufweisen:

- Aargau und Schwyz.

Und schliesslich besass ein Kanton auch weiterhin weder ein formelles Datenschutzgesetz noch eine generell-abstrakte Regelung unterhalb der Gesetzesstufe:

- Nidwalden.

Wahrlich keine Erfolgsgeschichte, was den kantonalen Grundrechtsschutz für den Schritt in die Informationsgesellschaft betrifft. Bei vielen Kantonen wird es des Anstosses durch Schengen bedürfen, bis sie sich zu bewegen beginnen. Eigentlich «ver-rückt»: Die Schweiz, die sich als (letzter) Hort der Freiheit in Europa sieht, braucht die europarechtliche Verpflichtung, bis sie ihren Einwohnerinnen und Einwohnern einen wirksamen Schutz des Grundrechts auf informationelle Selbstbestimmung gewährt …

Das Datenschutzkonzept im öffentlich-rechtlichen Bereich

In dieser Verfassung traf digma den öffentlich-rechtlichen Datenschutz an. Das Konzept des öffentlich-rechtlichen Datenschutzes war jenes, welches bereits das Mustergesetz[12] von 1983 vorgeschlagen hatte:

- *Gesetzmässigkeit:* Personendaten dürfen bearbeitet werden, wenn eine gesetzliche Grundlage dies vorsieht; das Bearbeiten von besonderen Personendaten (sensitive Personendaten und Persönlichkeitsprofile) bedarf einer qualifizierten gesetzlichen Grundlage.
- *Verhältnismässigkeit:* Das Bearbeiten von Personendaten muss verhältnismässig sein, d.h., es muss zur Zweckerreichung geeignet und erforderlich und den betroffenen Personen zumutbar sein.

Die Schweiz, die sich als Hort der Freiheit in Europa sieht, braucht die europarechtliche Verpflichtung, bis sie ihren Einwohnern einen wirksamen Grundrechtsschutz gewährt.

- *Treu und Glauben:* Das Bearbeiten von Personendaten hat nach Treu und Glauben zu erfolgen.
- *Zweckbindung:* Personendaten dürfen nur zu dem Zweck bearbeitet werden, zu dem sie (aufgrund der gesetzlichen Grundlage) erhoben worden sind, soweit nicht eine gesetzliche Grundlage ausdrücklich eine weitere Verwendung vorsieht oder die betroffene Person im Einzelfall einwilligt.
- *Richtigkeit (und Vollständigkeit):* Personendaten müssen richtig und, soweit es der Bearbeitungszweck erfordert, vollständig sein.
- *Transparenz:* Das Datenbearbeiten (mindestens die Datenerhebung) und der Bearbeitungszweck müssen für die betroffene Person erkennbar sein; unter Umständen muss die betroffene Person aktiv informiert werden.
- *Informationssicherheit:* Personendaten sind durch organisatorische und technische Massnah-

Kurz&bündig

Das Konzept des öffentlich-rechtlichen Datenschutzes ist seit den 1980er-Jahren praktisch unverändert geblieben. Wie hat es sich angesichts der Herausforderungen des ersten Jahrzehnts (E-Themen, 9/11 und Sicherheit, Öffentlichkeitsprinzip und Schengen) bewährt? Wo liegen die Schwächen? Der Gesetzgeber meldet sich schleichend ab als Schrankensetzer – fast konturlose Ermächtigungsnormen überbürden den Schutz der informationellen Selbstbestimmung zunehmend dem Verhältnismässigkeitsprinzip. Hinzu kommt die strukturelle Schwäche des Persönlichkeitsschutzes: In der Abwägung unterliegt der (abstrakte) Wert der Privatheit dem (konkreten) Vorteil. Fraglich ist, wie weit die Kompetenzverteilung zwischen Bund und Kantonen zur Schwächung beiträgt. Sicher aber sind Defizite in der Umsetzung der Gesetze zu verorten: Ist der politische Wille zum wirksamen Grundrechtsschutz überall vorhanden? Schliesslich fehlt wohl auch die Bereitschaft zur Gesamtsicht auf die gesellschaftlichen Auswirkungen durch die zunehmenden Datenbearbeitungen.

men vor Verlust, Entwendung, unerlaubter Bearbeitung und Kenntnisnahme zu schützen.

- *Rechte der betroffenen Personen:* Die betroffene Person hat (u.a.) das Recht, zu erfahren, ob und wenn ja welche Daten über sie bearbeitet werden, und unrichtige Daten berichtigen zu lassen.

Damit wird etwas sichtbar: Im öffentlich-rechtlichen Bereich können nicht die Datenschutzgesetze allein den Grundrechtsschutz garantieren. Was ist überhaupt Inhalt der Datenschutzgesetze?

Inhalt der Datenschutzgesetze als «formelles Datenschutzrecht»

Die Datenschutzgesetze des Bundes (im öffentlich-rechtlichen Teil) und der Kantone enthalten – neben der Regelung vom Gesetzeszweck und Geltungsbereich sowie den nötigen Begriffsdefinitionen[13] – die oben erwähnten Datenschutzgrundsätze (insb. Verhältnismässigkeit, Zweckbindung, Richtigkeit, Erkennbarkeit der Beschaffung und/oder Informationspflicht)[14], legen die Verantwortung des datenbearbeitenden öffentlichen Organs fest[15] und formulieren die Voraussetzungen, unter welchen das Datenbearbeiten[16] und, als Unterkategorie, das Datenbekanntgeben zulässig sind[17]. Dabei legen sie auch fest, wie die qualifizierten Voraussetzungen für das Bearbeiten und Bekanntgeben von besonderen Personendaten aussehen[18]. Sie enthalten Bestimmungen für das grenzüberschreitende Bekanntgeben von Personendaten[19] und privilegieren in der Regel das Datenbearbeiten und -bekanntgeben zu nicht personenbezogenen Zwecken (wie Statistik, Planung, Wissenschaft und Forschung)[20]. Häufig regeln sie auch das Bearbeitenlassen von Personendaten durch Dritte (Datenbearbeiten im Auftrag, Outsourcing)[21]

Das Datenschutzgesetz ist angewiesen auf eine Umsetzung im Sachrecht, gleichzeitig ist es dieser Rechtsetzung aber auch ausgeliefert.

und die Pflicht, bestimmte Datenbearbeitungen einer Vorabkontrolle zu unterziehen[22]. Ausserdem räumen sie der betroffenen Person Rechte ein: das Recht auf Auskunft und Einsicht[23] (samt der Voraussetzungen für die Einschränkung dieses Rechts[24]), auf Berichtigung unrichtiger Daten, auf Unterlassung, auf Beseitigung der Folgen des widerrechtlichen Bearbeitens und auf Feststellung der Widerrechtlichkeit eines Bearbeitens[25]. Und schliesslich regeln die Gesetze die Datenschutzaufsicht[26].

