Revisionsarbeiten im Europarat und der Europäischen Union und deren Auswirkungen auf die Schweiz

Robert Baumann [*]

Inhaltsverzeichnis

1. Kommunikation, Information und Manipulation

a. Mittel der Kommunikation, die uns die Welt ins Haus liefern...

Max Frischs Walter Faber trifft in Paris seinen ehemaligen ETH-Professor, Professor O. «Ich werde nie vergessen», so Faber, «wie wir in weissen Zeichenmänteln, Studenten, um ihn herumstehen und lachen über seine Offenbarung: Eine Hochzeitsreise (so sagte er immer) genügt vollkommen, nachher finden Sie alles Wichtige in Publikationen, lernen Sie fremde Sprachen, meine Herren, aber Reisen, meine Herren, ist mittelalterlich, wir haben heute schon Mittel der Kommunikation, die uns die Welt ins Haus liefern, es ist Atavismus, von einem

[*] Dr. iur., Rechtsanwalt, wissenschaftlicher Mitarbeiter des Bundesamts für Justiz. – Erweiterte Fassung des Referats anlässlich der Tagung der Schweizerischen Sektion der internationalen Juristenkommission zum Thema «Persönlichkeitsschutz im Zeitalter des Internet. Nationale und transnationale Fragestellungen» vom 26. April 2013 in Bern.

Ort zum andern zu fahren. Sie lachen, meine Herren, aber es ist so, Reisen ist ein Atavismus, es wird kommen der Tag, da es überhaupt keinen Verkehr mehr gibt, und nur noch die Hochzeitspaare werden mit einer Droschke durch die Welt fahren, sonst kein Mensch – Sie lachen, meine Herren, aber Sie werden es noch erleben!»[1]

Frisch nimmt im 1957 erschienenen «Homo Faber» Bezug auf ein Werk aus dem Jahre 1948 von Norbert Wiener, einem amerikanischen Mathematiker und Begründer der Kybernetik[2]. Wiener betonte, dass die materielle Beförderung allmählich durch Kommunikation abgelöst würde. Kritisch kommentierte der Philosoph und Schriftsteller Günther Anders 1956 diese «eigentlich umwälzende Leistung, die Radio und TV gebracht haben: (...) dass die Ereignisse (...) uns besuchen; dass die Welt zum Menschen, statt er zu ihr kommt»[3].

b. ... und uns in die Welt.

Auf eine andere Kehrseite der Fortschritte in der Kommunikationstechnik wies 30 Jahre später Dürrenmatt hin: Der Mensch heute sei ein beobachteter Mensch, der Staat beobachte ihn mit immer raffinierteren Methoden, findet der Logiker D. in Dürrenmatts Erzählung «Der Auftrag» aus dem Jahre 1986. Es ist die Zeit der Fichenaffäre.

In diese Zeit fallen auch die Vorbereitungen für das Datenschutzgesetz vom 19. Juni 1992 (DSG). Der Bundesrat formulierte in seiner Botschaft vom 23. März 1988 das Ziel, dass jedermann selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen und frei über die Aufnahme und Gestaltung seiner Informations- und Kommunikationsbeziehungen entscheiden können solle. Dies bedinge vorab den Schutz des Privat- und Familienlebens vor Beeinträchtigungen durch Private und den Staat, den Schutz von Informationen über die Ausübung von verfassungsmässigen Rechten, wie z.B. der Meinungsfreiheit oder des Stimm- und Petitionsrechts und die Verhinderung, dass der Einzelne zu einem rechtlosen Objekt der Datenbearbeitung wird; er solle vielmehr das Bild der Welt über ihn mitbestimmen können[4].

Heute ist es noch einmal anders, als es Dürrenmatt 1986 notiert hat: Primär wird heute nicht mehr der Staat als Bedrohung für die Privatsphäre wahrgenommen. Mit der Entwicklung des Internet werden private Unternehmen als Bedrohung angesehen, private Unternehmen, die uns über das Internet ausspionieren. Doch wir geben auch selbst aktiv die gewünschten Informationen ins Internet und damit in die Welt hinaus. Was eine Frau sonst als besonders schützenswertes Personendatum nur der Gynäkologin anvertraut, gibt sie mit ihrer Ovalutionskalender-App unbekannten Dritten preis und gewährt ihnen überdies auch noch

---

[1] Max Frisch, Homo Faber, zitiert nach Suhrkamp BasisBibliothek, 1. Aufl. 1998, S. 112.

[2] Norbert Wiener, Cybernetics or Control and Communication in the Animal and the Machine, M.I.T. 1948; s. Frisch, a.a.O., S. 291 Rz. 112, 16-17. – Kybernetik ist nach ihrem Begründer Norbert Wiener die Wissenschaft der Steuerung und Regelung von Maschinen, lebenden Organismen und sozialen Organisationen. Ein typisches Beispiel für das Prinzip eines kybernetischen Systems ist ein Thermostat. Er vergleicht den Istwert eines Thermometers mit einem Sollwert, der als gewünschte Temperatur eingestellt wurde. Ein Unterschied zwischen diesen beiden Werten veranlasst den Regler im Thermostat dazu, die Heizung so zu regulieren, dass sich der Istwert dem Sollwert angleicht. (Quelle: de.wikipedia.org)

[3] Günther Anders, Die Antiquiertheit des Menschen. Über die Seele im Zeitalter der zweiten industriellen Revolution, München 1956, zit. nach Frisch (Anm. 1), S. 291 Rz. 112, 16-17.

[4] Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988, BBl 1988 II 413, hier 417-418.

gleich Zugriff auf ihren Standort, ihre Kalenderdaten und ihr Adressbuch – sie gewährt ihnen mit anderen Worten mehr Einblicke als der Vertrauensärztin[5].

Der Staat scheint aber auch nicht ganz draussen zu sein. Das Unternehmen «Recorded Future» analysiert Internetdaten – offenbar v.a. soziale Netzwerke und Bewegungsprofile – und macht daraus Vorhersagen. Es soll eine Zusammenarbeit von Google und dem CIA sein. Google Street View sammelt Foto- und 3D-Daten sowie Daten über Funknetze: Netzwerknamen, Verschlüsselungsstärke, MAC-Adressen der verwendeten Gerät. Diese WLAN-Daten sollen zur WLAN-basierten Ortung dienen. Bei nicht verschlüsselten Netzwerken wurden auch die übermittelten Daten mitgeschnitten. Google Indoor Maps zeigt nun auch noch eine Innenansicht der Gebäude. Die nötigen Daten werden von den Eigentümern hochgeladen. So lässt sich z.B. einfach schon vor dem Besuch des Shopping-Centers erkennen, welcher Parkplatz am nächsten beim Lift ist. Militärische Anwendungen für solche Dienste sind natürlich ebenfalls denkbar. Benutzt werden die Daten aber auch von Zoll- und Polizeibehörden. Beispielsweise sind Informationen über Buchbestellungen und andere Käufe auf Amazon den Zoll- und Einwanderungsbeamten der USA offenbar frei zugänglich. So wurde ein Fall bekannt, bei dem einer Reisenden an einem amerikanischen Flughafen möglicherweise aufgrund ihrer Bestellungen bei Amazon die Einreise verweigert wurde[6]. Die Firma Axciom soll detaillierte Daten von 500 Millionen Kunden für Direktmarketingzwecke anbieten; sie soll ausserdem der amerikanischen Regierung Daten über 11 der 19 Attentäter vom 11. September 2001 geliefert haben[7]. Auch Google gewährt dem Staat Zugriff auf die Nutzerdaten[8]. Und wer sich die Datenschutzerklärungen von Online-Reiseveranstaltern wie z.B. Ebookers angeschaut hat, weiss, dass die «Regierung der Vereinigten Staaten und anderer Länder Zugriff auf die Aufzeichnungen der Passagierinformationen verlangen» können[9].

Das Internet schafft ein globales Dorf. Der Klatsch und die Überwachung finden global statt. Die dörfliche Kontrolle ist global geworden. Wir haben Kontrolle wie im Dorf[10]. Und wie im Dorf auch wird im Internet nichts vergessen. Nur, dass die Erinnerungen im Internet schwarz auf weiss bzw. in farbigen Bildern und Filmen gespeichert bleiben.

