Zeitschrift für Datenrecht und Informationssicherheit

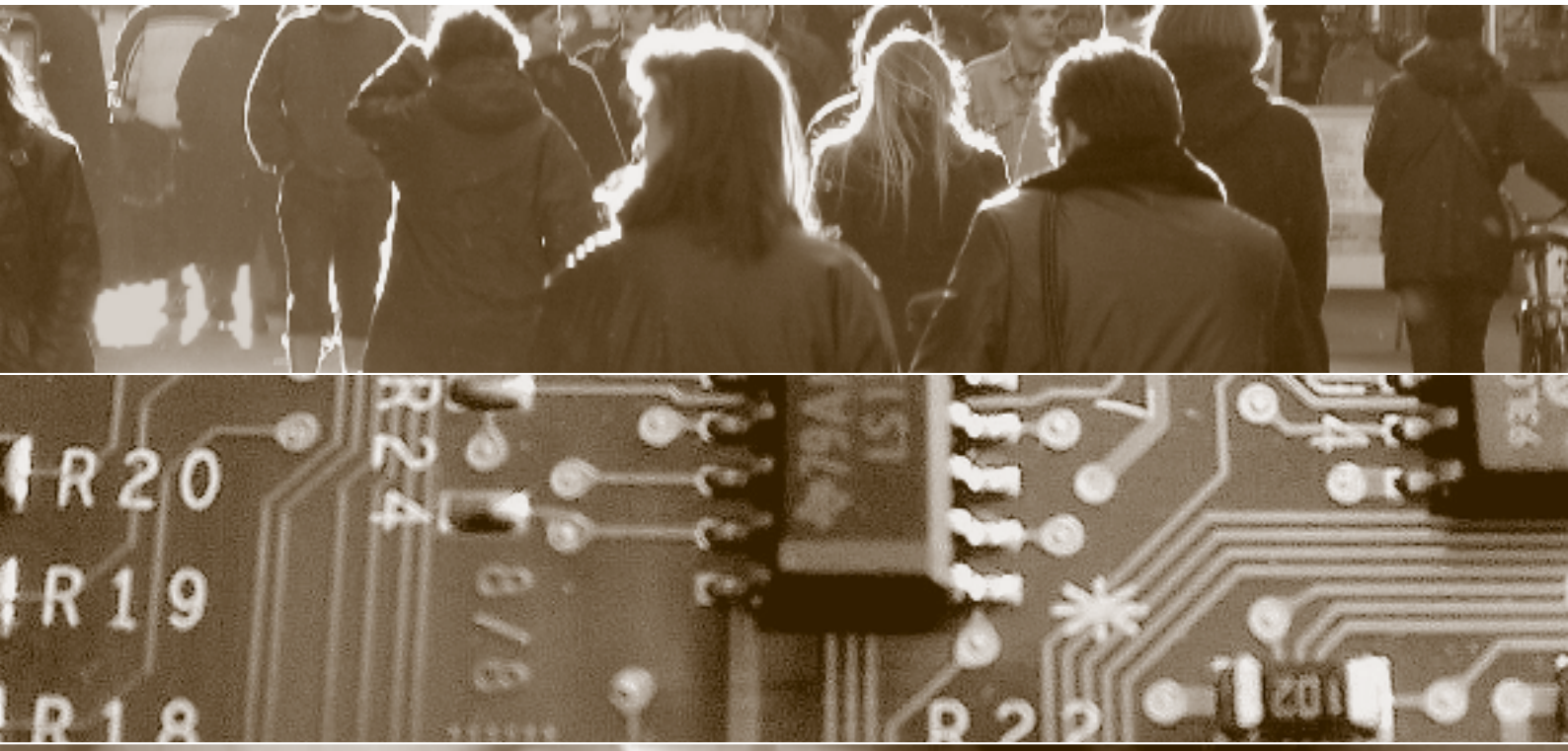
digma

www.digma.info 14. Jahrgang, Heft 3, September 2014

Schwerpunkt:

Internet-Governance

fokus: Zwischen Freiheit und Überwachung
fokus: Schutz vor Überwachung im Internet
report: Öffentlichkeitsprinzip oder Auskunftsrecht?



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

Schulthess §

Die Zeitschrift für kantonale Rechtsprechung

Zeitschrift für
kantonale Rechtsprechung

CAN

- **die wichtigsten kantonalen Entscheide in einer Zeitschrift**
- **macht die Rechtsprechung zur neuen ZPO und StPO bekannt**
- **liefert den Universitäten Grundlagen für Lehre und Forschung**

Erscheinungsweise: 4x jährlich

ISSN: 2235-6460

Jahresabonnement Inland: CHF 198.00

Jahresabonnement Studierende: CHF 98.00

Einzelausgabe: CHF 60.00

Bestellung

www.schulthess.com

☐ Jahresabonnement Inland	CHF 198.00
☐ Jahresabonnement für Studierende	CHF 98.00
☐ Aktuelle Einzelausgabe	CHF 60.00

Name Vorname

Firma

Strasse / Nr.

PLZ / Ort

E-Mail Kundennummer

Datum Unterschrift

CAN – Zeitschrift für kantonale Rechtsprechung macht nach der Vereinheitlichung des Zivilprozess- und Strafprozessrechtes die kantonale Rechtsprechung zugänglich. Gerade weil viele Fragen des Prozessrechts nicht durch das Bundesgericht abschliessend beurteilt werden, kann ein Vergleich mit anderen Kantonen Aufschluss über die Auslegung und Handhabung des prozessualen Rechts geben.

Die Entscheide sind thematisch gegliedert und ermöglichen so einen einfachen Vergleich der Rechtsprechung einzelner Kantone.

Fast zwanzig obere Gerichte aus der Deutschschweiz arbeiten aktiv an der CAN mit. Somit können sich Richter, Anwälte, Studierende und Interessierte aus Politik und Gesellschaft jährlich über die wichtigsten hundert kantonalen Entscheide informieren.

Schulthess Juristische Medien AG
Zwingliplatz 2
Postfach
CH-8022 Zürich
Telefon +41 44 200 29 19
Fax +41 44 200 29 08
zs.verlag@schulthess.com
www.schulthess.com

Schulthess §
Der Verlag zu Recht

Von Government zu Gouvernanz

Philipp Metzger, Direktor, Bundesamt für Kommunikation, Biel
philipp.metzger@bakom.admin.ch

Unsere Daten fliessen über verschiedene Landesgrenzen um die Welt und zurück. Die Spielregeln im globalisierten Netz werden zunehmend von ausländischen Firmen bestimmt. Auch die wichtigsten Teile der Internet-Infrastruktur wie zum Beispiel die Domain-Namen werden von privaten, oftmals kalifornischen Akteuren verwaltet und betrieben. Der Staat stand in dieser weitgehend privatisierten Online-Welt lange abseits. Dies wurde von grossen Teilen der Wirtschaft und der Nutzenden befürwortet. Seitdem das Internet fast in alle Bereiche unseres Lebens vorgedrungen ist und wir auch mit den Risiken konfrontiert werden, wissen aber viele nicht mehr, wem sie vertrauen können. In der Schweiz wie anderswo steigt der Druck auf den Staat. Er soll verlässlichere Regeln einführen und sie auch durchsetzen.

Über die Wünschbarkeit und die Stossrichtung neuer Regeln tauschen sich Behörden mit Wirtschaftsakteuren, Nutzenden und anderen Interessierten aus. Im Rahmen dieses «Multistakeholder»-Dialogs sind die künftigen Rollen der Beteiligten zu klären und zu vereinbaren. Wegen ihrer gesellschaftlichen Verantwortung sind die global tätigen Unternehmen in diesen Dialog einzubinden. Es braucht aber auch eine bewusste Bevölkerung, die ihre Erwartungen gegenüber der Wirtschaft und der Politik formuliert.

Ich bin überzeugt, dass Insellösungen nicht zum Erfolg führen werden. Die künftige Steuerung des weltweiten Netzes – die Internet-Gouvernanz – lässt sich nicht auf nationaler Ebene realisieren, sondern ist zumindest in den Grundsätzen global auszuhandeln. Das BAKOM engagiert sich seit Jahren in verschiedenen internationalen Foren und Konferenzen. So hat es bei der Verwaltung von Internetadressen über die ICANN (Internet Corporation for Assigned Names and Numbers) das Nutzungsrecht an der Internet Domain «.swiss» erworben, um diese im Interesse der Schweiz einzusetzen. Im April 2014 haben wir zudem zusammen mit dem Eidgenössischen Departement für auswärtige Angelegenheiten die *Geneva Internet Platform (GIP)* lanciert. Die GIP vermittelt Informationen und Erfahrungen im Bereich der Internet-Gouvernanz für interessierte Parteien, nicht zuletzt auch aus Entwicklungsländern. Ob online oder offline, ob in Form von Kursen oder über ihre Webseite – die GIP fungiert als neutrales Observatorium und Vermittlerin. Dabei macht sie sich im Interesse ihrer Nutzenden die Diversität und das im internationalen Genf wie kaum anderswo konzentrierte Know-how zunutze.

Ein aktives länderübergreifendes Engagement der im Einbezug aller massgebenden Akteure erfahrenen Schweiz nützt der internationalen Gemeinschaft, aber auch uns selber. Es dient dazu, unsere nationalen Interessen an «vernünftigen» Spielregeln im Internet dort zu beeinflussen, wo diese Regeln gemacht werden – und das ist meistens nicht in Bern oder Biel.

inhalt

fokus

Schwerpunkt:
Internet-Governance

Internet-Governance – ein Überblick

Das Internet hat nicht nur technologische und soziale Veränderungen mit sich gebracht, sondern auch das rechtliche Umfeld vor einen erheblichen Handlungsbedarf gestellt. Der neue Ansatz des «Multistakeholderism» erscheint vielversprechend, doch steht insoweit die verfahrensmässige «Verfestigung» erst am Anfang.

Schutz vor Überwachung im Internet

Die Enthüllungen von Edward Snowden haben zu grosser Verunsicherung geführt. Bürger und Unternehmen sehen sich schutzlos der Massenüberwachung ausgesetzt. Wie können Endanwender und Software-Entwickler die Privatsphäre besser vor Spionage schützen?

Resignation oder Revanche?

Müssen die Enthüllungen von Edward Snowden zu Resignation führen? Oder zu Revanchegedanken? Beides sei nicht anzuraten, meint der Autor. Es bestünden auf unterschiedlichen Ebenen Möglichkeiten, der massenhaften Ausspähung entgegenzutreten, um die Freiheit im Netz zu bewahren und digitale Grundrechte zu sichern.

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. (em.) Dr. iur. Rainer J. Schweizer, Dr. Günter Karjoth

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

Rubrikenredaktorin: Dr. iur. Sandra Husi-Stämpfli

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo: CHF 158.00, 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 19, Fax +41 (0)44 200 29 08, www.schulthess.com, zs.verlag@schulthess.com

Auftragsdaten-bearbeitung – zum Dritten

In der Praxis wird oft übersehen, dass eine Auftragsdatenbearbeitung vorliegt, und oft werden die Verträge deshalb nicht datenschutzkonform ausgearbeitet. Die Autorin richtet den Blick im dritten Teil der Reihe zur Auftragsdatenbearbeitung deshalb auf einige typische Vertragsverhältnisse, die tendenziell oder regelmässig eine Auftragsdatenbearbeitung umfassen.

Öffentlichkeits-prinzip oder Auskunftsrecht?

Das Bundesgericht bejaht wie das Zürcher Verwaltungsgericht die Pflicht, die Namen der an einer Sitzung über eine bestimmte Person sprechenden Sitzungsteilnehmer bekannt zu geben. Allerdings nicht mit korrekter Begründung: Es unterscheidet fälschlicherweise nicht zwischen dem Öffentlichkeitsprinzip und dem Recht auf Zugang zu den eigenen Personendaten.

Im Notfall «eCall» und alles wird gut

In dieser neuen Rubrik soll künftig regelmässig der Blick nach Europa und darüber hinaus gerichtet werden. Wie sind beispielsweise Entwicklungen, die in der EU stattfinden, aus Schweizer Sicht zu beurteilen?

Aus den Datenschutzbehörden

Ein Blick in die Büros der Datenschutzbehörden: Wo wird in einem Gesetz die Videoüberwachung geregelt? Welcher Datenschutzbeauftragte hat ein Merkblatt über die Anonymisierung in Word- und PDF-Dokumenten veröffentlicht?

report

forum

Zwischen Freiheit und Überwachung

Die Entwicklung des Internets als globale Plattform der Informationsgesellschaft braucht Regeln.