«Materielles Datenschutzrecht»

Wer nun aber in einem Datenschutzgesetz nachschauen will, ob eine Schulleitung, die Polizei oder ein Bundesamt bestimmte Personendaten bearbeiten darf, sucht dort vergebens. Die Datenschutzgesetze legen zwar formell die Voraussetzungen eines Datenbearbeitens fest – gesetzliche Grundlage, Verhältnismässigkeit, Zweckbindung usw. –, sie selber stellen aber diese Grundlage nicht dar. Die materielle Grundlage für ihr Datenbearbeiten findet die Schulleitung im Schulgesetz, die Polizei im kantonalen Polizeigesetz, in der schweizerischen Strafprozessordnung usw., das Bundesamt im Bundesgesetz, das seine Aufgaben festlegt. Dort ist niedergelegt, unter welchen (materiellen) Voraussetzungen die Schulleitung bestimmte Daten erheben (oder eben nicht erheben) darf; dort steht, welche Daten die Polizei unter welchen (materiellen) Voraussetzungen an welche anderen Behörden weitergeben (oder eben nicht weitergeben) darf, und dort steht, welche Daten das Bundesamt erheben, anderen öffentlichen Organen weitergeben darf oder eben geheim halten muss.

Das Datenschutzgesetz (als sog. «formelles Datenschutzrecht») ist somit auf die bereichsspezifischen Datenschutzregelungen in anderen Gesetzen angewiesen (sog. «materielles Datenschutzrecht» in Form von Befugnissen oder Pflichten zur Datenbearbeitung, von Melderechten oder -pflichten, von Ermächtigung oder Verpflichtung zur Datenbekanntgabe, von Geheimhaltungspflichten mit allfälligen Ausnahmen usw.), das der Gesetzgeber gestützt auf seine Aufgabenkompetenz erlassen kann.

Angewiesen und ausgeliefert

Ob der Datenschutz wirksam ist, ist somit nicht so sehr von den Datenschutzgesetzen abhängig, sondern vielmehr davon, wie im anwendbaren Sachrecht die konkreten, bereichsspezifischen Datenschutzbestimmungen ausgestaltet sind. Nicht die Bekanntgabe-Bestimmung des Datenschutzgesetzes bestimmt, ob die Grundrechte der Versicherten geschützt sind, sondern die Bestimmung im Krankenversicherungsgesetz, welche die Spitäler zur Bekanntgabe aller Diagnosedaten der Versicherten an die Krankenkassen verpflichtet. Mit anderen Worten: Das Datenschutzgesetz ist angewiesen auf eine Umsetzung im Sachrecht, gleichzeitig ist es dieser Rechtsetzung aber auch ausgeliefert. Als Recht der gleichen Normstufe dürfte das Sachrecht als *lex specialis* auch regelmässig dem Datenschutzgesetz als *lex generalis* vorgehen. Datenschutz im öffentlich-rechtlichen Bereich steht und fällt deshalb primär mit der bereichsspezifischen Gesetzgebung.

Herausforderungen im ersten Jahrzehnt

In dieser Abhängigkeit traf der öffentlich-rechtliche Datenschutz auf die Herausforderun-

gen des neuen Jahrtausends. Da waren einmal die E-Themen (E-Health, E-Government und E-Voting), aber auch die neuen Herausforderungen im Bereich der Sicherheit, das Öffentlichkeitsprinzip und Schengen.

Die E-Themen

E-Health

digma 2002.2 wandte sich E-Health zu[27] – übrigens nach einem *auftakt* «Keine Angst vor Entblössung intimster Geheimnisse?» von (damals noch Nationalrätin) Simonetta Sommaruga[28]. Die Behandlung in digma zeigt ein bekanntes Bild: Die Technik steht bereit, der Kostendruck wirkt als Treiber, das Recht sollte der Technik möglichst rasch folgen. Der Prozess zur Schaffung von Technikfolgerecht braucht hingegen Zeit und Reflexion; in Wirklichkeit steckt er fest zwischen Euphorie («jetzt können alle Probleme gelöst werden») und Widerstand («wenn ich etwas verlieren könnte, bin ich dagegen»).

Das zeigte sich spätestens auch in der digma-Nummer zur «Gesundheitskarte» (digma 2006.4[29]). Das Bundesparlament wollte nicht bloss Technikfolgerecht produzieren, sondern schuf ohne konzeptionelle Vorarbeiten gleich auch die Grundlage für eine Gesundheitskarte – sozusagen «Technikvorausschreiterecht» oder ein ungeschickter Reflex auf den Vorwurf, das Recht käme immer (zu) spät. Es war den Fachleuten aber längst klar, dass es für eine erfolgreiche Einführung einer Gesundheitskarte mehr braucht als bloss eine Ermächtigungsbestimmung in einem Bundesgesetz. In der folgenden Nummer wurde dann die vom Bundesamt für Gesundheit, vom Bundesamt für Kommunikation und von der Konferenz der kantonalen Gesundheitsdirektoren erarbeitete E-Health-Strategie des Bundes mit ihren drei Handlungsfeldern («elektronische Patientendossier», «Gesundheitskompetenz» [Online-Informationen und Online-Dienste] und «Umsetzung und Weiterentwicklung der Strategie») vorgestellt[30]. Der darin enthaltene Zeitplan war reichlich euphorisch – und das in einem Bereich, in welchem nicht bloss die Kompetenz zur Schaffung von (formellem) Datenschutzrecht zwischen Bund und Kantonen aufgeteilt ist – das ist hier noch das kleinere Problem –, sondern in welchem auch materiell Bund und Kantone zuständig sind[31]. Im Jahr 2010 sollte sich dann eine Expertenkommission (u.a.) über dieses Problem beugen und einen Lösungsvorschlag präsentieren[32]: Der Bund solle im Rahmen seiner Rechtsetzungszuständigkeit Standards verbindlich erklären und die Kantone einladen, sich ebenfalls daran zu halten. Auch wenn man sich auf das Wesentliche beschränkt und ein mehrstufiges Vorgehen vorsieht – das Grundproblem dürfte sein, dass man erwartet oder suggeriert, mit E-Health könnten die Probleme im Gesundheitswesen gelöst werden. Was soll aber eine E-Health-Strategie erreichen, wenn keine Einigkeit über eine Health-Strategie besteht? Eine Erscheinung notabene, die allen E-Themen anzuhaften scheint … Immerhin könnten nun über kleine Schritte doch Fortschritte erreicht werden. Anfang Dezember 2010 hat der Bundesrat die entsprechenden Rechtsetzungsaufträge[33] erteilt. Längerfristig wird aber nur eine Reform der Gesundheitsverfassung eine Lösung bringen.

E-Government

In digma 2002.4 war E-Government[34] erstmals das Thema – oder mindestens eine Erscheinung, die mit E-Government daherkommt: die «Datenpools in der Verwaltung» (etwa auch in Form der Geografischen Informationssysteme GIS). Dabei wurde vor der Gefahr gewarnt, dass sich die Speicherung personenbezogener Daten zu einer Speicherung auf Vorrat ohne Zweckbindung entwickle. «Gewachsene» Datenpools wie die «Datendrehscheibe» im Kanton Zürich oder der «Datenmarkt» im Kanton Basel-Stadt zeigen noch heute Regelungsdefizite, beispielsweise im Zusammenhang mit Fragen der Verantwortlichkeit, der Begrenzung von Zugriffsrechten und Verknüpfungen sowie mit der Zweckbindung.