---

5 Eine Übersicht über die Zugriffsrechte der verschiedenen Apps findet sich unter https://play.google.com/store/apps/details?id=com.popularapp.periodcalendar&hl=de.

6 http://de.wikipedia.org/wiki/Amazon.com («Datenschutz»); Michael Voregger, Datenhunger: Amazon, Terror-Abwehr und der Staatsschutz, spiegel.de, 26. Juli, 2005; vgl. Interpellation 13.30333 (Schwaab) vom 6. März 2013, «Personendaten von Schweizerbürgerinnen und -bürgern in den Händen amerikanischer Unternehmen: Wie können sie geschützt werden?»

7 New York Times vom 17. Juni 2012, abrufbar unter http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?pagewanted=all&_r=0.

8 Google kommt dabei v.a. den Anweisungen den USA nach. In der Periode Januar – Juni 2012 gewährte Google den USA in 90% der Fälle Zugriff auf die verlangten Nutzerdaten, der Schweiz dagegen nur in 68% der Fälle. Die Anfragen der USA betrafen dabei über 16‘000 Nutzer/Konten, die der Schweiz nur 113. Die USA verlangten bei weitem am meisten Auskunft, weit vor Indien mit rund 3‘400 Nutzern/Konten, und erhielten diese auch am meisten, weit vor Dänemark (78%);
s. http://www.google.com/transparencyreport/userdatarequests/.

9 http://www.ebookers.ch/info/win?id=PrivacyPolicy, Ziff. 6, Sicherheit (abgerufen am 5. April 2013).

10 Vgl. den BGE 138 II 346 (Google Street View), S. 372. Erw. 10.6.6, wonach «angesichts der in der heutigen Gesellschaft faktisch bestehenden Einbindung von Personendaten in die soziale Realität nicht ein totaler Schutz vor einer unbefugten Bildveröffentlichung gewährleistet werden kann».

c. Information und Manipulation

Die Rechenleistungen von Computerchips nimmt dabei exponentiell zu. Die Speicherkapazität wächst sogar noch schneller. Nach der Vernetzung von Computern treten wir jetzt in eine Phase des «Internets der Dinge» ein, in der Computerchips und Messsensoren bald überall in grossen Mengen verstreut sein werden, um riesige Datenmengen – «Big Data» – produzieren. Es werden nicht nur Smartphones, Computer und Fabriken vernetzt sein, sondern auch Autos, Heizungen, Lampen und Kleider. Die Verbrauchsdaten von Strom, Heizung und Wasser werden «online» gehen. Dazu kommen Kreditkartentransaktionen, Kundenkarten, Telekommunikations-Verbindungsdaten, Zugriffsstatistiken auf Websites, Mobilitätsmuster und vieles mehr. Je mehr Daten über uns generiert werden, desto mehr wird es Unternehmen möglich sein, unser Verhalten besser zu kennen als unser Freundeskreis, besser als unsere Partnerin, unser Partner. Besser, als es sich je ein Geheimdienst erträumt hätte[11].

Die Informationen dienen dazu, unser individuelles Verhalten zu erforschen. Wir erhalten in der Folge individualisierte Suchresultate, individualisierte Werbung, individualisierte Facebook-Freunde. Der Wahlsieg von Barack Obama wird nicht zuletzt IT-Experten zugeschrieben, welche unter Einsatz von «Big Data» und «Predicitive Analytics» den Wahlkampf minutiös planten und steuerten. Ihnen stand eine Datenbank mit Informationen über fast 200 Millionen Stimmbürgerinnen und Stimmbürger zur Verfügung – öffentlich verfügbare Daten kombiniert mit Daten aus den Registern der Partei, E-Mail-Adressen, Facebook-Profilen und dazugekauften Daten. Dank diesen Daten konnten Wahlhelfer unentschlossene, aber strategisch wichtige Personen direkt ansprechen[12].

Es werden Produkte und Dienstleistungen entwickelt, die den Bedürfnissen der Kunden besser entsprechen. Es gibt sogar «lernende Produkte», wie z.B. der Thermostat der Firma Nest, der den Lebensrhythmus der Bewohner erkennt und die Temperatur danach ausrichtet. Aus aggregierten Zeit- und Standortdaten von Android-Smartphones ermittelt die Google-Navigation für uns eine staufreie Route[13]. Kurz: Eine auf uns zugeschnittene, individualisierte Welt kommt zu uns. Das wird aber auch bedeuten: Computer werden mehr und mehr entscheiden, zu welchen Konditionen wir Kredite bekommen oder wie hoch unsere Versicherungsprämie ist, und zwar auf der Grundlage der über uns gesammelten Informationen[14].

Der Schritt von der Information zur Manipulation durch selektive Datenbearbeitung und -interpretation ist dabei klein. Die Art und Weise, wie die Daten gefiltert, verknüpft und neu

---

[11] Dirk Helbing, Google als Gott?, NZZ Nr. 66 vom 20. März 2013, S. 31, abrufbar unter http://www.nzz.ch/aktuell/wirtschaft/wirtschaftsnachrichten/google-als-gott-1.18049950. S. a. die Deklaration von Mexiko-Stadt der 33. Internationalen Konferenz der Datenschutzbeauftragten, abrufbar unter http://www.edoeb.admin.ch/org/00135/00136/index.html?lang=de.

[12] Günter Karjoth, Viele kleine Daten, grosse Wirkung, digma 2013, S. 4.

[13] Sören Preibusch, Big Data, Small Money, No Privacy?, digma 2013, S. 19.

[14] Dirk Helbing, Google als Gott?, NZZ Nr. 66 vom 20. März 2013, S. 31, abrufbar unter http://www.nzz.ch/aktuell/wirtschaft/wirtschaftsnachrichten/google-als-gott-1.18049950. Art. 8 Bst. b des Vorschlag des Konsultativausschusses des Europarats (T-PD) für eine Modernisierung der Konvention 108 sieht vor, dass bedeutende Entscheide nicht einzig auf der Grundlage automatisierter Datenbearbeitung erfolgen dürfen (abrufbar unter http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD%282012%2904rev3%20Fr.doc%20-%20Modernisation%20de%20la%20Convention%20108.pdf).

zusammengestellt werden, bleibt Verborgen. Wo genau Daten generiert werden, wer diese bearbeitet und zu welchem Zweck, auch. Manipulationen sind möglich.

Manipulationen können auch dadurch erfolgen, dass Unternehmen Personen bezahlen, welche in sozialen Netzwerken als unabhängige Konsumenten auftreten und positive Informationen über ihre Waren verbreiten. Dabei können nur wenige Personen Aktivitäten grösserer Gruppen vortäuschen. Es können gefälschte Blogs, sogenannte «Flogs» (Fake Blogs) oder Sockpuppets (gefälschte Online-Identitäten) eingesetzt werden, welche unabhängig erscheinen, aber reine Werbezwecke verfolgen. Ähnliche Methoden können auch eingesetzt werden, um die politische Meinungsbildung zu beeinflussen. Das Vorgehen wird «Astroturfing» oder «Kunstrasenbewegung» genannt, weil der Eindruck einer spontanen Bewegung aus der Basis der Bevölkerung – eine «Grassroots-Bewegung» – vorgetäuscht wird («AstroTurf» ist eine amerikanische Kunstrasenmarke). Sicherheitslücken ermöglichen einen Angriff auf die Privatsphäre, aber auch die Steuerung und Beschädigung des betroffenen Produkts, z.B. einer Heizanlage[15].