Bruno Baeriswyl, Herausgeber bruno.baeriswyl@dsb.zh.ch

Mit technischen Schutzmechanismen und einer aktiven Gestaltung und Steuerung soll das Internet seine prägende Rolle für die Informations- und Kommunikationsgesellschaft sozialverträglich wahrnehmen.

Die Entwicklung des Internets als Rückgrat der Informations- und Kommunikationsgesellschaft ist Traum und Albtraum zugleich. Nie hat man sich träumen lassen, dass diese Infrastruktur in so kurzer Zeit zu einer beherrschenden Technologie wird, die fundamentale Funktionsweisen unserer Gesellschaft so rasch verändert. Aber ebenso wenig hat man sich vorstellen können, dass das Netz der Freiheit dermassen ambivalent ist, dass es in wenigen Jahre auch zum Instrument der – fast – totalen Überwachungsmöglichkeiten mutieren kann.

Die Anfänge des Internets

Die ursprüngliche Kommunikationsinfrastruktur entstand im militärischen Umfeld und hat sich im zivilen Bereich an den Universitäten rasch verbreitet. Zu seiner globalen Bedeutung und zum allgemeinen Durchbruch fand das Internet mit dem «World Wide Web», ein Dienst, der das Abrufen und Verknüpfen von Informationen wesentlich erleichterte. Das Internet wird heute oftmals auch mit dem «World Wide Web» gleichgesetzt, was aber nur einen Teil der tatsächlichen Dienste des Internets umfasst, mithin aber den wichtigsten und den für die Internetnutzenden sichtbarsten Teil.

Die Entwicklung des Internets ist geprägt von US amerikanischen Technologien und Anwendungen. Nicht nur sind die Lieferanten von Hardware zur Vernetzung und Nutzung des Internets amerikanische Unternehmen, sondern auch die heute prägenden Anwendungen wie Suchmaschinen oder soziale Medien werden von diesen beherrscht.

Die gesellschaftlichen Veränderungen

Die rasante technologische Entwicklung prägt unsere Gesellschaft und führt in vielen Bereichen zu sozialen Veränderungen, deren Ausmass nicht abschätzbar ist. Themen, die vermehrt diskutiert werden, sind dabei der «gerechte» Zugang zur Kommunikationsinfrastruktur, die Frage der «Informations»-Macht, die Sicherheit kritischer Infrastrukturen oder der Stellenwert der Grundrechte beim Auf- und Ausbau des Internets und dessen Nutzung. Hierzu gehören auch der Schutz der persönlichen Freiheit und der Privatsphäre sowie die informationelle Selbstbestimmung

Freiheit oder Überwachung?

Die Enthüllungen von Edward Snowden über die Aktivitäten des amerikanischen Geheimdienstes NSA insbesondere auch im und mittels des Internets haben diese Diskussionen in den letzten Monaten neu fokussiert. Das Internet der Freiheit und der «unbegrenzten» Möglichkeiten zeigt sich plötzlich als ein Netz der permanenten und totalen Überwachung. Auch wenn man Spionage als legitimes Abwehrmittel eines Staates anerkennt, zeigt das Ausmass der Aktivitäten des amerikanischen Geheimdienstes und weiterer befreundeter Dienste eine klare Tendenz zur umfassenden Überwachung der Bevölkerung. Da die digitale Welt immer mehr zum Abbild der realen Welt wird, führt die Auswertung dieser Daten zum durchschaubaren und durchschauten Menschen in all seinen Lebensbereichen.

Heute werden die Abhängigkeit von der Technologie diskutiert und die Business-Modelle («Pay as you disclose your data») infrage gestellt. Doch ebenso rasch zeigt sich, dass die Abhängigkeit von der Technologie und die faktische Monopolstellung einiger grosser amerikanischer Unternehmen in diesem Bereich sich nicht so leicht ändern lassen. Zu lange hat man das Internet seiner Freiheit überlassen und beteuert, dass auch für die digitale Welt das gleiche Recht wie für die reale gelte. Doch der globale Aspekt des Internets und seiner Akteure wurde kaum beachtet, wenn auch die Wirkungslosigkeit des Rechts oftmals bedauert wird. In den letzten Jahren haben sich indessen Ansätze auf der Basis einer informellen Regelsetzung herausgebildet. Die Erwartungen an diese sind aufgrund der geschilderten Situation hoch.

Internet-Governance als Herausforderung

Mit dem Ansatz des «Multistakeholderism» ist eine informelle Regelsetzung für das Internet angedacht. Rolf H. Weber (Universität Zürich) gibt einen Überblick über die Entstehung und den aktuellen Stand der Internet-Governance-Aktivitäten (94 ff.). Seit rund zehn Jahren wird auf internationaler Ebene systematischer an einer Internet-Governance gearbeitet (Working Group on Internet Governance, WGIG). Die seit Beginn weg amerikanisch beeinflussten Gremien im Bereich des Internets sind dabei immer mehr internationalisiert worden, und heute spielen weitere Vereinigungen und Expertenforen eine wichtige Rolle in Bezug auf die Internet-Governance. Zentrale Internet-Governance-Themen sind Legitimität, Transparenz, Accountability und partizipative Entscheidungsverfahren. Wie weit dieser «Multistakeholderism» Wirkung zeigen wird, muss sich aber erst noch zeigen.

Der Schutz vor Überwachung

Die Enthüllungen in Bezug auf die Überwachung des Internets lassen ein Warten auf eine sozialverträgliche Regulierung des Internets als unrealistisch erscheinen. Es stellt sich deshalb auch die Frage, wie weit der Schutz des Grundrechts auf Privatsphäre mit den heutigen Mitteln der Technik im Internet gewährleistet werden kann. Hannes Federrath/Karl-Peter Fuchs/Dominik Herrmann (Universität Hamburg) zeigen auf, was die Enthüllungen von Edward Snowden im Einzelnen auf der technischen Ebene offenbart haben (100 ff.). Um einer Massenüberwachung zu entgehen, sind sowohl für Bürgerinnen und Bürger wie auch für Unternehmen technische Möglichkeiten vorhanden, um den Missbrauch von Daten erheblich zu erschweren. Allerdings ist die Schutzwirkung dieser Technologien unterschiedlich. Die Autoren sehen deshalb insbesondere im Einsatz von Open Source Software und deren unabhängiger Auditierung einen entwicklungsfähigen Schutzmechanismus.

Mit den Instrumenten zum Schutz der Privatsphäre im Internet beschäftigt sich auch Helmut Eiermann (Bereichsleiter Technik, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz) (108 ff.). Das Internet wurde zu lange in blauäugiger Unschuld als neutrales Kommunikationsnetz und Netz der Freiheit betrachtet, ohne zu realisieren wie Inhaltsdaten und Metadaten («Verkehrsdaten») von Dienstleistungsanbietern, aber auch – teilweise in Zusammenarbeit – von Geheimdiensten ausgewertet werden. Um die Grundrechte auch im Internet sicherstellen zu können, braucht es deshalb insbesondere die Nutzung von Verschlüsselungstechnologien. Indessen sind auch Schritte auf politischer Ebene notwendig, um die technologische Souveränität zurückzugewinnen. Damit soll eine Diskussion, die nach den Enthüllungen von Edward Snowden zwischen Resignation und Revanche hin und her kippte, auf eine sachliche Ebene geführt werden.

Anerkannte Normen und Regeln durchsetzen

Die Fragen, wie das Internet koordiniert, verwaltet und gestaltet werden soll, haben deshalb an Brisanz enorm zugenommen. Es muss möglich werden, auch in der digitalen Welt Normen und Regeln durchzusetzen, die in der physischen Welt bisher als allgemein anerkannt galten. Sollte dies nicht gelingen, wird die Informations- und Kommunikationsgesellschaft zu einem Abenteuer, das statt Freiheit mehr Abhängigkeit, Manipulation und einen Verlust der Privatheit bringt. Mit einer Stärkung der Internet-Governance kann hier Gegensteuer gegeben werden und können technologische Schutzmechanismen gefördert werden. ■

fokus-Thema dieser Ausgabe:
Internet-Governance

Internet-Governance – ein Überblick

Informelle Regelsetzung und Entscheidungsverfahren mit vielen Akteuren in einem Mehrebenen-System im Vormarsch

Rolf H. Weber, Prof. Dr. iur., Ordinarius für Privat-, Wirtschafts- und Europarecht an der Universität Zürich; Visiting Professor an der Hong Kong University, Hong Kong; Rechtsanwalt, Bratschi Wiederkehr & Buob AG, Zürich rolf.weber@rwi.uzh.ch

Internet-Governance betrifft die Festsetzung von Normen und Regeln in der Online-Welt durch eine Vielzahl von Akteuren in unterschiedlichen Rollen.

Der aus der englischen Sprache entlehnte Begriff der «Governance» geht auf das griechische Verb *«kubernáo»* steuern, lenken) und das lateinische Wort *«Gubernator»* zurück; «Governance» meint somit alle Aspekte von steuerndem und leitendem Verhalten[1].

Im Internet erfolgt die Governance nicht hierarchisch. Die Vielzahl der Akteure, die mitwirken wollen und auch sollen, macht indessen die Einrichtung neuer Handlungsformen unumgänglich; deren Möglichkeiten und Wirkungen verursachen indessen verschiedene Herausforderungen, die einer genaueren Betrachtung bedürfen.

Begriff und Bedeutung von Internet-Governance

Im Kontext des Internets hat sich die auf Empfehlung des ersten Weltgipfels für die Informationsgesellschaft (Genf, 2003) ins Leben gerufene Working Group on Internet Governance (WGIG) in ihrem Bericht von 2004 darauf geeinigt, Internet-Governance zu definieren als die «Entwicklung und Anwendung durch Regierungen, den Privatsektor, die akademische/technische Gemeinschaft und die Zivilgesellschaft, in ihren jeweiligen Rollen, von gemeinsamen Prinzipien, Normen, Regeln, Vorgehensweisen zur Entscheidungsfindung und Programmen, welche die Weiterentwicklung und die Nutzung des Internets beeinflussen»[2]. In der Lehre wird der Begriff auch umschrieben als fortlaufende Auseinandersetzungen und Beratungen darüber, wie das Internet koordiniert, verwaltet und geformt werden soll[3]. In Weiterführung dieses Gedankens erfasst Internet-Governance alle Mechanismen, Institutionen und Prozesse, die das Tun und Handeln im Internet organisieren und regulieren.

Die technische Struktur des Internets basiert auf einer Kombination von zwei paketvermittelnden Protokollen zur Informationsübertragung, dem Transmission Control Protocol (TCP) und dem Internet Protocol (IP). Unter Verwendung eindeutiger Sender- und Empfängeradressen (sog. IP-Adressen) identifizieren und übermitteln beteiligte Computer die Informationspakete in Bitfolgen (Zahlenfolgen), nicht in Buchstaben. Die numerischen Adressen sind indessen ab 1984 in für den Nutzer leichter zu merkende Worte (Domainnamen) umgewandelt worden, deren Verwaltung durch das Domain Name System (DNS) erfolgt. Domainnamen setzen sich aus mehreren, durch Punkte voneinander getrennten Namen zusammen, die ihrer (nach rechts hierarchisch aufsteigenden) Reihenfolge nach Top-Level-Domains (TLD), Second-Level-Domains, Third-Level-Domains, usw. heissen. Bei den Top-Level-Domains wird unterschieden zwischen den länderspezifischen Domains (country code Top-Level-Domain, ccTLD) und den allgemeinen (generischen) Top-Level-Domains (gTLD). Die ursprünglich sieben gTLD haben mehrfach eine Erweiterung erfahren, im neuesten grossen Verteilungsverfahren von gTLD auch mit der Möglichkeit der Wahl von z.B. Marken-, Städte-, Branchen- und Berufsnamen. Zudem sind seit 2010 Internationalized Domain Names (nicht englische Alphabete) verfügbar[4].

Organisation im Internet-Bereich

Angesichts der Entwicklung des Internets in den Vereinigten Staaten erstaunt es nicht, dass dessen technische und rechtliche Ausgestaltung durch US-Organisationen erfolgte. Nachdem ursprünglich militärische Stellen (ARPANET) und hernach Universitäten für die technischen Protokolle und das Domain Name System zuständig waren, wird das DNS seit 1998 durch die der Aufsicht des US-amerikanischen Handelsministeriums unterstehende Internet Corporation for Assigned Names and

Numbers (ICANN) verwaltet. Neben der ICANN sind aber noch weitere Organisationen von Bedeutung.