Die Technik steht bereit, der Kostendruck wirkt als Treiber. Der Prozess zur Schaffung von Technikfolgerecht braucht hingegen Zeit und Reflexion.

E-Voting

In der gleichen Nummer wurde auch zum ersten[35], aber nicht zum letzten Mal[36] E-Voting behandelt. Damit sich E-Voting auf breiter Front durchsetzen könne, müssten Sicherheitsprobleme wie die Authentifikation des Abstimmungsservers und die fehlende Nachvollziehbar- und Beweisbarkeit gelöst werden. Das Problem der unsicheren Client-Plattformen sei nach wie vor ungelöst. Von Ron Rivest stammt die pointierte Aussage, Botnets seien die potenziell grösste Wählergruppe … Heute muss für jeden Urnengang eine Obergrenze von Stimmberechtigten festgelegt werden, die ihre Stimme elektronisch abgeben können; damit soll das Risiko verhindert werden, dass bei Manipulationen ein Abstimmungsresultat «kippen» könnte … wahrlich keine zukunftsträchtige Konstellation, wenn immer bloss eine kleine Population elektronisch abstimmen darf!

Also auch hier die Frage: Warum E-Voting? Nur weil es modern ist? Was ist der Nutzen, den man sich daraus verspricht? Erwartet wird, dass

Fussnoten

1 Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG-Bund, SR 235.1).
2 AS 1998 1586.
3 Vgl. dazu Basler Kommentar Datenschutzgesetz, 2. Auflage, Basel/Genf/München 2006 (BSK-DSG²), Beat Rudin, Art. 38 N 12.
4 AS 2000 1891. Die Änderungen betrafen die folgenden Bereiche: Regierungs- und Verwaltungsorganisation, Freizügigkeit der Medizinalpersonen, Epidemien, Bürgerrecht, Aufenthalt und Niederlassung von Ausländern, Militärstrafprozess, Turnen und Sport, Armee, Stempelabgaben, Verrechnungssteuer, direkte Bundessteuer, Steuerharmonisierung, Wehrpflichtersatz, Zoll, ziviler Ersatzdienst, Wohnbau- und Eigentumsförderung, Arbeit, Jagd, Radio und Fernsehen. Vgl. dazu BSK-DSG²-Rudin, Art. 38 N 14.
5 AS 2000 1915, SR 235.2; vgl. dazu BSK-DSG²-Rudin, Art. 38 N 15.
6 AS 2000 2749 ff. Die Änderungen betrafen die folgenden Bereiche: Alters- und Hinterlassenenversicherung, Invalidenversicherung, Ergänzungsleistungen, berufliche Vorsorge, Krankenversicherung, Militärversicherung, Erwerbsersatz und Arbeitslosenversicherung. Vgl. dazu BSK-DSG²-Rudin, Art. 38 N 16.
7 BVerfGE 65, 1.
8 BGE 89 I 92, 98.
9 Rainer J. Schweizer, St. Galler Kommentar zu Art. 13 BV, Rz. 39.
10 Vgl. z.B. Beat Rudin, Die datenschutzrechtliche Umsetzung von Schengen in den Kantonen, in: Stephan Breitenmoser/Sabine Gless/Otto Lagodny (Hrsg.), Schengen in der Praxis, Erfahrungen und Ausblicke, Zürich/St. Gallen 2009, 213 ff., 215 (m.w.H.).
11 Der damalige Art. 9 des st. gallischen Staatsverwaltungsgesetzes kann als Beispiel für eine «Nichtregelung» dienen: «Die Bekanntgabe von Personendaten durch Organe der Staatsverwaltung ist zu beschränken. Sie kann aus wichtigen öffentlichen oder aus schutzwürdigen privaten Interessen zugelassen, mit Auflagen verbunden oder verweigert werden.» Sehr zur Freude der Exekutive, die sich möglichst nicht binden lassen will: Da kann mit öffentlichen und privaten Interessen gleich alles gerechtfertigt werden – vom Geheimhalten bis zum Bekanntgeben …
12 Mustergesetz für die Kantone (von der Konferenz der Justiz- und Militärdirektoren verabschiedet am 25. März 1983), wiedergegeben in: Rainer J. Schweizer/Beat Lehmann, Informatik- und Datenschutzrecht, Zürich 1988 ff., Ordnungs-Nr. 025-K.
13 Vgl. nur Art. 1–3 DSG-Bund, §§ 1–3 des zürcherischen Gesetzes vom 12. Februar 2007 über die Information und den Datenschutz (IDG-ZH, LS 170.4); §§ 1–3 des baselstädtischen Gesetzes vom 9. Juni 2010 über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG-BS, Kantonsblatt vom 12. Juni 2010, 914 ff., tritt voraussichtlich Mitte 2011 in Kraft).
14 Vgl. nur Art. 4, 5 und 7 DSG-Bund; §§ 9 und 12 IDG-ZH; §§ 9, 11, 12, 15, 16 IDG-BS.
15 Vgl. nur Art. 16 DSG-Bund; § 6 IDG-BS.
16 Vgl. nur Art. 17 DSG-Bund; § 8 IDG-ZH; § 9 IDG-BS.
17 Vgl. nur Art. 19 DSG-Bund; § 16 IDG-ZH; § 21 IDG-BS.
18 Vgl. nur Art. 17 Abs. 2 und 19 Abs. 1 DSG-Bund; §§ 8 Abs. 2 und 17 IDG-ZH; §§ 9 Abs. 2 und 21 Abs. 2 IDG-BS.
19 Vgl. nur Art. 6 DSG-Bund; §§ 19 IDG-ZH; § 23 IDG-BS.
20 Vgl. nur Art. 22 DSG-Bund; §§ 9 Abs. 2 und 18 IDG-ZH; §§ 10 und 22 IDG-BS.
21 Vgl. nur Art. 10a DSG-Bund; § 6 IDG-ZH; § 7 IDG-BS.
22 Vgl. nur § 10 IDG-ZH; § 13 IDG-BS.
23 Vgl. nur Art. 8 DSG-Bund; § 20 Abs. 2 IDG-ZH; § 26 IDG-BS.
24 Vgl. nur Art. 9 und 10 DSG-Bund; § 23 IDG-ZH; § 29 IDG-BS.
25 Vgl. nur Art. 25 Abs. 1 und 3 DSG-Bund; § 21 IDG-ZH; § 27 IDG-BS.
26 Vgl. nur Art. 26 ff. DSG-Bund; § 30 ff. IDG-ZH; § 37 ff. IDG-BS.
27 Georg C. von Below/Martin D. Denz, E-Health: Die Technik ist bereit, Einsatz moderner Informations- und Kommunikationstechnologien im Gesundheitswesen, digma 2002, 74 ff.; Tomas Poledna, Rahmenbedingungen von E-Health, Erste Erfahrungen und künftige Anwendungsformen im elektronischen Gesundheitswesen, digma 2002, 56 ff.; Matthias Horschik, Ohne Datenschutz kein E-Health, Kritische Momentaufnahme der datenschutzrechtlichen Situation im Gesundheitswesen, digma 2002, 64 ff.
28 Simonetta Sommaruga, Keine Angst vor Entblössung intimster Geheimnisse?, digma 2002, 55.
29 Bruno Baeriswyl, Auf leisen Sohlen zur Gesundheitskarte, Welche Rolle spielt die gesundheitskarte in einer umfassenden eHealth-Strategie?, digma 2006, 152 f.; Matthias Horschik, Von der Versicherten- zur Gesundheitskarte, Datenschutzrechtliche Überlegungen zur Einführung einer Gesundheitskarte, digma 2006, 154 ff.
30 Adrian Schmid, Strategie «eHealth» des Bundes, digma 2007, 20 ff.
31 Vgl. nur Art. 117 (Kranken- und Unfallversicherung) und Art. 118 BV (Schutz der Gesundheit).
32 «Umsetzung ‹Strategie eHealth Schweiz›: Empfehlungen zur rechtlichen Regelung, Bericht der ‹Expertengruppe eHealth› zuhanden des Eidg. Departements des Innern» vom 30. September 2010; Link auf der Seite <http://www.bag.admin.ch/themen/gesundheitspolitik/10357/10359/index.html?lang=de>.
33 Medienmitteilung des Eidg. Departement des Innern vom 3. Dezember 2010: «Elektronisches Patientendossier: Auftrag zur Ausarbeitung von Gesetzesgrundlagen», <http://www.admin.ch/aktuell/00089/index.html?lang=de&msg-id=36567>.
34 U.a. Lukas Fässler, Datenpools in der Verwaltung, Datenschutzrechtlicher Handlungsbedarf bei der Zusammenlegung von Datenpools in öffentlichen Verwaltungen, digma 2002, 160 ff.; Rolf Buser, Geoinformationen besser nutzen, Orts- und raumbezogene Informationen sind eine der wesentlichen Ressourcen des 21. Jahrhunderts, digma 2002, 166 ff.; Marco Fey, Rechtliche Aspekte von GIS, Überlegungen zu den datenschutzrechtlichen Implikationen von Geografischen Informationssystemen, digma 2002, 170 ff.
35 Rolf Oppliger, E-Voting sicherheitstechnisch betrachtet, Sicherheitsfragen und -probleme bei elektronischen Abstimmungsmechanismen, digma 2002, 184 ff.
36 Z.B. Rolf Oppliger, Anonymes E-Voting – eine Illusion? Ist anonymes E-Voting in der Praxis realisierbar oder handelt es sich um eine mathematische Illusion?, digma 2008, 24 ff.; ders., E-Voting auf unsicheren Client-Plattformen, digma 2008, 82 ff.; Herbert Burkert, Das «Wahlcomputer»-Urteil und E-Voting, digma 2009, 112 ff.
37 NZZ am Sonntag vom 5. Dezember 2010, 16 («Zürich stoppt das elektronische Wählen»); NZZ vom 6. Dezember 2010, 12 («Pause beim E-Voting»).
38 Aussage des (damaligen) Bundesanwalts Valentin Roschacher am Symposium on Privacy and Security 2003, zitiert in: Beat Rudin, Die Erosion der informationellen Privatheit – oder: Rechtsetzung als Risiko?, in: Thomas Sutter-Somm/Felix Hafner/Gerhard Schmid/Kurt Seelmann (Hrsg.), Risiko und Recht, Festgabe zum Schweizerischen Juristentag 2004, Basel/Genf/München/Bern 2004, 415 ff., 434 (Fn. 90).
39 Thilo Weichert, Überwachung: Einblick in die Praxis, Gängige Überwachungspraktiken im Bereich des öffentlichen und des pri-