2. Der Ruf nach Prävention, Transparenz und Kontrolle

a. Der Evaluationsbericht des Bundesrates

Der Bundesrat fordert vor dem Hintergrund dieser unüberschaubaren, undurchsichtigen Datenbearbeitungen in seinem Bericht vom 9. Dezember 2011 über die Evaluation des Datenschutzgesetzes mehr *Transparenz*[16]. Ausserdem solle die *Kontrolle* über einmal bekanntgegebene Daten verbessert werden; der Bundesrat denkt dabei an eine Stärkung der Aufsicht durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) und der Rechtsansprüche sowie deren Durchsetzung, z.B. mittels kollektiver Rechtsdurchsetzung, sowie eine Präzisierung des Rechts auf Vergessen. Er schlägt ausserdem eine *Sensibilisierung* für die Risiken von Persönlichkeitsverletzungen vor, die von den neuen technologischen Möglichkeiten ausgehen. Einen besonderen *Schutz* verdienten Minderjährige. Nicht zu vergessen ist die *Prävention*: Datenschutzprobleme sollen schon bei der Entwicklung neuer Produkte erkannt («Privacy by Design») und datenschutzfreundliche Technologien gefördert werden[17].

b. Die Revisionsarbeiten von Europarat und EU

Der Bundesrat will ausserdem dem Umstand Rechnung tragen, dass zurzeit in der EU und im Europarat Revisionsarbeiten im Gange sind: Diese betreffen das von der Schweiz ratifizierte Übereinkommen Nr. 108 des Europarates und die Richtlinie 95/46/EG[18].

---

15 Fernwärme – Hacker regeln die Temperatur, NZZ Nr. 89 vom 18. April 2013, S. 58.

16 BBl 2012 335, hier 341-342 u. 350.

17 BBl 2012 335, hier 350.

18 BBl 2012 335, hier 349; vgl. a. Luzius Mader/Martin Hilti, Europarechtliche Vorgaben im Bereich Datenschutz: Implikationen für die Schweiz, in: Astrid Epiney/Tobias Fasnacht (Hrsg.), Die Entwicklung der europarechtlichen Vorgaben im Bereich des Datenschutzes und Implikationen für die Schweiz, Zürich 2012, S. 69 ff.

Zum Übereinkommen Nr. 108 des Europarates liegt ein Vorschlag des Konsultativausschusses des *Europarats* (T-PD) für eine Modernisierung der Konvention 108 vor[19] vor. der T-PD hat die Beratung noch nicht abgeschlossen. Für den Ersatz der Richtlinie wird der Vorschlag der *Europäischen Kommission* für eine Datenschutz-Grundverordnung vom 25. Januar 2012 (nachfolgend «Datenschutz-Grundverordnung»[20]) gegenwärtig von der Arbeitsgruppe des Rates «Informationsaustausch und Datenschutz» (Working Party on Data Protection an Exchange of Information, DAPIX) behandelt. In der Begründung zur Datenschutz-Grundverordnung betont die Kommission, dass die wirtschaftliche Entwicklung Vertrauen in die «Online-Umgebung» voraussetze und der Schutz personenbezogener Daten daher eine zentrale Rolle spiele[21].

Ob die Datenschutz-Grundverordnung in den Anwendungsbereich des Schengen/Dublin Assoziierungsabkommens fällt, wird gegenwärtig diskutiert; ein abschliessender Entscheid steht noch aus[22]. Für diesen Bereich gilt hingegen der Vorschlag der Kommission für eine Richtlinie der Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung und Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr [23], die ebenfalls noch in der DAPIX beraten wird; im Folgenden befasse ich mich nicht mit der Richtlinie, die spezifisch den polizeilichen und justiziellen Bereich betrifft. Zu erwähnen ist schliesslich die sog. E-Privacy-Richtlinie der EU für mehr Transparenz im Internet[24].

Das EU-Datenschutzrecht erlaubt die grenzüberschreitende Datenübermittlung mit Drittstaaten, wenn diese ein «angemessenes Schutzniveau» gewährleisten[25]. Die Schweiz ist – ausser im Bereich von Schengen/Dublin – ein Drittstaat. Sie evaluiert das Datenschutzniveau periodisch, und je stärker sich die Schweiz vom EU-Niveau entfernen würde, desto mehr besteht das Risiko, dass die EU den Schweizer Datenschutz als ungenügend beurteilen könnte[26]. Dies würde einen Datenaustausch mit der EU – insbesondere auch mit in der EU ansässigen Unternehmen – viel schwieriger gestalten.

---

[19] T-PD_2012_04_rev3, abrufbar unter http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD%282012%2904rev3%20Fr.doc%20-%20Modernisation%20de%20la%20Convention%20108.pdf. Der T-PD wird Stellvertreter des EDÖB präsidiert.

[20] KOM(2012) 11 endgültig, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF

[21] KOM(2012) 11 endgültig, S. 1, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF.

[22] Vgl. Luzius Mader/Martin Hilti, Europarechtliche Vorgaben im Bereich Datenschutz: Implikationen für die Schweiz, in: Astrid Epiney/Tobias Fasnacht (Hrsg.), Die Entwicklung der europarechtlichen Vorgaben im Bereich des Datenschutzes und Implikationen für die Schweiz, Zürich 2012, S. 77.

[23] Kom(2012) 10 endgültig, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:DE:PDF.

[24] Richtlinie 2009/136/EG vom 25. November 2009, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:De:PDF.

[25] Art. 25 Richtlinie 95/46/EG vom 24. Oktober 1995, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:PDF.

[26] Im Hinblick auf die Inkraftsetzung des Schengen-Besitzstands wurde die Schweiz in der ersten Hälfte des Jahrs 2008 einer Evaluation durch die EU unterzogen. Aufgrund der Empfehlungen der EU wurde die Unabhängigkeit des EDÖB gestärkt; s. BBl 2009 6749, hier 6756

Anzufügen ist, dass der Bundesrat 1988 im ersten Integrationsbericht angekündigt hatte, die Europakompatibilität schweizerischer Erlasse zum festen Bestandteil bundesrätlicher Botschaften ans Parlament zu machen: Der für die Schweiz wichtigste Markt bestimmt die Spielregeln. Angestrebt werde in den Bereichen von grenzüberschreitender Bedeutung eine grösstmögliche Vereinbarkeit der schweizerischen Rechtsvorschriften mit denjenigen der europäischen Partner, was auch den Verzicht beinhalten könne, schweizerische Sonderlösungen um jeden Preis durchsetzen zu wollen[27]. Seither enthält jede Botschaft einen Abschnitt über die Europarechts-Kompatibilität eines vorgeschlagenen Erlasses. Diese Massnahme ist nicht einzigartig in Europa. Auch Schweden praktizierte ab 1988 und bis zum Beitritt zu den Europäischen Gemeinschaften den autonomen Nachvollzug; gemeinschaftswidrige Bestimmungen waren nur aus zwingenden Gründen zulässig[28].

c. Wirtschaftliche Aspekte

Personendaten sind in der digitalen Gesellschaft eine Währung geworden, mit der die Konsumentinnen und Konsumenten für Leistungen oder Rabatte bezahlen[29]. Beispiele sind Sparkarten (z.B. Supercard), Smartphone-Spiele (z.B. Angry Birds), Suchmaschinen (z.B. Google), Soziale Netzwerke (z.B. Facebook) oder Reisebüroleistungen (z.B. Ebookers). Eine Studie der Boston Consulting Group (BCG) von 2012[30] beziffert den Wert der digitalen Personendaten auf CHF 381 Mia. Die grössten Nutzniesser mit 40% sind laut der Studie die Öffentliche Hand und das Gesundheitswesen. Unternehmen nutzen digitale Personendaten insbesondere für personalisierte Werbung. Google z.B. macht 96% seines Umsatzes mit dem Verkauf von personalisierter Werbung; Amazon soll 25% seiner Verkäufe dank personalisierten Produkteempfehlungen erzielen. Daten können aber auch verkauft werden: Im Oktober 2012 hatte der spanische Telekommunikationskonzern Telefónica angekündigt, Standortdaten seiner Kunden aufbereiten und verkaufen zu wollen, mit dem Ziel, Wert aus «Big Data» zu schaffen[31]. Die Kostenersparnis, die die Konsumenten zumindest teilweise durch die Bezahlung mit digitaler statt realer Währung erzielen, schätzt BCG für das Jahr 2020 auf CHF 810 Mia. Umgekehrt sind Private auch bereit, mehr zu bezahlen, statt Daten preiszugeben[32].