ISOC-Gruppe

Im Zuge der Entwicklung des auf Selbstregulierung basierenden Internets wurde 1992 die Internet Society (ISOC) gegründet. Zweck der ursprünglich durch eine relativ geringe Anzahl von Technikern, Providern und Internet-Nutzern ins Leben gerufenen gemeinnützigen Organisation ist das Vorantreiben der Entwicklung des Internets, seiner Anwendungsmöglichkeiten und der mit dem Internet verbundenen Technologien. Die ISOC ist eine auf Mitgliedschaft basierende, nicht staatliche Gesellschaft von Einzelpersonen und Organisationen, die sich mit ihren derzeit mehr als 55 000 Mitgliedern (davon mehr als 130 Organisationen) für ein allen zugängliches, transparentes Internet einsetzt[5].

Organisatorisch hat die ISOC die Funktion der Muttergesellschaft für das Internet Architecture Board (IAB) und die Internet Engineering Task Force (IETF), eine offene, nicht eingetragene Gemeinschaft von Netzwerkdesignern und Forschern, die sich mit der Entwicklung und Umsetzung einheitlicher Internet-Infrastruktur Standards befasst. Die IETF als Expertenorganisation ist deshalb von grosser praktischer Bedeutung, weil die vereinbarten Standards die letztlich im Alltagsleben massgebliche Infrastruktur festlegen. Die Entscheide kommen im IETF durch Konsens zustande.

Die Haupttätigkeit der ISOC liegt in der Beteiligung an Diskussionen um die öffentliche Ordnung im Internet, sie stellt eine allen Interessengruppen offenstehende Diskussionsplattform für den «Internet-Governance-Prozess» dar. Das jüngste Thema der ISOC ist eine breit angelegte Untersuchung zu den verschiedenen Formen des «Multistakeholderism» im Internet.

ICANN

Die Internet Corporation for Assigned Names and Numbers (ICANN) ist ein nach kalifornischem Recht gegründetes Unternehmen ohne Gewinnabsicht mit Sitz in Marina del Rey, deren Zweck in der Förderung der Sicherheit, Stabilität und Interoperabilität des Internets besteht. In den letzten Jahren hat die ICANN auch Zweigniederlassungen in Istanbul und Singapur eröffnet. Die technische Verwaltung der gTLD liegt in den Händen der Internet Assigned Numbers Authority (IANA), die wiederum die Verwaltung und Zuteilung der Ressourcen weitestgehend auf die fünf gemeinnützigen regionalen Internet-Adressregister (Regional Internet Registries, RIR) übertragen hat; für Europa ist die RIPE-NCC mit Sitz in Amsterdam zuständig. In der Schweiz liegt die Kompetenz beim Bundesamt für Kommunikation (BAKOM), das bisher die konkrete Aufgabe der Verteilung von Internet Adressen an die Stiftung Switch delegiert hat; im Zusammenhang mit den neuen Domainnamen (v.a. «.swiss») ist indessen eine Anpassung der Verordnungsgrundlagen mit einer stärkeren Kompetenzattraktion beim BAKOM im Gange (Verordnung über die Internet-Domains).

Die USA haben sich seit der Gründung der ICANN vertraglich einen gewissen Einfluss auf die Organisation für die Internetadressen und das Domainnamen-System vorbehalten. Das ursprünglich zwischen der ICANN und der National Telecommunications and Information Administration, einer Behörde des amerikanischen Handelsministeriums, abgeschlossene Übereinkommen (Memorandum of Understanding) ist im Jahre 2006 durch ein Joint Project Agreement (JPA) und schliesslich im Jahre 2009 durch eine Erklärung verbindlicher Vereinbarungen (Affirmation of Commitments, AoC) ersetzt worden. Die vertraglich den USA eingeräumten Rechte wurden über die Jahre hinweg immer einschränkender formuliert, was nicht zuletzt auf die Kritik anderer Länder an der Vorrangstellung der USA zurückzuführen ist. Trotz der Einschränkung der Kontrollrechte sind die USA aber nach wie vor in der Lage,

Die USA haben sich seit der Gründung der ICANN vertraglich einen gewissen Einfluss auf die Organisation für die Internetadressen und das Domainnamen-System vorbehalten.

Kurz&bündig

Das Internet hat nicht nur grosse technologische und soziale Veränderungen während der letzten zwanzig Jahre mit sich gebracht, sondern auch das rechtliche Umfeld vor einen erheblichen Handlungsbedarf gestellt. Traditionelle Instrumente der Normsetzung wie internationale Verträge und nationale Gesetze bedürfen der wesentlichen Ergänzung durch die informelle Rechtssetzung, oft in Form von Selbstregulierungen. Eine solche Regelbildung hat sich aber den klassischen Anforderungen wie Legitimität, Transparenz, Accountability und Mitwirkung in den Entscheidungsverfahren zu stellen. Der neue Ansatz des «Multistakeholderism» erscheint vielversprechend, doch steht insoweit die verfahrensmässige «Verfestigung» erst am Anfang. Die bisherigen Erfahrungen lassen eine positive Einschätzung von Möglichkeiten und Wirkungen zu; prozedurale «Verfeinerungen» erweisen sich indessen noch als unabdingbar und stellen eine zentrale Aufgabe für die nächsten Jahre dar.

gewisse Entscheidungsprozesse zu steuern, insbesondere im Kontext der Kontrolle über den einflussreichen Root-Server A und die wichtigsten gTLD, weil das amerikanische Unternehmen VeriSign Inc., gestützt auf einen mit dem amerikanischen Handelsministerium abgeschlossenen Vertrag, die beiden gTLD «com» und «net» verwaltet. Immerhin lässt sich nicht übersehen, dass die US-Regierung die vorhandenen Vorrechte in der Praxis kaum je ausgeübt hat[6].

Oberstes Geschäftsführungs- und Vertretungsorgan der ICANN ist ein aus 21 Direktoren bestehender Verwaltungsrat, dessen Mitglieder (15 stimmberechtigte und 6 nicht stimmberechtigte Direktoren) von verschiedenen Gremien gewählt bzw. nominiert werden. Zur Gewährleistung einer ausgeglichenen globalen Repräsentation verfügt keine der fünf Weltregionen über eine einfache Mehrheit (d.h. mehr als 5 Direktoren) im Verwaltungsrat. Die Wahl von Mitgliedern nationaler Regierungen und zwischenstaatlicher Organisationen ist untersagt, um den Status von ICANN als private Selbstverwaltungsorganisation sicherzustellen. Beratende Unterstützung findet der Verwaltungsrat von den sog. ICANN Supporting Organizations[7].

Um der amerikanischen Dominanz im Bereich der Internet-Governance entgegen zu wirken, wurde die Durchführung eines unter UNO-Schirmherrschaft stehenden Weltgipfels zur Informationsgesellschaft beantragt.

Neben dem Nominating Committee, das sich aus siebzehn stimmberechtigten Mitgliedern zusammensetzt und dazu beitragen soll, dass eine vielfältige Vertretung im ICANN-Verwaltungsrat zustande kommt, hat insbesondere das Governmental Advisory Committee (GAC) in den letzten Jahren an Bedeutung gewonnen. Im GAC sitzen Vertreter von Regierungen, die zwar gegenüber der ICANN lediglich beratende Funktion haben, deren Stellungnahmen jedoch in der Praxis durchaus Beachtung finden.

Internet-Governance-Forum

Um der amerikanischen Dominanz im Bereich der Internet-Governance entgegenzuwirken, hat die Internationale Fernmeldeunion (ITU) die Durchführung eines unter der Schirmherrschaft der Vereinten Nationen stehenden Weltgipfels zur Informationsgesellschaft (World Summit on the Information Society, WSIS) beantragt; dieser Weltgipfel hat in zwei Phasen (2003 in Genf und 2005 in Tunis) stattgefunden. Die Genfer Prinzipien-Erklärung (Geneva Declaration of Principles), der Genfer Aktionsplan (Geneva Plan of Action), die Tunis-Verpflichtung (Tunis Commitment) und die Tunis-Agenda für die Informationsgesellschaft (Tunis Agenda for the Information Society) enthalten zwar keine Einigung über die konkrete Ausgestaltung der Verwaltung des Internets und schlagen keine Veränderung der durch die ICANN dominierten Organisationsstruktur vor, sie enthalten aber die Verpflichtung der Staaten, zu einer breiteren Abstützung der Internet-Governance-Diskussion beizutragen. Um eine Diskussionsplattform für allgemein-politische Aspekte rund um das Internet zu schaffen, hat der Weltgipfel in Tunis insbesondere die Einrichtung des Internet-Governance-Forums (IGF) beschlossen. Seit dem Jahre 2006 (Athen) findet jährlich eine viertägige IGF-Konferenz statt, die es allen Interessierten ermöglicht, sich an Diskussionen zu Schwerpunktthemen zu beteiligen. Inhaltlich geht es etwa um die Offenheit des Internets im Sinne freier Meinungsäusserung, um die Sicherheit im Internet, um den Zugang zum Internet oder um die Anerkennung verschiedener Internetkulturen[8].

Das IGF folgt somit dem sog. Multistakeholder-Ansatz, der die Idee verwirklichen soll, dass die mannigfaltigen Interessen der unterschiedlichen Internet-Nutzer sachgerecht zum Ausdruck gebracht werden können. In den letzten Jahren hat sich denn auch die Beteiligung der verschiedenen Interessengruppen, insbesondere aus Entwicklungsländern, am IGF verbessert. Über die Fortführung des IGF nach Ablauf der (ersten) zehnjährigen Periode soll im Herbst 2014 von der Generalversammlung der Vereinten Nationen befunden werden.

EuroDIG

Im Zuge des seitens vieler IGF-Teilnehmer zum Ausdruck gebrachten Interesses an der Fortsetzung der Dialoge auch auf regionaler und nationaler Ebene gründeten Interessenvertreter einiger europäischer Länder im Jahre 2008 den Euopean Dialogue on Internet Governance (EuroDIG). Mit der Einberufung dieses Forums zielten die Gründer auf die Schaffung einer Plattform, die das Bewusstsein der Europäer für die Bedeutung der Internet-Governance wecken und darüber hinaus den europäischen Interessenvertretern die Möglichkeit geben sollte, sich vor dem jeweils nächsten IGF über geplante Aktivitäten auszutauschen und sich so besser zu koordinieren. Seit der Gründungskonferenz von 2008 in Strassburg findet das

EuroDIG an jährlich wechselnden Austragungsorten statt[9].

Viele Länder kennen zudem ein nationales Internet-Governance-Forum. In der Schweiz haben interessierte Kreise im Frühjahr 2013 das Swiss IGF ins Leben gerufen[10]; zudem ist unter Mitwirkung der Schweizer Regierung kürzlich die nachfolgend noch zu erläuternde Geneva Internet Platform, die als internationales Diskussions- und Expertenforum fungieren soll, eingerichtet worden[11].

Zentrale Themen der Internet-Governance

Materielle Diskussionen zur Internet-Governance betreffen insbesondere Aspekte der Legitimität, Transparenz, Accountability und Mitwirkung der Öffentlichkeit in den für die Internet-Organisation zuständigen «Einheiten».

Legitimität

Im Hinblick auf die globale, gesellschaftliche, wirtschaftliche und politische Relevanz des Internets nimmt die Legitimität im Kontext der Internet-Governance eine wichtige Rolle ein. Legitimität definiert sich als der Glaube an bzw. das Vertrauen auf die Rechtmässigkeit politischer Herrschaft. Durch die Begründung einer Ermächtigung zur Festlegung von Regeln soll den Normadressaten das Gefühl vermittelt werden, ihre Interessen würden in die Entscheidungsprozesse einfliessen. Traditionell wird Legitimität mit dem Staat verknüpft; im Internet-Bereich liegen aber viele Entscheidungskompetenzen bei privaten Organisationen (ICANN, IETF), die nicht auf einer zweifelsfrei demokratischen Grundlage agieren.