sich einerseits generell mehr Stimmberechtigte an den Urnengängen beteiligen, und andererseits, dass sich insbesondere junge Stimmberechtigte für die Teilnahme gewinnen lassen. Ob dieser Nutzen erreicht wird, muss angesichts der jüngsten Meldungen allerdings bezweifelt werden. Nach den Aussagen des Wahlleiters im Kanton Zürich habe das E-Voting die Erwartungen bisher nicht erfüllt. Weder hätte sich die Stimmbeteiligung erhöht, noch nähmen mehr Junge an Wahlen oder Abstimmungen teil[37].

9/11 und Sicherheit

Ein zweiter roter Faden, welche durch die zehn digma-Jahre geht, ist die innere Sicherheit. Die dritte digma-Nummer war im Druck, als am 11. September 2001 die Terroranschläge in New York und Washington eine Entwicklung einläuteten, welche das ganze Jahrzehnt beeinflussen sollten. «Das ist Krieg gegen Amerika», gab der amerikanische Präsident den Tarif durch – im Gegensatz zum spanischen König, welcher im Anschluss an die Anschläge vom 11. März 2004 in Madrid davon sprach, die Täter seien Verbrecher, die strafrechtlich verfolgt werden müssen. Was hat sich seither nicht alles verändert! Nicht nur die Kontrollen an den Flughäfen (keine Nagelscheren, nur noch begrenzt Flüssigkeiten mit an Bord nehmen, Schuhe ausziehen, Nacktscanner) oder bei der Einreise (Fingerabdrücke und Fotos bei der Einreise in verschiedene Länder), auch die Ausweise (Fingerabdrücke und Fotos in digitaler Form in den Pässen) und der Informationsaustausch haben sich verändert (Passenger Name Records). Anonyme Handy-Abonnemente wurden abgeschafft, nachdem Terrorverdächtige Swisscom-Prepaid-Cards verwendet hatten – wegen der guten Roaming-Möglichkeiten[38]. Auch technologisch wurde nach 9/11 unter dem Stichwort «Terrorabwehr» auf breiter Front aufgerüstet (Gesichtserkennungs-Systeme an Flughäfen, Videoüberwachung, «Lauschangriff», Vorratsdatenspeicherung bei der elektronischen Kommunikation usw.), und die Pässe enthalten künftig einen Speicher mit biometrischen Merkmalen des Passinhabers.

digma 2002.1 widmete sich verschiedenen Aspekten von Surveillance[39] und schaute auch voraus auf die neuen technischen Möglichkeiten der automatisierten Auswertung von visueller Überwachung[40]. Ein spezielles Augenmerk richtete digma mehrmals auf die Videoüberwachung[41], die vielen als Wunderheilmittel erscheint, aber nach wissenschaftlichen Untersuchungen nur in bestimmten Konstellationen nachweislich die versprochene Wirkung entfaltet.

In den Sicherheitskontext gehört auch der Staatsschutz: Zwanzig Jahre sind vergangen, seit das Ausmass der «Fichenaffäre» bekannt wurde – und wieder macht der Staatsschutz Schlagzeilen. Inzwischen ist durch den Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte[42] mehr bekannt über die (Fehl-)Entwicklungen im Staatsschutz. Diese waren zuvor schon Thema in digma[43], ebenso das von der Eidgenössischen Datenschutzkommission als EMRK-widrig beurteilte «Nicht-Auskunftsrecht» nach Art. 18 BWIS[44] und die Pläne für die Reform des BWIS[45]. Im BWIS geregelt wurde zwischendurch auch die Bekämpfung des Hooliganismus; dazu stellten verschiedene Autoren in digma kritische Fragen[46], etwa zur Bundeskompetenz und der Grundrechtsverträglichkeit. Auch die Verkehrung des Grundrechtsschutzes als Schutz vor staatlichen Eingriffen durch die Forderungen nach einem «Grundrecht auf Sicherheit» bekam in digma eine klare und kompetente Antwort[47].