Damit eine Währung stabil ist, braucht es Vertrauen. Fast 90% der Personen, die «online» sind, denken nach der BCG-Studie aber, dass ihre Privatsphäre durch die Industrie bedroht ist. 79% forderten, die Unternehmen sollten transparenter über den Umgang mit ihren Personendaten informieren. Nur jeder Dritte wusste mehr oder weniger, welche Sektoren Daten sammeln, und nur jeder zehnte schützt seine Privatsphäre aktiv. Die Studie der BCG kommt deshalb zum Schluss, die grösste Herausforderung zur Erhaltung und Steigerung des

---

27 Bericht des Bundesrates vom 24. August 1988 über die Stellung der Schweiz im europäischen Integrationsprozess, BBl 1988 III 380.

28 Bertil Cottier, Suède, in: Schweizerisches Institut für Rechtsvergleichung (Hrsg.), Staasrechtliche Auswirkungen einer Mitgliedschaft in der Europäischen Union. Vier Studien im Rahmen des Integrationsberichts 1999, Zürich 1990, S. 256.

29 Vgl. etwa Sören Preibusch, Big Data, Small Money, No Privacy?, digma 2013, S. 18.

30 Boston Consulting Group, The Value of Our Digital Identity, November 2012, abrufbar unter http://www.lgi.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf.

31 Sören Preibusch, Big Data, Small Money, No Privacy?, digma 2013, S. 18.

32 Sören Preibusch, Big Data, Small Money, No Privacy?, digma 2013, S. 20-21.

Geschäfts mit den digitalen Personendaten sei es, einen transparenten, vertrauenswürdigen Datenfluss herzustellen[33]. BCG schätzt, dass zwei Drittel des potentiellen Werts digitaler Personendaten gefährdet seien, wenn dies nicht gelinge.

Die Federal Trade Commission der USA schätzte 2002, dass E-Commerce-Unternehmen jährlich $ 18 Mia. entgehen, weil sie zu viele Personendaten verlangt werden[34]. Auch Lücken in der Datensicherheit kommen Unternehmen teuer zu stehen. Das Hacken von Sonys PlayStation Network, bei dem die Personendaten von 77 Mio. Abonnenten gestohlen worden waren, zwang den Konzern, den Dienst für 24 Tage stillzulegen und verursachte ihm direkte Kosten von rund CHF 146 Mio[35]. Mängel im Datenschutz oder der Datensicherheit schädigen das Ansehen der Marke des betroffenen Unternehmens, die Kundenbeziehungen und die Reputation. «Datenschutzerklärungen», die zu extensiv zu Gunsten von Unternehmen sind, müssen auf Druck der Konsumenten wieder zurückgenommen werden, so geschehen z.B. im Fall von Facebook oder Instagram. Auf Konsumentenseite entstehen durch mangelnden Datenschutz bzw. zur Sicherstellung des Datenschutzes Kosten; in einer schon älteren Studie aus den USA sind diese auf von mehrere hundert Dollar pro Jahr und Familie geschätzt worden[36].

Damit auf Personendaten basierende Geschäftsmodelle dauerhaft bestehen bleiben können, braucht es gemäss der BCG-Studie verantwortungsbewusste Unternehmen, eine transparente Datenbearbeitung, eine informierte Einwilligung der Konsumenten und die Kontrolle der Personendaten durch die Konsumenten. Dies entspricht den Schlussfolgerungen des Bundesrates und der EU-Kommission: gefordert sind *Prävention*, *Transparenz* und *Kontrolle*.

An drei möglichen Massnahmen zur Verbesserung der Prävention, der Transparenz und der Kontrolle soll nachfolgend aufgezeigt werden, wie sich die Arbeiten auf europäischer Ebene auf die Revisionsarbeiten in der Schweiz auswirken.

3. Prävention: «Privacy by Design»

a. Ausganslage

Nach dem Grundsatz «Privacy by Design» (auch: integrierter Datenschutz, Datenschutz durch Technik) sollen Datenschutzprobleme schon bei der Entwicklung neuer Technologien festgestellt werden und nicht bloss nachträglich behoben werden[37]. Grundsätze, die für

---

[33] Ebenso Jamie Bartelett, The Data Dialogue, Demos, 2012, abrufbar unter http://www.demos.co.uk/files/The_Data_Dialogue.pdf?1347544233.

[34] Zit. in Robert Gellman, Privacy, Consumers, and Costs: How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete, Washington 2002, S. 4 u. 16, abrufbar unter http://epic.org/reports/dmfprivacy.pdf.

[35] S. die Hinw. in der Studie der Boston Consulting Group, S. 27, abrufbar unter http://www.lgi.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf.

[36] Zit. in Robert Gellman, Privacy, Consumers, and Costs: How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete, Washington 2002, S. 4, abrufbar unter http://epic.org/reports/dmfprivacy.pdf.

[37] Bericht des Bundesrates vom 9. Dezember 2011 über die Evaluation des Bundesgesetzes über den Datenschutz, BBl 2012 335, hier 346 Anm. 11.

«Privacy by Design» gelten sollen, sind an der 32. Internationalen Konferenz der Datenschutzbeauftragten verabschiedet worden[38]: Proactive not Reactive; Preventative not Remedial; Privacy as the Default; Privacy Embedded into Design; Full Functionality: Positive-Sum, not Zero-Sum; End-to-End Lifecycle Protection; Visibility and Transparency; Respect for User Privacy. «Privacy by Design» ist in den Augen der Datenschutzbeauftragten ein unverzichtbarer Bestandteil des Persönlichkeitsschutzes[39].

In der Praxis hat die datenschutzfreundliche Technikgestaltung indes bisher kaum Fuss gefasst. Für das fehlende Interesse führen die Datenbearbeiter die Kosten, die Ineffizienz von datenschutzfreundlichen Prozessen und die nicht mehr mögliche umfassende Auswertung der Personendaten an, während die betroffenen Personen keinen unmittelbaren Zusammenhang zwischen der Bekanntgabe von Personendaten und den möglichen Konsequenzen eines Missbrauchs dieser Daten sehen[40]. Vereinzelt scheint sich aber verbesserter Datenschutz als Wettbewerbsvorteil durchzusetzen: z.B. wird der Internet Explorer 10 von Windows mit der Voreinstellung «Do-not-Track» ausgeliefert. Von zunehmender Bedeutung ist die Selbstregulierung bei der *«Privacy Compliance»*, wobei die Datenschutz-Folgenabschätzung (Privacy Impact Assessment, PIA) am meisten Bedeutung hat, wie sie von der EU und anderen Institutionen entwickelt worden ist[41]. Des Weiteren enthält das DSG mit dem *Zertifizierungsverfahren* und dem Datenschutz-Qualitätszeichen (Art. 11 DSG) bereits eine Grundlage für die gesetzliche Anerkennung von regulierten Selbstregulierungen. Die Zertifizierung ist jedoch freiwillig. In der Praxis konnte sie sich nicht durchsetzen. Nur 15 Unternehmen sind zertifiziert, bei einem davon allerdings nur zwei Teilbereiche. Nur drei Unternehmen haben dem EDÖB die Zertifizierung gemeldet[42]. Und schliesslich hat der EDÖB eine *Empfehlungen* zur Anwendung von Privacy by Design erlassen: Er empfahl Google, «Google Street View» nach den Grundsätzen von «Privacy by Design» zu entwickeln[43].

In der Lehre wird angeregt, durch Regulierung die technische Ausgestaltung von Systemen von Anfang an auf datenschutzkonforme Wege zu bringen[44]. Vorgeschlagen wird einerseits die *«regulierte Selbstregulierung»*. Bei dieser definiert der Staat Regulierungsziele und den rechtlichen Rahmen, innerhalb dessen ein Ziel realisiert werden soll. Die Umsetzung und

---

38 Abrufbar unter http://www.ipc.on.ca/site_documents/pbd-resolution.pdf (Enlever ce lien si sur EDÖB ils n'ont plus la DRAFT); s. a. http://www.edoeb.admin.ch/org/00135/00136/index.html?lang=de. Vgl. dazu Martin Rost, Kirsten Bock, Privacy By Design und die Neuen Schutzziele. Grundsätze, Ziele und Anforderungen, DuD 1/2011, S. 30 ff., abrufbar unter https://www.european-privacy-seal.eu/results/articles/DuD2011-01-RostBock-PbD-NSZ.pdf.