Angesichts der starken Rolle der USA innerhalb der Organisation ICANN und der Tatsache, dass eine private Gesellschaft wie ICANN mit der Ausübung der bedeutenden Aufsichtsfunktion über das Domain Name System jedenfalls theoretisch über eine weite Entscheidungsmacht verfügt, stellen sich Fragen nach der demokratischen Legitimation von ICANN. Diese Kritik hat ICANN aufgenommen und verschiedene Reformen eingeleitet, insbesondere zur Berücksichtigung von Interessen anderer Stakeholder (Regierungen, Zivilgesellschaft). Anlässlich der NetMundial-Konferenz in São Paulo (April 2014) haben Regierungen, Internet-Organisationen und Zivilgesellschaft erstmals bei der Vorbereitung der Abschluss-Erklärung intensiv zusammengewirkt.

Die Einführung und Umsetzung des Multistakeholder-Ansatzes geht im Bereich der Internet-Governance zur Einbeziehung der gesamten Gesellschaft über den Umfang traditioneller Regulierungstheorien hinaus, welche im Allgemeinen dem Ansatz der strikten Trennung von Staat (öffentliches Recht) und Gesellschaft (Zivilrecht) folgen. Diese Entwicklung hinterfragt somit das traditionelle rechtliche und politische Verständnis und bezweckt die Analyse verschiedener Problembereiche mit Blick darauf, ob die zur Bewertung der Legitimität von Staaten angesetzten Kriterien auch auf Internet-Organisationen Anwendung finden können und wer als legitimer Interessenvertreter anzusehen ist[12].

Transparenz

Der Begriff «Transparenz» umfasst dem allgemeinen Verständnis nach Aspekte wie Klarheit, Verantwortung, Genauigkeit, Zugänglichkeit und Wahrhaftigkeit und lässt sich in die materielle, prozessuale und entscheidungsfindungsbezogene Transparenz unterteilen. Die Verständlichkeit und Nachvollziehbarkeit politischer Massnahmen verlangt z.B. offene Verfahren und begründete Entscheide.

Im Bereich der Internet-Governance ist Transparenz als Regelungsziel und als Eigenschaft des Regelungssystems selbst von Belang. Darüber hinaus ergibt sich die Notwendigkeit der Einhaltung von Transparenz auch im Sinne der Nachvollziehbarkeit von Vorgängen aus seiner Bedeutung für die Schaffung anderer wichtiger Regulierungsgrundsätze wie etwa denjenigen der Unabhängigkeit und der Accountability von Regulierungsbehörden.

Im Internet-Bereich liegen aber viele Entscheidungskompetenzen bei privaten Organisationen, die nicht auf einer zweifelsfrei demokratischen Grundlage agieren.

In den letzten Jahren hat die ICANN eine Reihe von Transparenzbestimmungen in ihre Organisationsdokumentente aufgenommen: So ist die ICANN verpflichtet, jede Handlung und Entscheidung durch transparente Mechanismen nachvollziehbar zu machen, um allen betroffenen Einheiten die Teilnahme an den politischen Entwicklungsprozessen zu ermöglichen. ICANN hat das Potenzial und die möglichen Dimensionen der Offenheit erkannt und arbeitet weiter an der Verbesserung der Transparenz-Bestimmungen[13].

Accountability

Neben der Transparenz ist die damit eng verknüpfte Accountability (ein die Rechenschaftspflicht und die Verantwortlichkeit um-

fassender Begriff) von Bedeutung; materiell geht es um die Anerkennung von und das Einstehenmüssen für Handlungen und Entscheidungen im Rahmen der festgelegten Verfahren. Die Accountability deckt im internationalen Kontext politische, philosophische und

Die öffentliche Kontrolle der Internet-Organisationen durch die Zivilgesellschaft ist ein unverzichtbares Instrument.

rechtliche Elemente ab; die Entscheidungsträger haben ihre Handlungen und Vorkehren zu erklären bzw. zu rechtfertigen sowie für etwaige Schadensverursachungen aufzukommen[14].

Im Kontext der Internet-Organisationen wird seit Jahren für die Verbesserung der Accountability von handelnden Entscheidungsträgern plädiert. Seit dem Abschluss der Affirmation of Commitments (2009) gehört die Verbesserung der Accountability auch zum «Regulierungsprogramm» der ICANN. Ein Expertenteam hat in einem Bericht bereits Schwachstellen identifiziert und ICANN aufgefordert, Massnahmen zu treffen. Zum Teil ist dies zwischenzeitlich geschehen; in einem zweiten Bericht weist das Expertenteam aber auf nicht erfüllte Forderungen und neue offene Anliegen hin[15]. Mit weiteren positiven Entwicklungen im Bereich der Accountability ist deshalb zu rechnen.

Fussnoten

1 Dieser Text beruht auf der ausführlicheren Publikation von Rolf H. Weber, Internet Governance in: Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht, Loseblatt, München 2014 (Lieferung September 2014).
2 Report of the Working Group on Internet Governance (WGIG), Juni 2005, <http://www.wgig.org./docs/WGIGREPORT.pdf>.
3 Milton Mueller, Networks and States: The Global Politics of Internet Governance, Cambridge MA 2010, 9.
4 Weber (Fn. 1), N 8 ff.
5 Vgl. <http://www.internetsociety.org/who-we-are/mission>.
6 Vgl. Weber (Fn. 1), N 30 ff.
7 Weber (Fn. 1), N 36 ff.
8 Weber (Fn. 1), N 41 ff.
9 Weber (Fn. 1), N 45 ff.
10 Vgl. <http://swiss-igf.ch>.
11 Vgl. <http://www.diplomacy.edu/capacity/GIP>.
12 Im Einzelnen zur Legitimität vgl. Rolf H. Weber, Shaping Internet Governance: Regulatory Challenges, Zürich 2009, 105 ff.
13 Im Einzelnen zur Transparenz vgl. Weber (Fn. 12), 121 ff.
14 Im Einzelnen zur Accountability vgl. Weber (Fn. 12), 132 ff.
15 Zu den Berichten des Accountability and Transparency Review Team 1 und 2 (ATRT) vgl. <https://www.icann.org/en/about/aoc-review/atrt>.
16 Im Einzelnen zur Mitwirkung vgl. Weber (Fn. 12), 148 ff.
17 Zum Multistakeholder-Konzept vgl. verschiedene Aufsätze im Sammelband von Roxana Radu/Jean-marie Chenou/Rolf H. Weber (eds.), The Evolution of Global Internet Governance, Principles and Policies in the Making, Zürich 2013.
18 Einen wissenschaftlichen Beitrag zur Diskussion leisten soll das derzeit laufende Projekt zu den Multistakeholder-Strukturen der ISOC.

Mitwirkung

Angesichts der privaten und geschäftlichen Bedeutung des Internets spielt die Beteiligung seiner Nutzer an Entscheidungsprozessen eine zentrale Rolle. Die öffentliche Kontrolle der Internet-Organisationen durch die Zivilgesellschaft ist ein unverzichtbares Instrument, welches in Kombination mit geeigneten Organisationsmechanismen eine publikumsbezogene Intervention in Entscheidungsprozesse ermöglichen soll. Die Einbeziehung aller interessierten Internet-Nutzer macht solche Prozesse nachvollziehbar und unterstützt das Vertrauen in die getroffenen Entscheidungen[16].

In den letzten Jahren hat sich für ein solches umfassendes Mitwirkungskonzept der Begriff «Multistakeholderism» durchgesetzt[17]. Inhaltlich geht das Multistakeholder-Konzept auf die eingangs erwähnte Umschreibung der Internet-Governance durch den WGIG-Bericht zurück. Entscheidend ist dabei die Frage, welche Rolle die einzelnen Stakeholder zu übernehmen haben. Insoweit besteht Gesprächsbedarf, weil die derzeitigen Internet-Regulierungen auf einem verworrenen Konzept von überstaatlichen, nationalen, verbandsmässigen und privaten Regeln bestehen. Abgesehen davon, dass in einem solchen Geflecht die Strukturen der Hierarchie und der Polyarchie vorkommen, erweist sich insbesondere die Festlegung der Akteure als nicht unproblematisch: Neben den Regierungen der Staaten, den Vertretern internationaler Organisationen und den Repräsentanten der Geschäftswelt setzt sich die Zivilgesellschaft aus einer fast unüberschaubaren Zahl von Einzelpersonen zusammen, die zum Teil überhaupt nicht deckungsgleiche Interessen haben.

Die Verwirklichung des Multistakeholder-Konzepts ist somit ein Lernprozess, der noch einige Zeit andauern dürfte. Immerhin haben die Erfahrungen anlässlich der NetMundial-Konferenz in São Paulo (Ende April 2014) gezeigt, dass die Realisierung solcher Strukturen nicht ausgeschlossen ist. Jedenfalls haben sich die Diskussionen als fruchtbarer erwiesen als die Verhandlungen der Staaten anlässlich der World Conference on International Telecommunications 2012 in Dubai. Regierungsvertreter haben anerkannt, dass nicht allein hinter verschlossenen Türen verhandelt werden darf; dies hat nicht zuletzt das Scheitern des Anti-Counterfeating Trade Agreement (ACTA) infolge der Demonstrationen auf der Strasse gezeigt. Erfolgversprechender ist vielmehr, die Vertreter der Zivilgesellschaft auch zu Wort kommen zu lassen und eine Mitwirkung aller am Internet interessierten Nutzer anzustreben[18].

Neueste Entwicklungen

Die Erfahrungen der letzten zwanzig Jahre haben gezeigt, dass sich die Internet-Governance nicht allein auf multilaterale Verträge und Konventionen (sog. «hard law») abstützen lässt. Selbst wenn dem Konzept des sog. «soft law» ein gesicherter rechtlicher Status fehlt und allgemein anwendbare Verfahrensprinzipien noch nicht entwickelt worden sind, erfordern die komplexen Vorgänge im Internet-Kontext neue Formen von Rechtsetzungsverfahren und rechtlichen Gestaltungen. Die «informelle» Rechtsetzung mit vielen Akteuren in einem Mehrebenen-System unter Einschluss aller interessierter Internet-Nutzer («Multistakeholderism») verspricht langfristig mehr Erfolg.

Die Schweiz hat sich seit über zehn Jahren aktiv in die Diskussionen um die Internet-Governance eingebracht. Vorerst fand der erste Teil des Weltinformationsgipfels Ende 2003 in Genf statt; hernach war die Schweiz prominent tätig bei der Verabschiedung der Tunis-Agenda und hat sich auch im Rahmen des Europarates immer wieder für die Verbesserung der Verfahren zur Entstehung von Internet-Regulierungen eingesetzt, etwa als «Mitgründerin» des EuroDIG.

Weil Genf ein wichtiger Standort von UNO-Organisationen ist und weil die Schweiz nicht zuletzt wegen des dortigen Domizils der Internationalen Fernmeldeunion einen substanziellen Beitrag auch zu Fragen der Internet-Governance leisten könnte, ist vor wenigen Monaten die Geneva Internet Platform ins Leben gerufen worden, welche die Funktion ausüben soll, als Forum zum Diskussions- und Meinungsaustausch zu dienen. Die ersten Aktivitäten haben bereits viele Interessenten auf die neue Plattform aufmerksam gemacht, die langfristige Bewährungsprobe steht aber noch aus. Wie auch immer die weitere Entwicklung der verschiedenen Initiativen zu Verbesserung des Multistakeholder-Konzepts verläuft, ist offensichtlich, dass die Möglichkeiten und neuen Handlungsformen zentrale Elemente der künftigen Internet-Governance sein werden. ■

Regierungsvertreter haben anerkannt, dass nicht allein hinter verschlossenen Türen verhandelt werden darf.

Schutz vor Überwachung im Internet

Wie können Endanwender und Software-Entwickler die Privatsphäre besser vor Spionage schützen?

Hannes Federrath, Prof. Dr.-Ing., Fachbereich Informatik, Universität Hamburg, Hamburg, Deutschland federrath@informatik.uni-hamburg.de

Karl-Peter Fuchs, M.A., Fachbereich Informatik, Universität Hamburg, Hamburg, Deutschland fuchs@informatik.uni-hamburg.de

Selbstschutzwerkzeuge wie Verschlüsselungs- und Anonymisierungsprogramme können die Kommunikation wirkungsvoll vor Überwachung schützen.