Zwanzig Jahre sind vergangen, seit das Ausmass der «Fichenaffäre» bekannt wurde – und wieder macht der Staatsschutz Schlagzeilen.

Öffentlichkeitsprinzip

Eine Entwicklung, die in der Schweiz schon in den 1990er-Jahren in Bern begonnen hat, hat sich Anfang des ersten Jahrzehnts fortgesetzt: die Einführung des Öffentlichkeitsprinzips. Aus Datenschutzsicht ist vor allem interessant, dass immer mehr Kantone dazu übergehen, Öffentlichkeitsprinzip und Datenschutz als zwei Seiten derselben Medaille auch in einem einzigen Gesetz zu regeln[48]. Andere Kantone und der Bund haben das Öffentlichkeitsprinzip ebenfalls eingeführt, aber in einem separaten Gesetz geregelt[49]. digma 2004.4 war der Informationsfreiheit[50] gewidmet. Darin wurden die laufenden Entwicklungen in Bund und Kantonen, aber auch in Europa nachgezeichnet und die Spannungsfelder zwischen Informationszugang und Schutz der Privatheit wie auch der öffentlichen Interessen ausgeleuchtet.

Die Schengen-Revisionen der Datenschutzgesetze

Die Frage, ob das Datenschutzrecht den Herausforderungen gerecht wird, war wiederholt Thema in digma[51]. 2003 war das Bundesdatenschutzgesetz zehn Jahre alt – eine Gelegenheit, einen Blick zurück auf die Entstehungsgeschichte zu werfen und danach zu fragen, ob es sich bewährt hat[52]. Auch die Revisionsvorlage des Bundesrates gab Anlass zur kritischen Betrachtung[53].

2004 hat die Schweiz mit der Europäischen Union die Bilateralen Verträge II abgeschlossen, darunter das Schengen-Assoziierungs-Abkommen

Fussnoten (Fortsetzung)

vaten Lebens, digma 2002, 4 ff.; Jürgen Welp, Auf dem Weg zum Überwachungsstaat?, Aktuelle Entwicklungen in der staatlichen Überwachung von Bürgerinnen und Bürgern, digma 2002, 18 ff.

40 David C. Hogg, Automated Visual Surveillance, A New Application and Field of Study for Computer Vision, digma 2002, 24 f.

41 Bruno Baeriswyl, Videoüberwachung im rechtsfreien Raum?, Datenschutzrechtliche Aspekte moderner Überwachung mittels optischen Geräten, digma 2002, 26 ff.; Francisco Klauser, Die Entwicklung einer «Sicherheitsstadt», digma 2004, 22 ff.; Beat Rudin, Videoüberwachung: Aufbewahrungsfrist (Besprechung von BGE 133 I 77), digma 2007, 34 ff.; privatim, Videoüberwachung braucht klare Grenzen, digma 2007, 122 f.; Philipp Mittelberger, Videoüberwachung im Lichte der Verfassung (Besprechung eines Entscheides der Datenschutzkommission des Fürstentums Liechtenstein), digma 2008, 140 ff.; Beat Rudin/Sandra Stämpfli, Wunderheilmittel Videoüberwachung?, digma 2009, 144 ff.

42 Datenbearbeitung im Staatsschutzinformationssystem ISIS, Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte vom 21. Juni 2010, BBl 2010 7665 ff.

43 Roland Stark, Staatsschutz – ein Hort für Widerholungstäter, digma 2009, 49; Beat Rudin, Staatsschutz unter Kontrolle? Aktuelle Überlegungen zum Staatsschutz zwanzig Jahre nach dem Bekanntwerden der «Fichenaffäre», digma 2009, 52 f.; Georg Kreis, Staatsschutz im Laufe der Zeit, Von der Skandalisierung zur Gleichgültigkeit – ein Blick zurück auf die Fichenaffäre vor zwanzig Jahren, digma 2009, 54 ff.; Markus Mohler, Staatsschutz braucht klare Regelungen, Schwierigkeiten im Staatsschutz an der Schnittstelle zwischen Bund und Kantonen, digma 2009, 60 ff.

44 Beat Rudin, «Indirekte Auskunft» nach Art. 18 BWIS (Besprechung des Urteils der EDSK vom 15. Februar/23. Mai 2006), digma 2006, 184 ff.; ders., fedpol vs. EDÖK, digma 2007, 33.

45 Lucien Müller/Nina Widmer/Rainer J. Schweizer, BWIS-II-Reform: kritische Bemerkungen, digma 2008, 124 ff.

46 Markus Schefer, BWIS-I: Kompetenzen und Grundrecht, Das Hooligan-Gesetz wirft Fragen in Bezug auf die Bundeskompetenz und die Vereinbarkeit mit Grundrechten auf, digma 2006, 60 ff.; Marcel Studer, Mit Datenbanken gegen Hooliganismus, Hooligan-Datenbanken als informationelle Massnahmen gegen Gewaltausschreitungen an Sportanlässen, digma 2006, 66 ff.; Thilo Weichert, Wie viel Sicherheit verträgt der Sport?, Technische Massnahmen und ihre Datenschutzverträglichkeit bei der Fussball-Weltmeisterschaft 2006, digma 2006, 70 ff.; Thomas Busset, Qui a volé la mascotte du gardien?, digma 2006, 128 ff.

47 Sabine Leutheusser-Schnarrenberger, Ein Grundrecht auf Sicherheit?, digma 2006, 118 ff.

48 Solothurn: Informations- und Datenschutzgesetz vom 21. Februar 2001 (BGS 114.1); Genf: Loi du 5 octobre 2001 sur l'information du public, l'accès aux documents et la protection des données personnelles (in der Fassung der Änderung vom 9. Oktober 2008) (RSG A 2 08); Zürich: Gesetz vom 12. Februar 2007 über die Information und den Datenschutz (LS 170.4); Aargau: Gesetz vom 24. Oktober 2006 über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (SAR 150.700); Schwyz: Gesetz vom 23. Mai 2007 über die Öffentlichkeit der Verwaltung und den Datenschutz (SRSZ 140.410); Wallis: Gesetz vom 9. Oktober 2008 über die Information der Öffentlichkeit, den Datenschutz und die Archivierung (noch nicht in Kraft); Basel-Stadt: Gesetz vom 9. Juni 2010 über die Information und den Datenschutz (Inkrafttreten 2011).

49 So neben dem Bund (Bundesgesetz vom 17. Dezember 2004 über das Öffentlichkeitsprinzip der Verwaltung, BGÖ, SR 152.3) z.B. die Kantone Bern (Gesetz vom 2. November 1993 über die Information der Bevölkerung, BSG 107.1) und Uri (Gesetz vom 26. November 2006 über das Öffentlichkeitsprinzip in der kantonalen Verwaltung, RB 2.2711).