39 Bericht des Bundesrates vom 9. Dezember 2011 über die Evaluation des Bundesgesetzes über den Datenschutz, BBl 2012 335, hier 346.

40 Bruno Baeriswyl, PET- ein Konzept harrt der Umsetzung, digma 2012, S. 18, m. Hinw.

41 Rolf H. Weber, Can Data Protection be Improved through Privacy Impact Assessments?, jusletter-it vom 12.9.2012, Rz. 1.

42 Ursula Uttinger, Datenschutzüberprüfungen: Zertifizierungen sowie andere Möglichkeiten oder: Was hat Art. 11 DSG verändert? in: Ueli Kieser/Kurt Pärli, Datenschutz im Arbeits-, Versicherungs- und Sozialbererich: Aktuelle Herausforderungen, St. Gallen 2012, S. 73 f.

43 18. Tätigkeitsbericht (2011/12), S. 40.

44 Kurt Pärli, Datenschutz durch Selbstregulierung?, digma 2011, S. 69, m. Hinw. auf Brunner und Rudin. Zur Regulierung, Deregulierung und Selbstregulierung s. etwa Christoph Errass, Kooperative Rechtsetzung, Zürich/St. Gallen 2010; Luzius Mader/Bernhard Rütsche, Regulierung, Deregulierung, Selbstregulierung: Anmerkungen aus legistischer Sicht, Referate und Mitteilungen des Schweizerischen Juristenvereins, Heft 1/2004, sowie ZSR 123 II 2004, S. 3 ff.

Konkretisierung des Regelungsziels wird danach betroffenen und beteiligten Privaten überlassen. Zu beachten sei dabei, dass die Selbstregulierung nicht nur von den Produzenten ausgeht, sondern auch die Verbände der Konsumenten, Arbeitnehmerinnen, Versicherten, Patientinnen etc. einbezogen werden[45]. Diskutiert wird andererseits die *private Selbstregulierung*. Weil sie von privaten Anreizen angetrieben werde, führe (private) Selbstregulierung zu bedürfnisorientierten Regelungen. Ein Hauptvorteil dieser Selbstregulierung könne darin gesehen werden, dass sie nicht an das Territorialitätsprinzip gebunden sei (internationale Abkommen hätten kaum Chancen, da kein internationaler Konsens zum Personendatenschutz bestehe; daher gebe es nur regionale Abkommen wie z.B. im Rahmen der EU[46]). Andere Vorteile lägen darin, dass Selbstregulierung effizient auf echte Bedürfnisse reagieren und die Technologien spiegeln könne, offen sei für einen permanenten Konsultationsprozess und rechtzeitige Anpassungen, wenn Technologien ändern, sowie dazu anreize, die selbstgegebenen Regeln zu beachten. Nachteile der Selbstregulierung seien die fehlende demokratische Legitimation (Problem der Outsider), die fehlende rechtliche Verbindlichkeit, die nicht immer gegebene Stabilität sowie insbesondere meist fehlende Durchsetzungsverfahren und Sanktionen[47]. Auch wird geltend gemacht, dass *Zielkonflikte* zwischen den neuen Technologien wie Smart Grids und Smart Metering und datenschutzfreundlicher Technikgestaltung bestünden: Mit den ersteren wird beabsichtigt, möglichst viele Personendaten zu sammeln, während letztere möglichst wenig Daten erfassen möchte[48]. Die Chancen und Risiken neuer Technologien seien deshalb in erster Linie in einem gesellschaftlichen Diskurs auszudiskutieren[49]. *Bereichsspezifische Regelungen* zur Einschränkung der negativen Folgen neuer Technologien könnten im Rahmen einer (staatlichen) *Vorabkontrolle* erfolgen[50] oder einer *Datenschutz-Folgenabschätzung* (Art. 33 Datenschutz-Grundverordnung) getroffen werden. Dabei sollten technische Massnahmen im Vordergrund stehen: Pseudonymisierung, Verschlüsselung, sichere Löschung, etc. [51] «Privacy by Design» ist ein Teil von PIA[52].

b. Vorstellungen des Bundesrates

Als erste Zielsetzung der Revisionsarbeiten nennt der Bundesrat, dass der Datenschutz früher greifen solle. Datenschutzprobleme sollen schon bei der Entwicklung neuer Technologien festgestellt und geprüft werden. Damit soll verhindert werden, dass bestehende Datenschutzprobleme lediglich nachträglich durch Korrekturprogramme behoben werden (Vertiefung des Konzepts «Privacy by Design»). Daneben sollen datenschutzfreundliche Technologien gefördert werden. Untersuchen möchte der Bundesrat ausserdem, ob die

---

[45] Kurt Pärli, Datenschutz durch Selbstregulierung?, digma 2011, S. 67 u. 69.

[46] Rolf H. Weber, Can Data Protection be Improved throug Privacy Impact Assessments?, jusletter-it vom 12.9.2012, Rz. 10.

[47] Rolf H. Weber, Can Data Protection be Improved throug Privacy Impact Assessments?, jusletter-it vom 12.9.2012, Rz. 6-7.

[48] Bruno Baeriswyl, PET- ein Konzept harrt der Umsetzung, digma 2012, S. 18 ff.

[49] Bruno Baeriswyl, PET- ein Konzept harrt der Umsetzung, digma 2012, S. 21.

[50] Verschiedene Kantone kennen eine Vorabkontrolle durch den Datenschutzbeauftragten für Datenbearbeitungen durch öffentliche Organe, wenn diese ein besonderes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt (z.B. § 10 IDG-ZH, Art. 17a DSG-BE, § 23 DSG-LU, Art. 8 DSG-SG).

[51] Bruno Baeriswyl, PET- ein Konzept harrt der Umsetzung, digma 2012, S. 21.

[52] Rolf H. Weber, Can Data Protection be Improved through Privacy Impact Assessments?, jusletter-it vom 12.9.2012, Rz. 36.

Selbstregulierung verstärkt werden sollte, etwa indem Branchenorganisationen eine vom EDÖB zu genehmigende «Gute Praxis» definieren[53].

c. Vorschläge von Europarat und EU

Nach dem Vorschlag des Konsultativausschusses des *Europarats* (Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, T-PD) für eine Modernisierung der Konvention 108 sollen Produkte und Dienstleistungen nach dem Grundsatz «Privacy by Design» entwickelt werden (Art. 8bis Abs. 3[54]).

Art. 23 der Datenschutz-Grundverordnung sieht vor, dass der für die Datenbearbeitung Verantwortliche zum Zeitpunkt der Festlegung der Verarbeitungsmittel technische und organisatorische Massnahmen und Mittel durchführen muss, die sicherstellen, dass die Datenbearbeitung der Datenschutz-Grundverordnung genügt und die Rechte der betroffenen Personen wahrt. Es sollen nur die für die spezifischen Zwecke der Bearbeitung benötigen Daten bearbeitet werden (Grundsatz der Datensparsamkeit). Der Vorschlag der Kommission sah ursprünglich vor, dass die Kommission in delegierten Rechtsakten die Details und technische Standards festlegt. Diese Ermächtigung ist im neusten Entwurf der Arbeitsgruppe des Rates (DAPIX) aber gestrichen worden, wie fast alle Delegationsklauseln zu Gunsten der Kommission.