Seit Juni 2013 veröffentlichen führende Medien fast wöchentlich neue Geheimdokumente, die plastisch aufzeigen, mit welchen Methoden die Nachrichtendienste NSA, GCHQ und BND im Internet spionieren. Schon viele Jahre zuvor hatten Experten davor gewarnt, dass «die Dienste» unkontrolliert alle Aktivitäten im Internet überwachen. Snowdens Enthüllungen sind also im Grunde nichts Neues. Trotzdem sind sie von unschätzbarem Wert, da die abstrakte Gefahr erst durch die vielen Details begreifbar geworden ist.

Wir wissen nun, dass sich die Dienste im Laufe der Jahre ein umfangreiches technisches Repertoire erarbeitet haben, das eine weitgehende Überwachung aller Internetnutzer erlaubt: Erstens können sie auf alle Daten, die bei Internet-Anbietern wie Facebook, Google und Dropbox hinterlegt sind, zugreifen[1]. Zweitens haben die Nachrichtendienste zentrale Knotenpunkte der Internet-Infrastruktur infiltriert, um den Datenverkehr für Wochen bzw. Monate, vielleicht auch für Jahre, zu speichern und auszuwerten[2]. Drittens ist bekannt, dass einige Nachrichtendienste Hardware, Software und sogar kryptografische Verfahren, die von Benutzern und Internet-Anbietern eingesetzt werden, unbemerkt mit Schwachstellen und Hintertüren versehen haben, um eine spätere Überwachung zu erleichtern[3].

Angesichts dieser umfangreichen Fähigkeiten stellen sich die folgenden Fragen: Kann man sich vor der Überwachung durch Nachrichtendienste überhaupt noch zuverlässig schützen? Sind die heute verfügbaren Schutzwerkzeuge noch sicher? Was ist von hastig gestarteten Initiativen, etwa der «E-Mail made in Germany» und dem «Schengen-Routing» sowie den zahlreichen «sicheren» Cloud-Diensten zu halten?

Während perfekter Schutz vor Nachrichtendiensten kaum möglich ist, lässt sich durch den Einsatz bereits heute verfügbarer Schutzwerkzeuge der Aufwand zur Überwachung so stark erhöhen, dass eine verdachtsunabhängige Massenüberwachung weitgehend ausgeschlossen werden kann.

Wir möchten einen Beitrag zur Versachlichung der Debatte leisten. Dazu setzen wir uns im Folgenden mit dem Repertoire der Nachrichtendienste auseinander, hinterfragen den Nutzen der angesprochenen Initiativen und diskutieren die Wirksamkeit verschiedener Schutzmechanismen.

Zugriff auf Daten beim Anbieter

Zunächst betrachten wir die Möglichkeit der Überwachung durch den Zugriff auf die Daten, die bei Online-Anbietern hinterlegt sind. Während persönliche Daten früher nur auf den von aussen schwer erreichbaren Endgeräten abgespeichert wurden, sind sie heute wesentlich leichter zugänglich, da sie häufig «in der Cloud» liegen. Die Online-Anbieter unterliegen teilweise rechtlichen Auflagen, die sie dazu verpflichten, Nachrichtendiensten und anderen Ermittlungsbehörden Zugriff auf ihren Datenbestand zu gewähren. In den Vereinigten Staaten kommt hierfür z.B. ein sog. «National Security Letter»[4] zum Einsatz. Dem Dienstanbieter wird dabei üblicherweise untersagt, die von der Überwachung betroffenen Kunden zu informieren. Öffentlich gemacht wurde dieses Vorgehen insbesondere durch den Anbieter Lavabit, dessen Gründer sich nach Vorlage einer entsprechenden Überwachungsanordnung nur durch die Einstellung des Betriebs zu helfen wusste[5].

Bei den meisten Internet-Angeboten sind die auf den Servern hinterlegten Nutzerdaten dem Zugriff durch Nachrichtendienste schutzlos ausgeliefert – auch wenn die Anbieter mit Verschlüsselungstechniken werben. Häufig wird lediglich ein Verfahren zur Verbindungs-

verschlüsselung eingesetzt (zum Beispiel HTTPS). Dabei werden die Daten ausschliesslich auf dem Kommunikationsweg zwischen Nutzer und Anbieter verschlüsselt übertragen. Der Anbieter entschlüsselt die Daten, bevor er sie weiterverarbeitet. Wie der Lavabit-Fall zeigt, ist es unerheblich, ob ein Anbieter die Daten in seinem System verschlüsselt abspeichert, da er dazu verpflichtet werden kann, die Daten zu entschlüsseln. Bei den populären (meist amerikanischen) Diensten Facebook, Dropbox, Google Drive, Apple iCloud, WhatsApp und Skype muss man also davon ausgehen, dass Nachrichtendienste mitlesen.

Um der Überwachung zu entgehen, müssen die Benutzer sicherstellen, dass ausser ihnen selbst niemand ihre Daten entschlüsseln kann – auch nicht der Dienstanbieter. Dies gelingt nur, wenn die Benutzer die Verschlüsselung selbst in die Hand nehmen. Die Daten müssen dazu noch im Vertrauensbereich des Nutzers (z.B. auf seinem Endgerät) mit einem anerkannten Kryptoverfahren verschlüsselt werden. Darüber hinaus muss gewährleistet sein, dass der verwendete kryptografische Schlüssel den Vertrauensbereich nicht verlässt.

Experten bevorzugen hier altbekannte Programme, die sich über viele Jahre bewährt haben. So können Dateien etwa mit dem seit 2004 verfügbaren TrueCrypt verschlüsselt werden, bevor sie in der Cloud abgelegt werden. Die Weiterentwicklung von TrueCrypt[6] wurde im Juni 2014 allerdings vorläufig eingestellt. Als Ersatz bietet sich die relativ neue Software «BoxCryptor»[7] an. Zur Absicherung von Voice-over-IP-Telefonaten wird die von Phil Zimmermann entwickelte Software «zfone»[8] empfohlen. Zur Verschlüsselung von Echtzeit-Chats kann das von vielen Instant-Messenger-Programmen unterstützte Protokoll «Off-the-Record» bzw. OTR[9] verwendet werden. Zur Absicherung der auf Smartphones üblicherweise eingesetzten asynchronen Kommunikation (wie von WhatsApp und Apple iMessage bekannt) ist OTR aus technischen Gründen allerdings weniger geeignet. Neben dem vor allem in Europa populären kommerziellen Angebot «Threema»[10] gibt es für diesen Anwendungsfall inzwischen auch einige kostenlose und quelloffene Alternativen, etwa «Telegram»[11] und «TextSecure»[12]. Die Sicherheit dieser Dienste kann allerdings momentan noch nicht abschliessend beurteilt werden.

Schutz vor Überwachung durch den Einsatz von Verschlüsselung ist jedoch nur bei Diensten möglich, bei denen der Anbieter die Klartextdaten zur Diensterbringung nicht benötigt. Manche Online-Angebote entfalten ihren Nutzen allerdings nur dann, wenn der Dienstanbieter mit den Daten «arbeiten» kann. Die derzeit existierenden Verschlüsselungstechniken stossen hier an ihre Grenzen. Die Forschungsfelder «secure multi-party computation» und «homomorphic encryption» arbeiten an dieser Herausforderung[13]. Allerdings sind diese kryptografischen Lösungen noch sehr ineffizient und damit meist unpraktikabel.

Für versierte Nutzer kommt noch ein anderer Ansatz infrage, um die eigenen Daten vor dem Zugriff durch Nachrichtendienste zu schützen und trotzdem in die Vorzüge des Cloud-Computings zu kommen: Sie können zu Hause (in ihrem Vertrauensbereich) ihren eigenen Server einrichten und diesen über den eigenen Breitband-Internetzugang an das Internet anbinden. Für den sicheren Zugriff auf die «private» Cloud reicht dann eine Verbindungsverschlüsselung (etwa mit HTTPS) aus. Die Installation eines solchen Heim-Servers wird durch Software-Angebote wie «OwnCloud»[14] zunehmend benutzerfreundlicher. Die Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit der eigenen Daten setzt allerdings technischen Sachverstand und Disziplin voraus: Zum einen muss der Server bei der Einrichtung sicher konfiguriert werden, zum anderen müssen regelmässig Sicherheitsupdates eingespielt werden.

Dominik Herrmann, Dr., Fachbereich Informatik, Universität Hamburg, Hamburg, Deutschland herrmann@informatik.uni-hamburg.de

Bei den meisten Internet-Angeboten sind die auf den Servern hinterlegten Nutzerdaten dem Zugriff durch Nachrichtendienste schutzlos ausgeliefert.

Kurz&bündig

Die Enthüllungen von Edward Snowden haben zu grosser Verunsicherung geführt. Angesichts des umfangreichen technischen Repertoires der Nachrichtendienste sehen sich viele Bürger und Industrievertreter der Massenüberwachung schutzlos ausgeliefert. Tatsächlich lässt sich der Aufwand zur Überwachung durch diverse bereits heute verfügbare Schutzmechanismen erheblich erhöhen. Sowohl für Bürger als auch für die Wirtschaft ist heute der flächendeckende Einsatz entsprechender Schutztechniken möglich. Nicht alle Lösungen bieten jedoch die gleiche hohe Sicherheit. Insbesondere sollte stärker auf quelloffene Softwareentwicklung und unabhängige Auditierung Wert gelegt werden, damit Sicherheitslücken in Zukunft schneller entdeckt und behoben werden können.

Überwachung der Kommunikationsinhalte

Der im vorigen Abschnitt beschriebene Zugriff auf die Daten, die auf den Servern eines Online-Anbieters gespeichert sind, ist für die Nachrichtendienste vergleichsweise aufwändig. Jeder Online-Anbieter, der auf diese Weise überwacht werden soll, muss die angeforderten Daten im Einzelfall entweder manuell sammeln und an den Nachrichtendienst übermitteln oder aber eine entsprechende Abfrageschnittstelle zur Verfügung stellen.

Kritiker der blossen Verbindungsverschlüsselung werfen den Unternehmen daher vor, die Kunden hinsichtlich der tatsächlichen Sicherheit zu täuschen und lediglich eine «Wohlfühlatmosphäre» zu schaffen.

Die Nachrichtendienste bedienen sich daher einer weiteren Aufklärungstechnik: Sie überwachen den Datenverkehr an zentralen Internet-Knotenpunkten, etwa auf den Routern, die Daten über transatlantische Glasfaserkabel transportieren. Dort können sie alle Kommunikationsinhalte unabhängig vom verwendeten Online-Anbieter beobachten. Bei der Überwachung der Glasfaserkabel kann allerdings auch innerdeutscher Datenverkehr erfasst werden: Der aus technischer Sicht effizienteste Transportweg entspricht im Internet nämlich nicht immer der kürzest möglichen Verbindung, er kann also auch über die Vereinigten Staaten führen.

Im Oktober 2013 wurden deutsche Innenpolitiker auf dieses Problem aufmerksam. Sie schlugen vor, durch gesetzliche Regulierung sicherzustellen, dass innerdeutscher Datenverkehr ausschliesslich über deutsche Leitungen transportiert wird. Die Deutsche Telekom, die in Deutschland das grösste Netz betreibt, befürwortete diesen auch als «Schengen-Routing» bezeichneten Vorschlag nachdrücklich. Kritiker wiesen hingegen darauf hin, dass es der Deutschen Telekom beim Schengen-Routing weniger um den Datenschutz gehe als vielmehr darum, ihre Vormachtstellung weiter auszubauen[15]. Zuverlässigen Schutz vor Überwachung durch ausländische Nachrichtendienste könne das als «Schlandnet» von Kritikern verspottete Vorhaben ohnehin nicht bieten: Innerdeutscher Datenverkehr könnte weiterhin von deutschen Behörden abgehört und Nachrichtendiensten anderer Länder zur Verfügung gestellt werden[16]. Wie inzwischen bekannt ist, wurde diese Form der Kooperation in der Vergangenheit etwa am deutschen Knotenpunkt DE-CIX in Frankfurt praktiziert[17].

Die Überwachung der Verbindungen ist effektiv, solange ein Grossteil der transportierten Nachrichten im Klartext übertragen wird. Abhilfe verspricht hier die Initiative «E-Mail made in Germany»[18], die u.a. von der Deutschen Telekom und den Anbietern 1&1 (mit den Angeboten GMX, web.de und freenet) im August 2013 ins Leben gerufen wurde[19]. Das Ziel der Initiative besteht darin, die Vertraulichkeit des Nachrichteninhalts auf dem Transportweg zu schützen. Dazu werden die E-Mails auf den einzelnen Verbindungsabschnitten verschlüsselt übertragen.