50 Beat Rudin, Informationsfreiheit – Investition in Vertrauen, Schritte auf dem Weg zu einem veränderten Verständnis der Rolle der Bürger als Partner im demokratischen Dialog, digma 2004, 144 f.; Isabelle Häner, Die Funktion des Öffentlichkeitsprinzips, Überlegungen zum Wesen des Öffentlichkeitsprinzips in der Verwaltung, digma 2004, 146 ff.; Patrick Sutter, Vertrauen durch Informationszugang, Von der Notwendigkeit eines umfassenden Rechts auf Zugang zu amtlichen Informationen, digma 2004, 150 ff.; Stephan C. Brunner, Interessenabwägung im Vordergrund, Hinweise im Hinblick auf die praktische Anwendung des Öffentlichkeitsgesetzes auf Bundesebene, digma 2004, 160 ff.; Bruno Baeriswyl, Informationsprozess im Mittelpunkt, Entwurf eines Informations- und Datenschutzgesetzes im Kanton Zürich, digma 2004, 166 ff.; Alexander Dix, Informationsfreiheit: Kleinere weisse Flecken, Die Entwicklung des Informationsfreiheitsrechts in Europa und in der Europäischen Union, digma 2004, 170 ff.

51 So z.B. Bruno Baeriswyl/Beat Rudin, Datenschutzgesetze – wie weiter?, digma 2001, 126 ff.; Rainer J. Schweizer/Patrick Sutter, Zur Revision des Datenschutzgesetzes, digma 2001, 130 ff. Ebenso digma 2008.2 zum Thema Wirkung und Evaluation: u.a. Beat Rudin, Evaluation: ein Blick auf die Wirksamkeit, Datenschutzgesetze, Datenschutzbeauftragte, Datenschutzmassnahmen – und damit ein besserer Datenschutz?, digma 2008, 60 f.; Luzius Mader, Zur Evaluation von Gesetzen, Vom normativen Idealismus zur evidenzorientierten Gesetzgebung – einleitende Bemerkungen zur Gesetzesevaluation, digma 2008, 62 ff.; Bruno Baeriswyl, Die Wirksamkeit von Datenschutzbehörden, Effizienz und Effektivität der Datenschutzbehörden sind Schlüsselfaktoren eines wirkungsvollen Datenschutzes, digma 2008, 66.

52 Peter Forstmoser, 10 Jahre Gesetz – 30 Jahre Diskussion, Von den Anfängen des Datenschutzes in der Schweiz, digma 2003, 50 ff.; Rainer J. Schweizer, Die Informatik fordert das Recht heraus, Vermittlung des gesellschaftlichen und ökonomischen Wertes des informationellen Persönlichkeitsschutzes, digma 2003, 58 ff.; Hans Rudolf Trüeb, Von Metropolis zum Global Village, Das Verhältnis von Datenschutz und Informationstechnologie, digma 2003, 64 ff.; Hansjürgen Garstka, Soziotechnisches Regelsystem, Die Rolle des Rechts für die Gewährleistung der informationellen Selbstbestimmung, digma 2003, 72 ff.

53 Bruno Baeriswyl/Beat Rudin, Moderner Datenschutz als Wachstumschance, digma 2004, 74 f.

54 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Personenverkehr, ABl. L 281 v. 23.11.1995, 31 ff.

55 Übereinkommen (des Europarates) zum Schutze des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981, SR 0.235.1 (im Folgenden: ER-Konv 108).

56 Vgl. dazu Bruno Baeriswyl, Die Schengen-Dublin-Anforderungen, digma 2006, 146; privatim, Handlungsbedarf nach der Schengen-Evaluation, digma 2008, 98 f.; aber auch Band 2 der digma-Schriften: Beat Rudin, Datenschutzgesetze – fit für Europa, Europarechtliche Anforderungen an die schweizerischen Datenschutzgesetze, digma-Schriften Band 2, Zürich/Basel/Genf 2007.

57 Rahmenbeschlusses 2008/977 vom 28. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350 v. 30.12.2008, 60 ff.). Vgl. dazu Markus H.F. Mohler, Der neue Besitzstand von Schengen und

(SAA) und das Dublin-Assoziierungs-Abkommen (DAA). Den Schengen-Beitritt gab's für die Schweiz aber nicht umsonst: Wer von den Vorteilen von Schengen profitieren will, muss auch bestimmte Anforderungen erfüllen. Weil die Sicherheitsbehörden sehr stark an einem Beitritt zu Schengen/Dublin interessiert waren, wurden auch die erhöhten Datenschutz-Anforderungen in Kauf genommen. Die Datenschutzgesetzgebungen in Bund und Kantonen mussten eine «Schengen-Evaluation» bestehen: Sie mussten den Anforderungen der EG-Datenschutzrichtlinie 95/46/EG[54] und der Datenschutzkonvention des Europarates[55] genügen[56] (hinzu kam in jüngster Vergangenheit noch der Rahmenbeschluss 2008/977[57]). Zweiteres war zwar bereits seit dem Inkrafttreten der ER-Konv 108 für die Schweiz am 1. Februar 1998 notwendig; dass etliche kantonale Gesetze dies nicht taten (oder – wie oben erwähnt – verschiedene Kantone noch gar keine Datenschutzgesetzgebung besassen), blieb aber faktisch ohne Konsequenzen.

Die Schengen-Datenschutzanforderungen haben – wie erwähnt – einen Entwicklungsschub ausgelöst. Die Anforderungen betreffen einerseits die materiellen Regelungen: Welche Voraussetzungen muss das Datenschutzgesetz für das Datenbearbeiten aufstellen? Welche Rechte müssen den betroffenen Personen eingeräumt werden? Andererseits betreffen die Anforderungen institutionelle Aspekte, insbesondere die Unabhängigkeit und Wirksamkeit der Datenschutzaufsicht. Die im Gefolge der Schengen-Assoziierung der Schweiz angepassten Datenschutzgesetze erfüllen die materiellen Anforderungen weitgehend. Defizite bestehen hingegen nach wie vor bezüglich der Datenschutzaufsicht – und zwar sowohl, was die Unabhängigkeit als auch was die Wirksamkeit betrifft[58]. In vielen Kantonen stellt beispielweise die Exekutive die Datenschutzaufsicht mit einem jederzeit kündbaren Arbeitsvertrag an; das Parlament ist in keiner Weise an der Wahl der Aufsicht beteiligt, also entscheiden allein die zu Kontrollierenden über die Kontrolleure. Und in sehr vielen Kantonen sind die der Datenschutzaufsicht zugeteilten Ressourcen weit entfernt von dem, was es für eine wirksame Aufsicht mindestens brauchte[59].

Datenschutzaufsicht

Gerade das zuletzt angesprochene Thema, die Datenschutzaufsicht, war ebenfalls mehrfach Gegenstand von digma-Beiträgen – auf der einen Seite die Frage nach der Unabhängigkeit[60], anderseits aber auch die Frage nach dem Selbstverständnis der Datenschutzbeauftragten[61]. Dass es hier grosse Unterschiede gibt, dürfte offensichtlich sein – das hier zu vertiefen, würde aber zu weit führen.

Im Rückblick: Schwächen des öffentlich-rechtlichen Datenschutzes

Bei einem kritischen Rückblick auf die vergangenen zehn Jahre treten verschiedene Schwächen des Datenschutzes im öffentlich-rechtlichen Bereich zutage.