Angemerkt sei, dass die *OECD* «Terms of Reference» verabschiedet hat, die als Leitfaden zur Überprüfung der OECD-Privacy-Guidelines dienen und die «Privacy by Design» als Schlüsselelement zur Verbesserung des Datenschutzes bezeichnen[55].

d. Beurteilung

Im Grundsatz ergibt sich «Privacy by Design» aus Art. 4 Abs. 2 DSG, wonach die Bearbeitung von Personendaten verhältnismässig sein soll. Auch die Grundsätze von Treu und Glauben, Zweckbindung und Erkennbarkeit (Art. 4 Abs. 2-4 DSG) dürften regelmässig verletzt sein, wenn ein Produkt den Datenschutz durch Technik nicht verwirklicht (z.B. wenn eine App wie etwa das äusserst populäre «Angry Birds» auf die Adressdaten des Smartphones zugreift oder der Heizzähler nicht nur zur Feststellung des Verbrauchs und die Kostenstellung benutzt wird, sondern auch, um die Heizgewohnheiten der Mieterinnen und Mieter zu erfassen). In Bezug auf private Datenbearbeiter stellt sich primär die Frage, ob eine Einwilligung zu solchen Datenbearbeitungen rechtsgültig erfolgte (Art. 13 Abs. 2 Bst. a DSG; Frage der ungewöhnlichen AGB). Relevant ist auch Art. 3 Abs. 1 Bst. u UWG, wonach die Benutzung von Daten zu Werbezwecken verboten ist, wenn ein Kunde einen entsprechenden Vermerk im Telefonbuch hat; eine Praxis zu dieser neuen Bestimmung muss sich erst noch etablieren.

---

53 Bericht des Bundesrates vom 9. Dezember 2011 über die Evaluation des Bundesgesetzes über den Datenschutz, BBl 2012 335, hier 350.

54 T-PD_2012_04_rev3, abrufbar unter http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD%282012%2904rev3%20Fr.doc%20-%20Modernisation%20de%20la%20Convention%20108.pdf.

55 http://www.oecd.org/sti/thereviewoftheoecdprivacyguidelines.htm

Mit einer *Sensibilisierung* der Produzenten und der besseren *Durchsetzung* des bestehenden Rechts könnte somit schon einiges erreicht werden. Der *EDÖB* könnte vermehrt Empfehlungen zur «Privacy by design» machen und bei einer Nichtbefolgung an das Bundesverwaltungsgericht gelangen (Art. 29 Abs. 3 u. 4 DSG). Er hat wie erwähnt schon empfohlen, Produkte (im konkreten Fall «Google Street View») nach dem Grundsatz von «Privacy by Design» zu entwickeln. Produzenten und Konsumenten könnten durch Informationen darüber, welche Produkte datenschutzfreundlich sind, sensibilisiert werden, analog zum Krankenkassenvergleich des BAG. Die Klagen nach UWG stehen zudem auch *Berufs- und Wirtschaftsverbänden*, *Konsumentenschutzorganisationen* sowie dem *Bund* offen (Art, 10 Abs. 2 UWG). Organisationen von gesamtschweizerischer Bedeutung steht die *Verbandsklage* zum Schutz der Persönlichkeit von bestimmten Personengruppen offen (Art. 80 ZPO). Diese Möglichkeiten könnten bei Bedarf genutzt werden. Der EDÖB und die Gerichte könnten so den allgemeinen DSG-Grundsätzen in Bezug auf «Privacy by design» Konturen verleihen.

Die Ressourcen des EDÖB sind allerdings begrenzt, und Klagen von Verbänden oder Privaten hatten bislang keine Bedeutung. Eine Konkretisierung der Verpflichtung zu «Privacy by Design», wie sie der Europarat, die OECD und die EU vorsieht, wäre deshalb ein Möglichkeit. Die Stossrichtung des Bundesrates und die Stossrichtungen, die der Europarat, die OECD und die EU verfolgen, gehen in die gleiche Richtung und sind relatif offen formuliert. Datenschutzverletzungen sollen schon bei der Konzeption eines Produkts oder einer Dienstleistung verhindert werden. Eine für die Schweiz denkbare Lösung wäre es, dass Branchenvertreter, Konsumentenorganisationen und der EDÖB *Leitlinien für eine «Gute Praxis»* ausarbeiteten. Diese könnten für verbindlich erklärt werden, mit der Möglichkeit, davon abzuweichen, wenn ein Datenbearbeiter gleichwertigen Schutz garantieren kann. Die Leitlinien könnten auch fakultativen Charakter haben. Derjenige, der die Leitlinien anwendete, würde dabei von der Vermutung profitieren, dass er seine Sorgfaltspflichten erfüllt hat. Denkbar wäre schliesslich auch eine *Zertifizierungspflicht* zum Nachweis, dass die Privacy-by-Design-Anforderungen erfüllt wurden. Diese Zertifizierungspflicht könnte allenfalls auf Datenbearbeitungen beschränkt werden, die besondere Risiken bergen.

Es wäre im Sinne der Europakompatibilität natürlich gut zu wissen, was die EU plant. Was die EU für eine Regelung vorsehen wird, ist aber im Detail noch offen. In der EU wird gegenwärtig über eine Zertifizierungspflicht diskutiert.

4. Transparenz: Informierte Zustimmung

a. Ausganslage

Unternehmen ziehen aus der Anhäufung von Personendaten geschäftlichen Nutzen. Grundlage für die Datenbearbeitung sind Datenschutzvereinbarungen, Allgemeine Geschäftsbestimmungen und Dienstnutzungsbestimmungen, mit denen die Datenbearbeiter weitreichende Einverständniserklärungen zur Erhebung, Speicherung, Nutzung und Weitergabe von Daten einholen. Die erhobenen Daten durchlaufen mehrere

Verarbeitungsschritte, damit aus «Big Data» schliesslich gewinnbringend nutzbare Hinweise wird[56].

Damit auf Personendaten basierende Geschäftsmodelle dauerhaft bestehen bleiben können, braucht es gemäss der schon erwähnten BCG-Studie von 2012[57] verantwortungsbewusste Unternehmen, eine transparente Datenbearbeitung, eine informierte Einwilligung der Konsumenten und die Kontrolle der Personendaten durch die Konsumenten. Dabei bestehe ein Spannungsverhältnis zwischen dem Wunsch der Konsumenten nach Kontrolle ihrer Privatsphäre und dem Bedürfnis nach bequemen Anwendungen, die es bei der Wahl zwischen «Opt-in» und «Opt-out» erläutern zu berücksichtigen gelte. Opt-in bedeutet, dass der Benutzer Cookies akzeptieren kann oder nicht, Opt-out, dass er die Cookies deaktivieren muss. Cookies können Logins, Passwörter und Präferenzen abspeichern, was für den Nutzer praktisch ist. Sie können aber auch dazu verwendet werden, das Surfverhalten einer Person im Internet zu verfolgen. Online-Werber können anhand von Cookies, die sie über unterschiedliche Webseiten verteilen, Nutzerprofile anlegen und Konsumenten gezielt bewerben (sog. Online Behavioural Advertising, OBA).

In der Schweiz gilt für Cookies das Prinzip des Opt-out (Art. 45*c* Bst. b FMG; eine ausdrückliche Einwilligung ist nur für die Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen nötig, Art. 4 Abs. 5 DSG). Das Bearbeiten von Daten auf fremden Geräten durch fernmeldetechnische Übertragung ist erlaubt, wenn die Benutzerinnen und Benutzer über die Bearbeitung und ihren Zweck informiert und darauf hingewiesen werden, dass sie die Bearbeitung ablehnen können. Es liegt an der betroffenen Person, sich gegen eine zu weit gehende Bearbeitung ihrer Personendaten zu wehren, indem sie diese ablehnt. Voraussetzung dafür ist, dass sie die Beschaffung der Personendaten und deren Zweck erkennen konnte (Art. 4 Abs. 3 u. 4 DSG). Andernfalls schützten sie nur die Grundsätze von Treu und Glauben und der Verhältnismässigkeit vor einer übermässigen Aushöhlung der Privatsphäre[58]. Sie können sich dabei auf das DSG (Art. 4 Abs. 2) und den neuen Art. 8 UWG berufen. Unlauter handelt danach insbesondere, wer allgemeine Geschäftsbedingungen verwendet, die in Treu und Glauben verletzender Weise zum Nachteil der Konsumentinnen und Konsumenten ein erhebliches und ungerechtfertigtes Missverhältnis zwischen den vertraglichen Rechten und den vertraglichen Pflichten vorsehen[59]. Die Neufassung strich das in Art. 8 UWG bisher geltende Erfordernis der Irreführung; der Nachweis der Täuschungsgefahr entfällt, so dass nun eine offenere Inhaltskontrolle von allgemeinen Geschäftsbestimmungen möglich erscheint.

b. Vorstellungen des Bundesrates

Der Bundesrat möchte die Transparenz über Datenbearbeitungen erhöhen, «insbesondere in neuen komplexen Konstellationen, in denen Datenbearbeitungen weder für die Betroffenen

---

56 Sören Preibusch, Big Data, Small Money, No Privacy?, digma 2013, S. 18.

57 Boston Consulting Group, The Value of Our Digital Identity, November 2012, abrufbar unter http://www.lgi.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf.