Da es sich dabei nur um eine Verbindungsverschlüsselung handelt, liegen die Nachrichten auf den Mailservern allerdings wie bisher im Klartext vor. Kritiker werfen den Unternehmen daher vor, mit dem Problembewusstsein ihrer Kunden zu spielen, sie hinsichtlich der tatsächlichen Sicherheit zu täuschen und lediglich eine «Wohlfühlatmosphäre» zu schaffen[20]. Auch bei anderen Kommunikationsangeboten, die in Deutschland derzeit als «sicher» beworben werden, liegen die Nachrichten auf den Servern der Dienstanbieter zumindest kurzzeitig im Klartext vor (wenn die Nutzer keine zusätzlichen Massnahmen ergreifen). Dies trifft sowohl auf den von der Bundesregierung favorisierten Dienst DE-Mail zu als auch auf den von der Deutschen Post angebotenen E-POSTBRIEF[21].

Zuverlässigen Schutz vor Überwachung bietet lediglich die sogenannte Ende-zu-Ende-Verschlüsselung. Werden E-Mails konsequent mittels Ende-zu-Ende-Verschlüsselung gesichert, kann der Nachrichteninhalt weder auf den Verbindungen noch auch auf den Servern beobachtet werden. Dabei verschlüsselt der Absender einer Nachricht diese mit einem Schlüssel, den lediglich der Empfänger der E-Mail kennt. Die Herausforderung besteht

Literatur

- Borisov Nikita/Goldberg Ian/Brewer Eric A., Off-the-Record Communication, or, Why Not To Use PGP, in Workshop on Privacy in the Electronic Society (WPES '04), 77–84, ACM, 2004.
- Yao Andrew C., Protocols for Secure Computations, in Foundations of Computer Science (SFCS '82), 160–164, IEEE Computer Society, 1982.
- Chaum David, Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Communications of the ACM 24/2, 84–90, 1981.
- Danezis George/Clayton Richard, Introducing Traffic Analysis, in Digital Privacy: Theory, Technologies and Practices, 95–117, Auerbach Publications, 2007.

darin, den Verschlüsselungsschlüssel zwischen den Kommunikationsparteien auf sicherem Wege auszutauschen. In der Praxis haben sich für die Schlüsselverteilung die zwei konkurrierenden Ansätze S/MIME und PGP (bzw. das Open-Source-Pendant GnuPG) etabliert. Während beim S/MIME-Ansatz sog. Zertifizierungsstellen die Überprüfung der Teilnehmeridentität übernehmen, wird diese Aufgabe bei PGP von den Teilnehmern selbst durchgeführt.

Obwohl beide Verfahren schon vor vielen Jahren vorgeschlagen worden sind, werden sie bislang nur von einer Minderheit der Nutzer eingesetzt. Die geringe Akzeptanz ist zum einen auf die unzureichende Software-Unterstützung bzw. die wenig benutzerfreundliche Umsetzung in den gängigen E-Mail-Programmen zurückzuführen. Zum anderen sind viele Nutzer nicht bereit, sich das erforderliche Fachwissen für die Schlüsselerzeugung und -beglaubigung anzueignen bzw. den Aufwand zu betreiben, der für diese Aktivitäten erforderlich ist. Hier besteht noch Verbesserungsbedarf seitens der Software-Anbieter. Fachgesellschaften wie die deutsche Gesellschaft für Informatik (GI) rufen daher dazu auf, stärker als bisher auf Verschlüsselung zu setzen[22].

Überwachung der Kommunikationsumstände

Bei den bisherigen Beispielen ging es um die Vertraulichkeit der Kommunikationsinhalte. Aber auch die Überwachung der Kommunikationsumstände, d.h. wer wie lange mit wem kommuniziert, kann die Vertraulichkeit verletzen. Häufig lassen Kommunikationsbeziehungen auch Rückschlüsse auf Kommunikationsinhalte zu. So kann eine E-Mail, die an eine auf Insolvenzrecht spezialisierte Anwaltskanzlei geschickt wird, beispielsweise als Indiz dafür gewertet werden, dass eine Firma in finanziellen Problemen steckt. Dieser Schluss gelingt auch dann, wenn der Nachrichteninhalt verschlüsselt ist.

Leider ist die heutige Kommunikationsinfrastruktur im Internet nicht auf den Schutz von Kommunikationsumständen ausgelegt: Bei Verschlüsselung einer E-Mail mittels PGP oder S/MIME muss etwa die E-Mail-Adresse des Empfängers im Klartext vorliegen, damit sie an den richtigen Mail-Server zugestellt werden kann. Weiterhin ist im Internetprotokoll, das die Basis aller Internetdienste wie E-Mail und Websurfen ist, jedes Datenpaket mit einer Absender- und Empfängeradresse im Klartext versehen. Diese Art der Adressierung ermöglicht ein flexibles Routing während der Übermittlung der Datenpakete: Das Routing kann in Abhängigkeit von der aktuellen Auslastung dynamisch festgelegt werden.

Um die Kommunikationsumstände im Internet dennoch zu schützen, können sogenannte datenschutzfreundliche Techniken eingesetzt werden. Als vergleichsweise effiziente datenschutzfreundliche Technik gelten die Mix-Netze[23]. Der Grundgedanke des Mix-Verfahrens ist es, Nachrichten (etwa E-Mails) rekursiv zu verschlüsseln und über mehrere unabhängige anonymisierende Zwischenstationen (die sogenannten Mixe) zu leiten. Jeder Mix entfernt eine Verschlüsselungsschicht und erfährt dabei die Adresse des jeweils nächsten Mixes, beziehungsweise – im Fall des letzten Mixes – die Adresse des eigentlichen Empfängers. Im Ergebnis sind die Sender- und Empfängeradressen auf IP-Ebene zwar weiterhin einsehbar, sie geben aber nur Aufschluss über ein Teilstück der eigentlichen Kommunikationsbeziehung. Selbst die Mixe erfahren nur einen Teil der Route.

Die heutige Kommunikationsinfrastruktur im Internet ist nicht auf den Schutz von Kommunikationsumständen ausgelegt: Auch bei Verschlüsselung einer E-Mail muss die Empfängeradresse im Klartext vorliegen.

Allerdings können Nachrichtendienste versuchen, die verschlüsselten Datenströme im Mix-Netz zu analysieren, um die Anonymität wieder aufzuheben (Verkehrsanalyse). Die Rekonstruktion der Kommunikationsbeziehungen gelingt, wenn sich aus dem übertragenen Datenvolumen und den zeitlichen Abständen, in denen Nachrichten an einen Mix gesendet und von ihm weitergeleitet werden, ein charakteristisches Muster ergibt, das an mehreren Stellen im Mix-Netz zu beobachten ist. Hat beispielsweise nur ein Nutzer während eines solchen Angriffs eine Nachricht gesendet und kann der Angreifer alle Kommunikationsverbindungen der Mixe überwachen, ist eine triviale Verkettung der Teilstrecken möglich. Aus diesem Grund leiten Mixe eingehende Nachrichten im Idealfall nicht unmittelbar weiter, sondern warten, bis mehrere Nutzer Nachrichten beigetragen haben, um sie anschliessend zusammen und umsortiert wieder auszugeben. In Abhängigkeit von der Anzahl der Nutzer und der maximal tolerierbaren Verzögerung können dadurch Verkehrsanalysen erheblich erschwert werden.

Ein praktisch nutzbarer Anonymisierungsdienst zur E-Mail-Anonymisierung ist beispielsweise Mixminion[24]. Wegen der Verzögerung durch die Mix-Operationen und die Umleitung der Nachrichten über die Mixe muss allerdings eine Zustellungszeit von mehreren Minuten bis Stunden in Kauf genommen werden. Mit Tor[25] und JonDonym[26] existieren auch Lösungen für den anonymen Zugriff auf das World Wide Web. Um eine akzeptable Performanz zu gewährleisten, verzichten diese beiden Dienste allerdings auf das (ernsthafte) Sammeln und verzögerte Weiterleiten von Daten unterschiedlicher Nutzer: Sämtliche Daten werden unverzüglich weitergeleitet. Wegen der hohen Nachfrage nach anonymer Kommunikation sind die beiden Dienste dennoch chronisch überlastet. Im Vergleich zum direkten Internetzugriff muss mit zusätzlichen Verzögerungen im einstelligen Sekundenbereich gerechnet werden.

Wird auf Ende-zu-Ende-Verschlüsselung verzichtet, besteht die Gefahr, dass die Kommunikationsüberwachung durch die Verwendung eines Anonymisierungsdienstes sogar erleichtert wird.

Wegen der unmittelbaren Weiterleitung der Datenströme bieten Tor und JonDonym keinen zuverlässigen Schutz vor Beobachtern, die sich der oben erwähnten Verkehrsanalysen bedienen. Auch Angreifer, die lediglich einen Teil der Kommunikation überwachen, können Verkehrsanalysen durchführen: Häufig reicht es aus, vor dem ersten Mix (z.B. direkt auf dem Internetanschluss eines Verdächtigen) und nach dem letzten Mix zu überwachen (etwa direkt vor oder auf einem Server mit kriminellen Inhalten). Eine Aufstellung der relevanten Angriffe findet sich beispielsweise in Danezis et al. 2007.

Die vollständige Überwachung der Kommunikation in einem Anonymisierungsnetz ist allerdings sehr aufwändig: So besteht das Tor-Netz inzwischen aus mehr als 3000 Mixen, die über die ganze Welt verteilt sind. Daher ist es wenig verwunderlich, dass Nachrichtendienste anstelle der Verkehrsanalyse auf alternative Überwachungstechniken zurückgreifen: Die NSA soll etwa die Nutzer im Tor-Netz durch Verbreiten von Schadsoftware angegriffen haben. Dabei wurde eine Schwachstelle in der Client-Software von Tor ausgenutzt, die es den Überwachern ermöglichte, einzelne Nutzer zu deanonymisieren[27]. Im Vergleich zur passiven Überwachung des Datenverkehrs ist ein solches aktives Eingreifen wesentlich aufwändiger bzw. leichter aufzudecken. Einige Experten gehen daher davon aus, dass die NSA noch nicht dazu in der Lage ist, sämtliche Kommunikationsbeziehungen im Tor-Netz zu überwachen.

In jedem Fall kann durch die Verwendung von datenschutzfreundlichen Techniken die massenhafte Überwachung erheblich erschwert werden. Allerdings ist zu bedenken, dass die genannten Anonymisierungsdienste keine Ende-zu-Ende-Verschlüsselung vorsehen. Beim Einsatz von Mixminion sollten E-Mails also zusätzlich mittels PGP oder S/MIME verschlüsselt werden. Bei Tor und JonDonym ist darauf zu achten, dass sensible Daten nur auf HTTPS-gesicherten Webseiten eingegeben werden. Wird auf Ende-zu-Ende-Verschlüsselungstechniken verzichtet, besteht die Gefahr, dass die Überwachung der Kommunikation durch die Verwendung eines Anonymisierungsdienstes sogar erleichtert wird: Die übertragenen Inhalte liegen in diesem Fall sowohl auf dem letzten

Fussnoten

1 Vgl. <http://epic.org/privacy/nsl/>.
2 Vgl. <http://www.sueddeutsche.de/digital/geheimdienste-bnd-leitete-telefondaten-an-nsa-weiter-1.2016504>.
3 Vgl. <http://leaksource.info/2013/12/30/nsas-ant-division-catalog-of-exploits-for-nearly-every-major-software-hardware-firmware/>.
4 Siehe Fn. 1.
5 Vgl. <http://www.wired.com/2013/10/lavabit_unsealed/>.
6 Vgl. <http://truecrypt.sourceforge.net>.
7 Vgl. <https://www.boxcryptor.com/>.
8 Vgl. <http://zfoneproject.com/>.
9 Vgl. Borisov et al. 2004.
10 Vgl. <https://threema.ch/de/>.
11 Vgl. <https://telegram.org/>.
12 Vgl. <https://whispersystems.org/>.
13 Vgl. Yao 1982.
14 Vgl. <http://www.owncloud.com/>.
15 Vgl. <https://netzpolitik.org/2013/schengen-routing-de-cix-und-die-bedenken-der-balkanisierung-des-internets/>.
16 Vgl. <http://www.zeit.de/digital/internet/2013-11/schlandnet-telekom-nsa-internet>.
17 Siehe Fn. 2.
18 Vgl. <http://www.e-mail-made-in-germany.de/>.
19 Vgl. <http://heise.de/-19329629>.
20 Vgl. <http://ccc.de/de/updates/2013/sommermaerchen>.
21 Vgl. <https://www.gi.de/aktuelles/meldungen/detailansicht/article/de-mail-fuer-schriftverkehr-mit-behoerden-muss-standardmaessig-ende-zu-ende-verschluesselt-werden.html>.
22 Vgl. <https://www.gi.de/aktuelles/meldungen/detailansicht/article/offener-brief-an-alle-gi-mitglieder.html>.
23 Vgl. Chaum 1981.
24 Vgl. <http://mixminion.net/>.
25 Vgl. <https://www.torproject.org/>.
26 Vgl. <https://anonymous-proxy-servers.net/>.
27 Vgl. <https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html>.
28 Vgl. <http://www.heartbleed.com>.
29 Vgl. <https://www.indiegogo.com/>.
Alle URL letztmals besucht am 11.7.2014.