Das nur vermeintliche Nadelöhr der gesetzlichen Grundlage

Das Konzept des öffentlich-rechtlichen Datenschutzes besitzt zwei «Nadelöhre», mit welchen ein überbordendes Datenbearbeiten verhindert werden soll: das Erfordernis der gesetzlichen Grundlage und die Verhältnismässigkeit. Sehr vereinfacht kann gesagt werden: Der Gesetzgeber erlaubt oder verbietet – die rechtsanwendende Verwaltung setzt angemessen um. Diese Vereinfachung trifft natürlich nicht ganz zu: Auch der Gesetzgeber kann nicht beliebig erlauben oder verbieten – er ist an übergeordnetes Recht gebunden und muss in der Rechtsetzung die Verhältnismässigkeit auch beachten (Art. 5 Abs. 3 BV). Doch auf Bundesebene hapert es mit den «checks and balances» bereits hier: Wenn der Bundesgesetzgeber Verfassungsrecht verletzt, indem er ohne verfassungsrechtliche Kompetenz aktiv wird oder eine unverhältnismässige Regelung trifft, bleibt

Die Datenschutzgesetze erfüllen die materiellen Anforderungen weitgehend. Defizite bestehen hingegen weiterhin bezüglich Unabhängigkeit und Wirksamkeit der Datenschutzaufsicht.

das ungeahndet: Die Bemühungen, auf Bundesebene eine Verfassungsgerichtsbarkeit einzurichten, um genau solche Verstösse korrigieren zu können, sind bisher aufgrund der einseitigen Überhöhung des Demokratieprinzips («bei uns entscheidet das Volk» – auch wenn dabei Verfassung und Völkerrecht verletzt werden) versandet.

Eine zweite Einschätzung: Das «Nadelöhr» der gesetzlichen Grundlage verliert an Wirksamkeit, wenn der Gesetzgeber sich als Schrankensetzer verabschiedet. Das «Nadelöhr» gesetzliche Grundlage würde verlangen, dass der Gesetzgeber sehr genau abwägt, was die Rechtsanwendung zur Erfüllung ihrer Aufgaben soll tun dürfen. Wenn der Gesetzgeber aber fast reflexartig «abhakt», was ihm von Verwaltung und Exekutive vorgelegt wird, wenn er konturlose Ermächtigungen schafft («darf besonders schützenswerte Personendaten bearbeiten, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist»), statt der Verwaltungstätigkeit Schranken zu setzen, dann verliert die gesetzliche Grundlage die Wirkung,

die ihr eigentlich von Art. 36 BV und den entsprechenden Kantonsverfassungsbestimmungen zugedacht ist. Das «formelle Datenschutzrecht», die Datenschutzgesetze, können, ja müssen auf dieser abstrakten Ebene bleiben; das «materielle Datenschutzrecht», die bereichsspezifischen Da-

Nicht die verteilte Rechtsetzungskompetenz für den Erlass der Datenschutzgesetze ist das Problem, sondern die verteilte Rechtsetzungskompetenz z.B. im Gesundheitsbereich.

tenschutzbestimmungen, müsste aber möglichst präzis (so konkret, wie es in einer generell-abstrakten Norm möglich ist) festlegen, welche Daten unter welchen Voraussetzungen von welchem öffentlichen Organ erhoben (oder eben nicht erhoben), zu welchem Zweck bearbeitet und an andere Behörden weitergegeben (oder eben nicht weitergegeben) werden dürfen. Tut es dies nicht, indem es sich auch auf die abstrakte Ebene zurückzieht, läuft das Konzept des öffentlich-rechtlichen Datenschutzes ins Leere.

Damit wird die ganze Last der Einschränkung staatlichen Datenbearbeitens dem Verhältnismässigkeitsprinzip aufgebürdet – und damit der rechtsanwendenden Verwaltung überlassen. Die Verwaltung aber wird ihre Aufgabenerfüllungsinteressen tendenziell immer höher gewichten als entgegenstehende Interessen Betroffener … Damit gerät das Gebäude von «checks and balances» aus dem labilen Gleichgewicht.

Strukturelle Schwäche des Persönlichkeitsschutzes: Vorteil vs. Wert

Hinzu kommt eine strukturelle Schwäche: Die Verwaltung auf individuelle-konkreter Ebene ohnehin, aber auch der Gesetzgeber auf generell-abstrakter Ebene, sie treffen immer *Einzelentscheide* (z.B. über die Zulässigkeit von Datenbearbeitungen in einem bestimmten Aufgabenzusammenhang). In der dabei erfolgenden (Einzel-) Abwägung stehen die (konkreten) Informationsbedürfnisse der Aufgabenerfüllung der Privatheit als (generellem) Freiheits*wert* gegenüber, wobei regelmässig die fassbareren konkreten Bedürfnisse überwiegen[62]. Solche Rechtsetzung birgt die Gefahr, dass vor lauter je einzeln gerechtfertigten Regelungen mit einem Mal das «insgesamt» erträgliche Mass überschritten wird. Selbst wenn der Gesetzgeber im «materiellen Datenschutzrecht» Schranken setzen will, läuft er Gefahr, den konkreten Aufgabenzusammenhang zulasten des Grundrechtsschutzes vorzuziehen.

Kompetenzverteilung

Mithin wird vermutet, die Datenschutz-Rechtsetzungskompetenzverteilung zwischen Bund und Kantonen trage nicht zur Stärkung des Datenschutzes im öffentlich-rechtlichen Bereich bei. Das ist genauer zu betrachten: Die Datenschutzgesetze (als «formelles Datenschutzrecht») unterscheiden sich heute – aufgrund der im Gefolge der Schengen-Assoziierung der Schweiz notwendig gewordenen Anpassungen an die europarechtlichen Anforderungen – nicht mehr entscheidend. Grössere Unterschiede gibt es allenfalls noch in den Anforderungen an die qualifizierte Rechtsgrundlage für das Bearbeiten von besonderen Personendaten und bei besonderen Bearbeitungen (etwa bei Online-Abrufverfahren) und – vor allem – bei der Datenschutzaufsicht.

Diese Unterschiede sind es aber nicht, welche die Klagen über die Zersplitterung des Datenschutzes auslösen. Überhaupt betreffen die Kla-

Fussnoten (Fortsetzung)

Dublin, in: Stephan Breitenmoser/Sabine Gless/Otto Lagodny (Hrsg.), Schengen und Dublin in der Praxis, Weiterentwicklungen der Rechtsgrundlagen, Zürich/St. Gallen 2010, 7 ff., 33; Beat Rudin/Sandra Stämpfli, Datenschutzrechtliche Weiterentwicklungen – neue Herausforderungen, in: Stephan Breitenmoser/Sabine Gless/Otto Lagodny (Hrsg.), Schengen und Dublin in der Praxis, Weiterentwicklungen der Rechtsgrundlagen, Zürich/St. Gallen 2010, 197 ff., 207 ff.

58 Vgl. dazu Beat Rudin, Die datenschutzrechtliche Umsetzung von Schengen in den Kantonen, in: Stephan Breitenmoser/Sabine Gless/Otto Lagodny (Hrsg.), Schengen in der Praxis, Erfahrungen und Ausblicke, Zürich/St. Gallen 2009, 213 ff., insb. 237 ff. und 244 ff.