58 Vgl. David Rosenthal, Das Bauchgefühl im Datenschutz, in: Datenschutz-Forum Schweiz (Hrsg.), Von der Lochkarte zum Mobile Computing. 20 Jahre Datenschutz in der Schweiz, Zürich 2012, S. 84.

59 Vgl. dazu Erdem Büyüksagis, La bonne foi dans l'art. 8 LCD: un remède à l'impuissance des consommateurs face aux clauses générales «soi-disant» négociés?, AJP 2012 S. 1393; Florent Thouvnin, Art. 8 UWG: Zur Strukturierung eines strukturlosen Tatbestandes, Jusletter vom 29. Oktober 2012.

noch für den EDÖB ohne Weiteres erkennbar sind». Dabei müsse aber im Auge behalten werden, dass die betroffenen Personen nicht mit einer Informationsflut überfordert werden[60].

c. Vorschläge von Europarat und EU

Der Vorschlag des Konsultativausschusses des *Europarats* (T-PD) für eine Modernisierung der Konvention 108 sieht vor, dass eine Datenbearbeitung nur durchgeführt werden darf, wenn eine spezifische, freie, informierte Zustimmung der betroffenen Person oder eine legitime gesetzliche Grundlage vorliegt (Art. 5 Abs. 2[61]). Ob die Zustimmung auch explizit und eindeutig sein soll, ist noch umstritten; es ist also noch offen, ob der Europarat dem Opt-in- oder dem Opt-out-Modell folgen wird.

Die Datenschutz-Grundverordnung der *EU* sieht vor, dass eine Einwilligung explizit erfolgen muss (Art. 4 Ziff. 8); nach Art. 6 Abs. 1 Bst. a muss für eine rechtmässige Datenbearbeitung z.B. die betroffenen Person die Einwilligung für einen oder mehrere genau festgelegte Zwecke geben. Die betroffene Person kann die Einwilligung jederzeit widerrufen (Art. 7 Abs. 3 Datenschutz-Grundverordnung). Die Datenschutz-Grundverordnung sieht ausserdem vor, dass die Einwilligung keine Rechtsgrundlage für eine Datenbearbeitung darstellt, wenn zwischen der Position der betroffenen Person und dem für die Bearbeitung Verantwortlichen ein erhebliches Ungleichgewicht besteht (Art. 7 Abs. 4 Datenschutz-Grundverordnung); diese Bestimmung war aber sehr umstritten und wurde von der DAPIX gestrichen. Die E-Privacy-Richtlinie der EU für mehr Transparenz im Internet[62] will mehr Transparenz und Sicherheit für Verbraucher schaffen. Sie sieht in Art. 5 Abs. 3 die Einwilligung des Users nach eingehender Information über Art und Zweck der Datenbearbeitung vor. Er soll also eine informierte Zustimmung erteilen können (sog. «Informed Consent»). Ausnahmen gelten für Verfahren, deren alleiniger Zweck die Übertragung einer Nachricht ist, damit ein ausdrücklich gewünschter Dienst zur Verfügung gestellt werden kann (sog. «Session-Cookies»).

Die Umsetzung der Richtlinie ist nicht einfach, gilt es doch, einen praktikablen Weg zu finden, um den Anforderungen an die informierte Zustimmung zu genügen, ohne ein benutzerfreundliches Surfen zu verhindern. Als Reaktion hat die europäische Werbebranche die Initiative ergriffen und einen Verhaltenskodex für ihre Mitglieder erlassen. Der Nutzer soll auf ein Icon klicken können, das bei der Anwendung von OBA eingeblendet wird, das dem User erklärt, wer sich hinter der Werbung verbirgt und was mit seinen Nutzerdaten geschieht. Sodann soll er die Möglichkeit erhalten, sein Opt-out zu erklären und Firmen zu sperren, die derartige Cookies verwenden[63].

---

60 Bericht des Bundesrates vom 9. Dezember 2011 über die Evaluation des Bundesgesetzes über den Datenschutz, BBl 2012 335, hier 341-342 u. 350.

61 T-PD_2012_04_rev3, abrufbar unter http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD%282012%2904rev3%20Fr.doc%20-%20Modernisation%20de%20la%20Convention%20108.pdf.

62 Richtlinie 2009/136/EG vom 25. November 2009, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:De:PDF.

63 EDÖB, Erläuterungen zur E-Privacy-Richtlinie der EU für mehr Transparenz im Internet, abrufbar unter http://www.edoeb.admin.ch/datenschutz/00626/00878/00967/index.html?lang=de.

Die E-Privacy-Richtlinie der EU ist erst in einigen EU-Mitgliedstaaten umgesetzt werden. Einige Staaten haben eine Opt-in-Lösung gewählt; eine Browservoreinstellung genügt nicht, mit gewissen Ausnahmen z.B. für Cookies, die der Funktionalität der Website dienen (Frankreich, Vereinigtes Königreich, Niederlande, Griechenland)[64]. Es wird interessant sein, zu sehen, ob der Europarat eine Opt-in- oder eine Opt-out-Lösung beschliesst oder die Frage offen lässt. Dies scheint wahrscheinlich. Die 27 EU-Staaten haben im Europarat mit seinen 47 Mitgliedstaaten zwar eine Mehrheit, aber eine «unité de doctrine» in dieser Frage fehlt.

d. Beurteilung

Der EDÖB geht davon aus, dass mit der E-Privacy-Richtlinie in der EU die bisherige Opt-out-Lösung durch ein Opt-in nach informierter Zustimmung ersetzt worden ist. Die Ausgestaltung solle aber gleichzeitig benutzerfreundlich und einfach handhabbar sein[65]. Der Wunsch des Bundesrates nach mehr Transparenz spricht grundsätzlich für eine Opt-in Lösung, was eine Änderung von Art. 45*c* Bst. b FMG bedingen würde. Es gälte dann, einen praktikablen Weg zu finden, der Transparenz schafft, ohne das Surfen unnötig zu verkomplizieren. Mit dem obligatorischen Einblenden von Datenschutzerklärungen, die der User einfach wegklickte, würde kaum mehr Transparenz geschaffen. Praktikable Lösungen wären z.B. grafische Darstellungen wie etwa Lichtsignale, die je nach Datenhunger auf grün, orange oder rot stehen.

5. Kontrolle: Recht auf Vergessen

a. Ausganslage

Das Recht auf Vergessen gibt der betroffenen Person einen Anspruch darauf, dass nicht ohne bedeutende Rechtfertigung erneut über vergangene Tatsachten berichtet wird, die geeignet sind, ihren Ruf oder ihre Ehre zu schädigen[66]. Das Recht auf Vergessen basiert auf dem zivilrechtlichen Persönlichkeitsschutz (Art. 27 ff. ZGB). Es ergibt sich aber auch aus den allgemeinen Grundsätzen des Datenschutzrechts (Verhältnismässigkeit, Zweckbindung). Ob diese Bestimmungen bei der Datenbearbeitung im Internet und insbesondere in den Sozialen Netzwerken genügen, ist umstritten. Zwar sieht Art. 15 Abs. 1 DSG eine Klage auf Vernichtung der Daten vor. Effiziente Suchprogramme sowie unbegrenzte und immer günstigere Speicherkapazitäten führen aber dazu, dass im Internet nichts vergessen geht und der negative Zeitungsartikel oder die heute peinliche Partyphoto aus der Jugendzeit im Netz erhalten bleibt und bei einer Namenssuche rasch wieder auftaucht[67].