Mix (der von einem Nachrichtendienst betrieben werden könnte) als auch auf dem Weg von dort zum eigentlichen Empfänger im Klartext vor.

Schutz vor Manipulationen

Sämtliche der oben genannten Schutzmechanismen bieten nur dann Schutz, wenn sie keine Sicherheitslücken enthalten, die von Nachrichtendiensten ausgenutzt werden können. Neben unabsichtlich eingebauten Sicherheitslücken (Bugs) sind hier auch absichtlich eingebaute Schwachstellen (Backdoors) zu nennen. Es ist davon auszugehen, dass die Nachrichtendienste erhebliche Ressourcen darauf verwenden, Lücken in existierender Software zu finden bzw. in Software und Internetprotokolle einzubetten. Die Sicherheit der eingesetzten Software lässt sich nur durch fachkundige Überprüfung gewährleisten.

Da Sicherheitslücken leicht übersehen werden, setzt man zur Überprüfung auf das Mehraugenprinzip, das sich am besten umsetzen lässt, wenn der Quelltext eines Programms veröffentlicht wird (Open-Source-Software). Spätestens seit Bekanntwerden der Heartbleed-Sicherheitslücke ist allerdings deutlich geworden, dass das Open-Source-Modell alleine keine Garantie für Sicherheit bietet: In der OpenSSL-Bibliothek, die auf einem Grossteil der Server im Internet eingesetzt wird, befand sich eine schwerwiegende Sicherheitslücke über einen Zeitraum von mehreren Monaten, bevor sie zufällig von einem Google-Mitarbeiter entdeckt wurde[28]. Dieses Beispiel macht einerseits deutlich, dass sicherheitsrelevante Software zwingend regelmässig von Experten auditiert werden muss und andererseits, dass diese Auditierung noch nicht in ausreichendem Umfang durchgeführt wird.

Daraus ergeben sich die folgenden zwei Herausforderungen: Zum einen sollte Sicherheitssoftware in Zukunft grundsätzlich und wie bereits seit Langem von Experten empfohlen, quelloffen entwickelt werden. Nur so wird die Voraussetzung geschaffen, dass Fehler zeitnah entdeckt und behoben werden können. Zum anderen müssen neue Wege gefunden werden, um für eine weitere Verbreitung von Auditierung zu sorgen, um die Fehler auch tatsächlich identifizieren zu können.

Hinsichtlich der ersten Herausforderung sind insbesondere die Hersteller in der Pflicht. Das früher häufig vorgebrachte Argument, dass sich mit Open-Source-Software kein Geld verdienen lässt, wurde durch viele, insbesondere mittelständische Unternehmen widerlegt. Allerdings ist dafür zum Teil eine Anpassung des Geschäftsmodells nötig: Mit Consulting, Schulungen, Abomodellen, Service-Verträgen und der Entwicklung massgeschneiderter Zusatzmodule lässt sich unter Umständen sogar mehr Geld verdienen als mit der Entwicklung und dem Vertrieb von Closed-Source-Software.

Die Schwierigkeit der zweiten Herausforderung liegt insbesondere darin begründet, dass die Menge und Komplexität der auf Endgeräten eingesetzten Software bereits heute so gross ist, dass die fortlaufende Überprüfung aller Komponenten einen erheblichen Ressourcenaufwand erfordert. Aus diesem Grund kann das Mehraugenprinzip nur funktionieren, wenn Auditierung von den Softwarenutzern aktiv eingefordert wird. Nutzer sollten sich, wenn immer möglich, für auditierte Open-Source-Software entscheiden. Ein entsprechendes Kauf- oder Nutzungsverhalten könnte auf lange Sicht zu einer erheblichen Verbesserung der Situation beitragen. Für die nahe Zukunft und im Fall von kostenloser Software (für die typischerweise wesentlich schwerer freiwillige und dennoch ausreichend qualifizierte Auditoren zu finden sind) sind neue kreative Lösungen gefragt. Crowdfunding könnte etwa ein geeigneter Ansatz sein, um eine unabhängige Auditierung von Open-Source-Software zu ermöglichen: Steht für einen Anwendungsfall keine auditierte Open-Source-Software zur Verfügung, können Nutzer sich zu einer Interessengemeinschaft zusammenschliessen und über eine Crowdfunding-Plattform wie Indiegogo[29] weitere Interessenten zur Finanzierung eines Audits finden. Wie vielversprechend dieser Ansatz ist, lässt sich an der Auditierung von TrueCrypt erkennen, für die in einem Zeitraum von nur zwei Monaten über 46 000 USD eingesammelt wurden.

Es ist davon auszugehen, dass die Nachrichtendienste erhebliche Ressourcen darauf verwenden, Lücken in Software zu finden bzw. einzubetten.

Grundsätzlich sollte der Anspruch an Open-Source-Software nicht kostenlose Nutzbarkeit oder die im Vergleich zu Closed-Source-Software geringeren Kosten sein. Vielmehr sollten die Überprüfbarkeit und Erweiterbarkeit von Open-Source-Software im Vordergrund stehen. Einen Teil des durch Open-Source-Software eingesparten Geldes in deren Auditierung zu investieren, wäre sowohl im Interesse der Softwarenutzer als auch der Hersteller.

Schlussfolgerungen

Insgesamt haben die Fallbeispiele in diesem Artikel gezeigt, dass Internetnutzer die Überwachung ihrer Aktivitäten durch den Einsatz von Schutzwerkzeugen erheblich erschweren bzw. verhindern können. Würden alle Nutzer geeignete Schutzwerkzeuge einsetzen, müssten die Nachrichtendienste zur Überwachung auf aktive Angriffstechniken ausweichen, etwa die Installation eines trojanischen Pferdes unter Ausnutzung einer Sicherheitslücke. Im Vergleich zur kaum Aufwand verursachenden Überwachung unverschlüsselter Kommunikation, bei der die Nutzer den Nachrichtendiensten die Kommunikationsinhalte quasi «auf dem Präsentierteller» überreichen, stiege dadurch der Angriffsaufwand so stark, dass eine verdachtsunabhängige Massenüberwachung selbst für einen Nachrichtendienst mit erheblichen Ressourcen nicht mehr ökonomisch wäre.

Internetnutzer können die Überwachung ihrer Aktivitäten durch den Einsatz von Schutzwerkzeugen erheblich erschweren bzw. verhindern.

Zum Schutz ihrer Privatsphäre müssen Internetnutzer in die Sicherheit ihrer IT-Infrastruktur investieren. Dabei sollten sie gezielt auf quelloffene und auditierte Software setzen. In der Wissenschaft sollte, neben der obligatorischen Weiterentwicklung bestehender und Gestaltung neuer Schutzmechanismen, insbesondere mehr Wert auf die Verbesserung der Benutzbarkeit von Sicherheitslösungen gelegt werden. Schliesslich entscheidet die Benutzbarkeit von Software massgeblich darüber, ob sie von den Nutzern akzeptiert wird. Umgekehrt müssen aber auch die Nutzer in ihrem eigenen Interesse einen gewissen Mehraufwand in Kauf nehmen: Es geht hierbei schliesslich nicht nur um den Schutz vor Nachrichtendiensten, sondern auch vor Internetkriminellen, neugierigen oder missgünstigen Kollegen sowie, in der Industrie, um die Wahrung von Geschäftsgeheimnissen vor konkurrierenden Unternehmen. ■

agenda

ISSE 2014
14.–15. Oktober 2014, Brüssel
http://www.isse.eu.com/

Datenschutz im Gesundheitswesen – privatim
29. Oktober 2014, 13.45–17.15, Zug
http://www.privatim.ch

Sicherung des Grundrechts auf Datenschutz in der EU
30.–31. Oktober 2014, Paris
http://www.era.int

38. Datenschutzfachtagung (DAFTA)
20.–21. November 2014, Köln
https://www.gdd.de/veranstaltungen

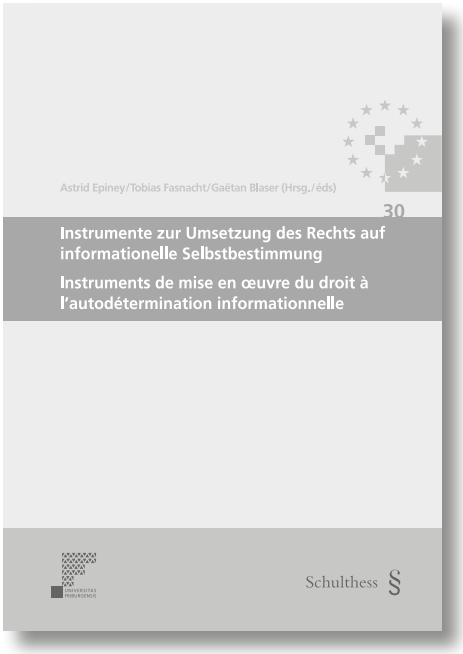
ISSS: Berner Tagung 2014
«Big Data: Die Herausforderungen für die Informationssicherheit»
26. November 2014
http://www.isss.ch

ZertiFA 2014
Zertifikate, Audits, Gütesiegel für Security und Datenschutz
2. Dezember 2014, Berlin
http://www.computas.de

Computers, Privacy and Data Protection (8th International CPDP Conference)
21.–23. Januar 2015, Brüssel
http://www.cpdpconferences.org/

DuD 2015
Datenschutz und Datensicherheit
15.–16. Juni 2015, Berlin
http://www.computas.de

20. Symposium on Privacy and Security
Jubiläumsveranstaltung
Stiftung für Datenschutz und Informationssicherheit
27. August 2015, Zürich
http://www.privacy-security.ch



Erschienen	Dezember 2013
ISBN	978-3-7255-6950-2
	144 Seiten, broschiert
Preis	CHF 62.00

Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung Instruments de mise en œuvre du droit à l'autodétermination informationnelle

Forum Europarecht, Band 30

Astrid Epiney/Tobias Fasnacht/Gaëtan Blaser (Hrsg.)

Dieser Tagungsband enthält die schriftliche Fassung der an der sechsten schweizerischen Datenschutzrechtstagung 2013 in Freiburg vorgetragenen und diskutierten Referate. Im Fokus steht die (kritische) Auseinandersetzung mit der verfassungsrechtlichen Ausgestaltung des Rechts auf informationelle Selbstbestimmung in der schweizerischen Lehre und Rechtsprechung. Ergänzend werden sodann verschiedene Instrumente besprochen, die international diskutiert werden, um diesem Grundrechtsgehalt normative Wirkung zu verleihen bzw. ihn zu konkretisieren und durchzusetzen.

Cet ouvrage réunit les versions écrites des conférences présentées lors de la sixième Journée suisse du droit de la protection des données, organisée à Fribourg en juin 2013. Les diverses contributions proposent une analyse critique de la garantie constitutionnelle à l'autodétermination informationnelle. Ce sujet est abordé tant du point de vue de la doctrine que de celui de la jurisprudence. Divers instruments développés au niveau international et destinés à mettre en œuvre et à concrétiser ce droit fondamental sont également présentés.

Herausgeber:
Prof. Dr. iur. Astrid Epiney, LL.M.
Tobias Fasnacht, MLaw
Gaëtan Blaser, MLaw

Schulthess Juristische Medien AG
Zwingliplatz 2, Postfach
CH-8022 Zürich/Switzerland
Telefon +41 44 200 29 29
Fax +41 44 200 29 28
buch@schulthess.com
www.schulthess.com

Schulthess §

Resignation oder Revanche?