59 Vgl. dazu Beat Rudin, Die datenschutzrechtliche Umsetzung … (Fn. 58), 242, 245 ff.; ders./Sandra Stämpfli, Datenschutzrechtliche Weiterentwicklungen … (Fn. 57), 221 ff.

60 Vgl. dazu Beat Rudin, Völlig unabhängige Datenschutzaufsicht (Besprechung des Urteils C-518/07 des EuGH vom 9. März 2010), digma 2010, 879 ff.; ebenso drei Bände der digma-Schriften: ders., Datenschutzgesetze – fit für Europa (Fn. 56), 71 ff.; Isabelle Häner, Unabhängigkeit der Aufsichtsbehörden, Umsetzung am Beispiel der Datenschutzaufsicht des Kantons Zürich, digma-Schriften Band 3, Zürich/Basel/Genf 2008; Bernhard Waldmann/André Spielmann, Unabhängigkeit der Datenschutzaufsicht, Rechtsgutachten im Auftrag des Kantons Freiburg, digma-Schriften band 5, Zürich/Basel/Genf 2010.

61 Insbesondere Bruno Baeriswyl, Vom Selbstverständnis der Beauftragten, Wie die europäischen Datenschutzbeauftragten mit «Street View» umgehen, digma 2009, 108 ff.; Beat Rudin, Von Gewinnern und anderen, digma 2006, 200; allgemeiner: Hanspeter Thür, Rolle der Datenschutzbeauftragten, Aufgaben und Instrumente der Datenschutzbehörden im Wandel, digma 2003, 80 ff.

62 Jean Nicolas Druey spricht in diesem Zusammenhang von einer «strukturellen Schwäche des Personenschutzes»: Jean Nicolas Druey, Von der strukturellen Schwäche des Personenschutzes im Informationsrecht, in: Bruno Baeriswyl/ Beat Rudin (Hrsg.), Perspektive Datenschutz, Praxis und Entwicklungen in Recht und Technik, Zürich/ Baden-Baden/Wien 2002, 145 ff.

gen nicht das «formelle Datenschutzrecht». Hier wird nämlich überall, im Bund wie in allen Kantonen, für das Bearbeiten von Personendaten eine gesetzliche Grundlage und die Einhaltung des Verhältnismässigkeitsprinzips verlangt. Wo also sollen die beklagenswerten Unterschiede liegen? Sie liegen im «materiellen Datenschutzrecht» bzw. in der kantonalen Zuständigkeit für die Rechtsetzung in bestimmten Materien. Im Umfeld von E-Health beispielsweise wird beklagt, dass in jedem Kanton die Voraussetzungen für E-Health-Anwendungen geschaffen werden müssen – das muss und kann aber nicht in den Datenschutzgesetzen erfolgen, sondern in den Gesundheitsgesetzen oder in den Spitalgesetzen. Nicht die verteilte Rechtsetzungskompetenz für das «formelle Datenschutzrecht» (also für den Erlass der Datenschutzgesetze) ist das Problem, sondern die verteilte Rechtsetzungskompetenz im Gesundheitsbereich, im Polizeibereich, im Schulbereich usw. (also die Kompetenz zum Erlass «materiellen Datenschutzrechts»). Das würde sich somit nur ändern, wenn aus den entsprechenden Kantonskompetenzen Bundeskompetenzen würden.

Allerdings könnte man sich fragen, inwieweit es schaden würde, schweizweit ein einheitliches Datenschutzgesetz zu schaffen. Die Argumente, die 1977 für einen Verzicht auf eine Bundeskompetenz angeführt wurden (in der Verwaltung einer ländlichen Gemeinde würde ganz anders gearbeitet als in einem grossen Bundesamt, das über Grossrechner verfüge), gelten längst nicht mehr – beide haben heute die gleiche Hard- und Software im Einsatz …

Umsetzung

Schliesslich – aber das soll hier nicht mehr vertieft werden – liegen grosse Unterschiede in der Umsetzung des Datenschutzrechts. Das hat viel mit Kultur zu tun: Inwieweit gehört die Achtung der Grundrechte der Personen, über welche öffentliche Organe Daten bearbeiten, zum Grundverständnis der entsprechenden Organe? Zu einer Verstärkung der Gewichtung des Grundrechtsschutzes können sicher die Datenschutzaufsichtsbehörden beitragen:

- wenn sie institutionell stark genug verankert werden,
- wenn sie ressourcenmässig stark genug ausgestattet werden,
- wenn dafür von ihrer Fach- und Sozialkompetenz her geeignete Persönlichkeiten ausgewählt werden und
- wenn diese ein entsprechendes Selbstverständnis entwickeln.

Dies alles funktioniert aber nur dort, wo der entsprechende politische Wille dafür besteht, wo also die über Rechtsetzung, Wahl und Budget entscheidenden Organe eine Instanz wollen, welche die Achtung der Grundrechte der Personen, über welche öffentliche Organe Daten bearbeiten, stärken soll. Womit wir wieder am Anfang dieses Abschnittes bei den unterschiedlichen Kulturen angelangt wären …

Ausblick: «Neuer Datenschutz» im öffentlich-rechtlichen Bereich?

Braucht es einen «neuen Datenschutz» im öffentlich-rechtlichen Bereich? Die Diskussion ist nicht neu und wird nicht nur in der Schweiz geführt. Stichworte sind das Verhältnis von Recht und Technik, Systemdatenschutz («privacy by design»), Datenschutz als Standard («privacy by default»), Datensparsamkeit und Datenvermeidung. Diese Diskussion kann hier nicht vertieft werden – aber eines sei noch angemerkt: Es wird auch darum gehen, von einer Formalisierung des Datenschutzes zu einer Materialisierung überzugehen. Es kann nicht genügen, einfach eine gesetzliche Grundlage zu schaffen, weil Datenbearbeiten eine gesetzliche Grundlage braucht. Es wird künftig vielmehr darum gehen, die inhaltliche Diskussion darüber zu führen, welches Datenbearbeiten gesellschaftsverträglich ist. Die Effizienz der Aufgabenerfüllung ist nicht alles – es muss vermehrt auch eine Gesamtsicht auf die gesellschaftlichen Auswirkungen der zunehmenden Datenbearbeitungen gesucht werden. Der gläserne Mensch ist nicht nur nicht im Interesse des Individuums. Die Privatheit, die informationelle Selbstbestimmung, ist nicht bloss ein «privates» Grundrecht, sondern liegt auch im öffentlichen Interesse, da Staat, Gesellschaft und Wirtschaft keine gläsernen und damit manipulierbaren Menschen brauchen können. Der auf die Mitwirkung seiner Bürgerinnen und Bürger angewiesene Staat, die auf Selbstverantwortung der Menschen bauende Gesellschaft und die auf mündige Konsumentinnen und Konsumenten zählende Wettbewerbswirtschaft sind auf selbst-, und nicht fremdbestimmte Menschen angewiesen. ■

Die Umsetzung des Datenschutzrechts hat viel mit Kultur zu tun: Inwieweit gehört die Achtung der Grundrechte zum Grundverständnis der entsprechenden Organe?

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 123.00** (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 §