---

64 Geddy van Elburg, SIGEU Whitepaper on privacy compliance, Digital Analytics Association 2013, abrufbar unter http://www.digitalanalyticsassociation.org/?page=white paper_privacy

65 EDÖB, 18. Tätigkeitsbericht 2010/2011, S. 44.

66 Melanie Studer/Matthias Schweizer/Elke Brucker-Kley, Sterben und Erben in der digitalen Welt, Jusletter vom 12. Dezember 2012, Rz. 45; s. zur Entwicklung des Begriffs Rolf H. Weber, Der Ruf nach einem Recht auf Vergessen, digma 2011/3, S. 102.

67 Melanie Studer/Matthias Schweizer/Elke Brucker-Kley, Sterben und Erben in der digitalen Welt, Jusletter vom 12. Dezember 2012, Rz. 49 ff.

Vor diesem Hintergrund hat der Nationalrat 2012 ein Postulat angenommen, das den Bundesrat beauftragt, die Einführung eines «Rechts auf Vergessen im Internet» zu prüfen[68]. Zudem soll der Bundesrat prüfen, wie die Nutzerinnen und Nutzer dieses Recht besser geltend machen können. Auch der EDÖB fordert ein Recht auf Vergessen. Er denkt dabei an eine Verfallsfrist der Daten, eine Desindexierungspflicht, eine Regelung der Geolokalisierung, das Recht zu surfen, ohne beobachtet und profiliert zu werden, das Recht, sich der Veröffentlichung oder Indexierung von Daten im Internet zu widersetzen usw.[69].

Technisch lässt sich ein Recht auf Vergessen auf verschiedene Arten umsetzen: mit einem Verfalldatum für digitale Informationen; einer zeitgesteuerten, nicht wiederherstellbaren Löschung von Daten; oder mit einer Benachrichtigung zur Überprüfung auf Aktualität an die betroffenen Personen. Dies wird im Ansatz bereits genutzt; Wiki-Plattformen erinnern ihre Autoren in regelmässigen Abständen daran, ihre Artikel zu aktualisieren oder allenfalls zu löschen[70].

b. Vorstellungen des Bundesrates

Der Bundesrat hält im Evaluationsbericht fest, dass die Kontrolle und die Herrschaft über einmal bekannt gegebene Daten ein wichtiger Aspekt des Datenschutzes seien. Es solle eine Präzisierung des Rechts auf Vergessen erwogen werden[71]. Das oben erwähnte Postulat, das möchte, dass die Einführung eines Rechts auf Vergessen geprüft wird, hat der Bundesrat zur Annahme empfohlen.

c. Vorschläge von Europarat und EU

Im vorliegenden Entwurf einer revidierten *Konvention 108* ist ein Recht auf Vergessen nicht ausdrücklich vorgesehen. Im zuständigen Ausschuss (T-PD) wird die Auffassung vertreten, dass dieses Recht durch andere Bestimmungen abgedeckt ist: durch den Grundsatz der Verhältnismässigkeit (Art. 5 Abs. 1), die beschränkte Aufbewahrung (Art. 5 Abs. 3 Bst. e) und das Beschwerde- und Löschungsrecht der betroffenen Person (Art. 8 Bst. b u. e). Art. 17 der *Datenschutz-Grundverordnung* sieht hingegen ausdrücklich ein «Recht auf Vergessenwerden und auf Löschung» vor. Insbesondere sieht Art. 7 Abs. 3 der Datenschutz-Grundverordnung wie erwähnt vor, dass die betroffene Person das Recht hat, ihre Einwilligung zur Datenbearbeitung jederzeit zu widerrufen. Der Vorschlag der Kommission regelt in Art. 17 Abs. 2 der Datenschutz-Grundverordnung zudem, was geschieht, wenn die Daten, die gelöscht werden sollen, im Internet verbreitet wurden: Der für die Veröffentlichung Verantwortliche muss alle vertretbaren Schritte, auch technischer Art, unternehmen, um Dritte zu informieren, dass eine betroffene Person die Löschung verlangt. Alle Querverweise und Kopien sind zu löschen.

---

68 Postulat 12.3152 (Schwaab) vom 14. März 2012, «Recht auf Vergessen im Internet».

69 EDÖB, 18. Tätigkeitsbericht (2010/1011), S. 119.

70 Melanie Studer/Matthias Schweizer/Elke Brucker-Kley, Sterben und Erben in der digitalen Welt, Jusletter vom 12. Dezember 2012, Rz. 61.

71 Bericht des Bundesrates vom 9. Dezember 2011 über die Evaluation des Bundesgesetzes über den Datenschutz, BBl 2012 335, hier 350.

d. Beurteilung

Die Stossrichtung der Bemühungen des Europarates, der EU und des Bundesrates sind auch beim «Recht auf Vergessen» deckungsgleich. Der Europarat setzt aber auf bereits bestehende Prinzipien und Verfahren: Verhältnismässigkeit, Beschränkung der Aufbewahrungsdauer, Beschwerde- und Löschungsrecht. Die EU-Regelung beschreitet mit der ausdrücklichen Verankerung eines «Rechts auf Vergessenwerden» einen anderen Weg. Mit dem Recht, die für einen bestimmten Zweck gegebene Einwilligung jederzeit zu widerrufen (Art. 7 Abs. 3 Bst. b Datenschutz-Grundverordnung), geht das EU-Recht weiter als das geltende Schweizer Recht: Eine Einwilligung kann nach geltendem Schweizer Recht nur vor erfolgter Bearbeitung widerrufen werden; danach bleibt nur die Möglichkeit, die Einwilligung wegen Willensmängeln anzufechten, z.B. wegen Irrtums (Art. 23 ff. OR)[72]. Ein Ausbau des «Rechts auf Vergessen» könnte den Persönlichkeitsschutz, der mit dem Internet schwieriger geworden ist, wieder stärken. Die technischen Mittel zu seiner Durchsetzung scheinen auch zu bestehen.

6. Weiteres Vorgehen

Der Bundesrat hat das EJPD beauftragt, ihm bis Ende 2014 Vorschläge über eine allfällige Revision des Datenschutzgesetzes zu unterbreiten. Zuständig zur Vorbereitung der Vorschläge ist das Bundesamt für Justiz. Es analysiert gegenwärtig zusammen mit einer Begleitgruppe Möglichkeiten, die im Evaluationsbericht erwähnten Schwächen des Datenschutzgesetzes zu beheben. Dabei muss es auch die Arbeiten im Europarat und in der EU berücksichtigen.

Diese sind noch im Fluss, was eine abschliessende Analyse verunmöglicht. Die Kommission betont in den Erläuterungen zur Datenschutz-Grundverordnung wie oben erwähnt die Bedeutung der Online-Geschäfte für die Wirtschaft und die Wichtigkeit, Personendaten zu schützen[73]. Der Schutz der Personendaten ist nötig, um das nötige Vertrauen in Online-Geschäfte zu schaffen – das betont auch die BCG-Studie[74]. Zwischen Online-Geschäft und Personendatenschutz bestehen aber auch Zielkonflikte: Die Geschäftsseite möchte möglichst viele Daten erfassen, während aus Sicht des Datenschutzes dem Grundsatz der Datensparsamkeit Nachachtung verschafft werden soll. Wohin sich die Reformarbeiten in diesem Spannungsverhältnis bewegen, ist noch nicht entschieden. Die Vorschläge gehen aber in die Richtung von mehr Prävention, Transparenz und Kontrolle, mit anderen Worten in die Richtung von mehr Konsumentenschutz.

Angesichts der grenzüberschreitenden Datenbearbeitungen wäre eine Harmonisierung der Schweizer und der EU-Lösung sicher sinnvoll. Da der Evaluationsbericht des Bundesrates in die gleiche Richtung zielt, sollte diese keine grösseren Probleme bereiten. Der Gesetzgeber wird sich aber entscheiden müssen, ob er im Datenschutz vorwärtsmachen und die im Evaluationsbericht ausgemachten Lücken möglichst schnell schliessen will, oder ob er der Europakompatibilität mehr Bedeutung beimissen und zunächst einmal abwarten will, was die EU und der Europarat beschliessen.

---

[72] David Rosenthal/Isabelle Jöhri, Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 4 Abs. 5 Rz. 104.

[73] S. oben, Kap. 2.a. am Ende.

[74] S. oben, Kap. 2.b., insb. 2. Absatz.