Die Methoden der Internet-Überwachung durch Nachrichtendienste und mögliche Gegenstrategien

Helmut Eiermann, Leiter des Bereichs Technik beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, Mainz, Deutschland h.eiermann@datenschutz.rlp.de

Häufige Reaktionen auf die Enthüllungen Edward Snowdens waren Resignation oder Revanchegedanken. Das mag verständlich sein, anzuraten ist beides nicht.

Yes, we can!», lautete der Slogan aus dem amerikanischen Präsidentschaftswahlkampf 2008. Er ist, neben dem Konterfei Obamas von Shepard Fairey[1], eines der beiden Dinge, die regelmässig mit dem amerikanischen Präsidenten assoziiert werden.

«Yes, we scan!», lautet seit letztem Jahr eine auf die NSA-Aktivitäten anspielende Abwandlung, und auch ikonografisch hat Obama Konkurrenz bekommen. Eines der 2013 meistpublizierten Bilder zeigt einen leicht melancholisch wirkenden jungen Mann mit Brille und 3-Tage-Bart[2]. Edward Snowden scheint zu spüren, dass die von ihm öffentlich gemachten Überwachungspraktiken auf immer mit seinem Namen verknüpft sein werden.

Die Enthüllungen Snowdens haben ein Ausmass der Überwachung offenbart, das selbst skeptischste Mutmassungen übertroffen hat[3]. Die Reaktionen schwanken zwischen Resignation und Revanche. Angesichts der Internet-Dominanz Amerikas und der technischen Fähigkeiten der NSA mögen Zweifel erlaubt sein, ob sich eine Gegenwehr überhaupt lohnt. Dennoch gibt es Möglichkeiten, der Sammelwut entgegenzutreten, um die Freiheit im Netz zu bewahren und digitale Grundrechte zu sichern.

Methodik und Reichweite der Überwachung

Die grossflächige Überwachung der Internet-Kommunikation fusst im Wesentlichen auf zwei Ansätzen:

- *Überwachung, Sammlung und Auswertung des über die globalen Kommunikationsverbindungen laufenden Datenverkehrs.* Die Namen der entsprechenden Überwachungsprogramme lauten FAIRVIEW, STORMBREW, BLARNEY oder OAKSTAR, zusammengefasst unter dem Oberbegriff UPSTREAM. Erleichtert wird dies durch die Situation, dass ein Grossteil der globalen Internetverbindungen über die USA führt oder von Ländern der sogenannten «Five Eyes»-Gruppe (z.B. Grossbritannien) gebündelt wird. Hinzu kommt, dass die nationalen Telekommunikationsanbieter selbst nicht oder nur ausnahmsweise über eigene interkontinentale Verbindungen verfügen und sich hierzu globaler sogenannter «Tier-1-Provider» bedienen, welche die Backbone-Strukturen des Internets betreiben. Bei einem Grossteil davon handelt es sich um US-amerikanische Unternehmen.
- *Sammlung von Daten direkt bei amerikanischen Anbietern von Internet- und Kommunikationsdiensten (PRISM).* So vielfältig die von Google, Facebook, Yahoo, Microsoft, Apple usw. angebotenen Dienste sind (E-Mail, Chat, Videoplattform, Videokonferenz, Soziale Netzwerke, Clouddienste usw.), so vielfältig und zahlreich sind auch die dabei gewonnenen Daten.

Hinzu kommt, dass auch dann, wenn Dienste eines europäischen Anbieters genutzt werden, die Zugriffe aus Kapazitäts- oder Kostengründen häufig über die USA geleitet werden[4]. Soweit die Zugriffe nicht verschlüsselt erfolgen, können auf diese Weise Verbindungs- und Inhaltsdaten abgegriffen werden. Der Anspruch der NSA auf eine möglichst vollständige Erfassung der Kommunikation wird mit offensivem Selbstbewusstsein vorgetragen: «Man braucht den Heuhaufen, um die Nadel zu finden», meint denn auch NSA-Chef Keith Alexander[5].

Ergänzt wird die grossflächige Überwachung der Internet-Kommunikation durch die gezielte Manipulation oder Infiltration einzelner Systeme, Dienste oder Kommunikationsverbindungen. Diese sogenannten Tailored Access Operations[6] sind zum Teil massgeschneidert auf das jeweilige Zielobjekt. Die zugehörige Werkzeugsammlung[7] wird angesichts der Vielfalt bedarfsweise kompromittierbarer Systeme bisweilen als «Shopping»-Katalog bezeichnet[8]. Vor dem Angriff steht die Aufklärung; im Rahmen

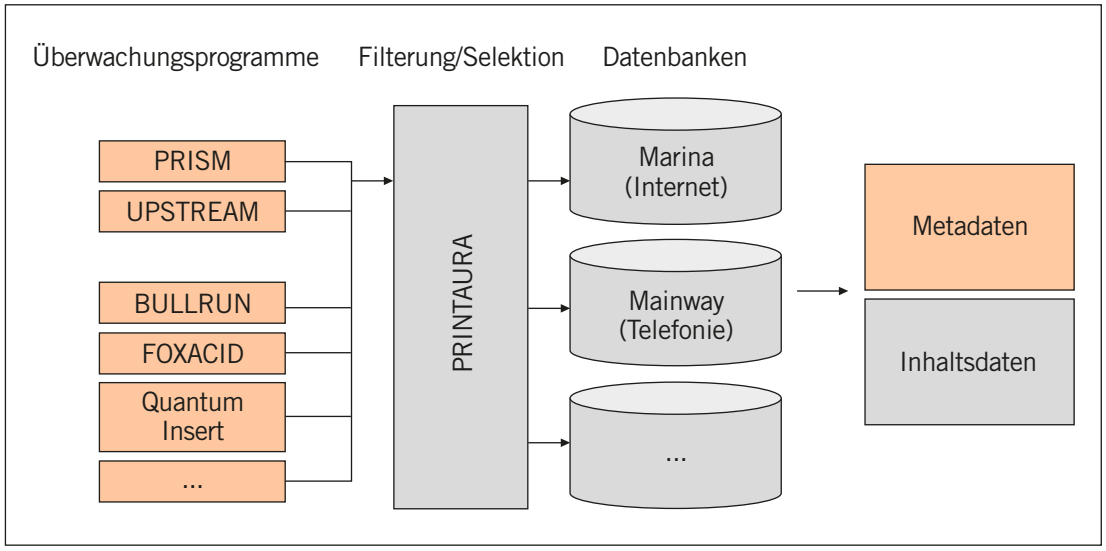


Abb. 1: PRISM/UPSTREAM/TEMPORA

des HACIENDA-Projekts werden daher die IT-Systeme ganzer Länder automatisiert auf Schwachstellen, Verwundbarkeiten in der Infrastruktur der Netze und potenzielle Nutzbarkeit hin untersucht[9].

All dies ist trotz staatlicher Einwirkungsmöglichkeiten nicht zum Nulltarif zu haben, und so verwundert es nicht, dass das Budget der NSA für die Sammlung von Daten (2,5 Mrd. USD) und deren Auswertung (1,6 Mrd. USD)[10] bald grösser ist als die Wirtschaftsleistung manches europäischen Landes.

Die dargestellten Verfahrensweisen betreffen zunächst die technischen Möglichkeiten der Überwachung. Von Fällen wie der Überwachung der Mobiltelefonate der deutschen Bundeskanzlerin oder Informationen in den Snowden-Dokumenten[11] abgesehen, bleibt der Natur von Nachrichtendiensten entsprechend vielfach offen, wie viele Personen konkret betroffen sind. Auch der im Juni 2014 erstmals veröffentlichte Transparenzreport der NSA[12] bleibt in vielen Punkten unklar. Konkrete Hinweise auf die Reichweite der Internet-Überwachung liefern jedoch einzelne Äusserungen, wie die des stellvertretenden NSA-Direktors Chris Inglis, dass unter Umständen die Kommunikationspartner der zweiten und dritten Ebene («two or three hops») überwacht werden[13]. Oder, in der Terminologie sozialer Netzwerke, die Freunde von Freunden von Freunden. Bei angenommenen 150 elektronischen Kontakten einer Person innerhalb eines bestimmten Zeitraums (Telefonate, Textnachrichten, E-Mails, Postings, Kommentaren, Likes, Shares etc.) wären dies im dritten Schritt mehr als drei Millionen Betroffene. 90 Prozent davon sind unverdächtig[14].

Die Macht der Metadaten

Ein Effekt der Snowden-Veröffentlichungen ist, dass die Bedeutung der sogenannten Metadaten, d.h. die eine Kommunikation arrondierenden, von den eigentlichen Inhalten losgelösten Informationen, in das öffentliche Bewusstsein gehoben wurde. Zwar sind Informationsgehalt und Aussagekraft von Metadaten keine neue Erkenntnis[15], wie sehr sie Kommunikationsverhalten, Lebensumstände, Interessen, Vorlieben oder Mobilitätsverhalten der

Das Budget der NSA für die Sammlung von Daten und deren Auswertung ist bald grösser als die Wirtschaftsleistung manches europäischen Landes.

Kurz&bündig

Die Enthüllungen Snowdens haben ein Ausmass der Überwachung offenbart, das selbst skeptischste Mutmassungen übertroffen hat. Die Überwachung der Internet-Kommunikation fusst auf zwei zentralen Ansätzen: der Überwachung, Sammlung und Auswertung des globalen Datenverkehrs und dem Abgreifen der Daten bei Anbietern von Internet- und Kommunikationsdiensten. Sie folgt der Philosophie *«You need the haystack to find the needle».* 90 Prozent der betroffenen Nutzer sind unverdächtig. Die Überwachung konzentriert sich dabei auf Metadaten, die auch losgelöst von den Inhalten einer Kommunikation Lebensumstände, Interessen, Vorlieben oder Mobilitätsverhalten der Nutzer offenbaren. Gründe genug also, um in Resignation zu verfallen. Auch Revanchegedanken mögen verständlich sein, anzuraten ist beides nicht. Auf unterschiedlichen Ebenen bestehen Möglichkeiten, der massenhaften Ausspähung entgegenzutreten, um die Freiheit im Netz zu bewahren und digitale Grundrechte zu sichern.

Nutzer offenbaren und zum Teil voraussagen lassen, war in der allgemeinen Öffentlichkeit bislang jedoch weitgehend unbekannt. Dass Zeitpunkt, Ort, Dauer und Rufnummern eines Telefonats auch ohne den Inhalt des Gesprächs interessantes Wissen bergen, konnte man schon den eigenen Einzelverbindungsnachweisen entnehmen. Dass ein Tweet von 140 Zeichen mit seinen ca. 40 Metainformationen[16] in weiten Teilen das kommunikative Umfeld des Absenders erkennen lässt, ist vielen nicht bekannt. Gerade soziale Netzwerke mit ihren vermaschten 1:n-Beziehungen eröffnen mit ihren Metadaten eine wahre Fundgrube der Erkenntnis. Die Geschäftsmodelle Facebooks und Googles basieren gerade auf dieser Transparenz ihrer Nutzer.

Vieles von dem, was Snowden enthüllt hat, geht auf eine blauäugige Unschuld zurück, mit der das Internet als neutrales Kommunikationsmedium betrachtet wurde.

Metadaten sind jedoch auch die eher unauffälligen Begleitdaten eines Internet-Zugriffs: IP-Adressen, Cookies, Browserdaten, App-IDs, oder Geräte-Fingerprints[17]. Diese werden ergänzend zu E-Mail-Adressen, Telefonnummern oder Login-Namen als «weiche Selektoren» genutzt, um im steten Datenstrom des Internets relevante Kommunikationspartner oder Datenzugriffe ausfindig zu machen[18]. Auch wenn der Nutzer Cookies löscht, seinen Browser aktualisiert oder ein anderes Endgerät nutzt, beim nächsten E-Mail-Abruf, der nächsten Anmeldung am Sozialen Netzwerk oder dem nächsten Besuch der Suchmaschine werden die Selektoren ergänzt bzw. auf den neuesten Stand gebracht und verknüpft. Dies erlaubt über die Auswertungsprogramme XKEYSCORE und BOUNDLESS INFORMANT Abfragen nach dem Muster *«Meine Zielperson nutzt Google-Maps. Kann ich dies nutzen, um seine E-Mail-Adresse herauszufinden? Wonach hat sie im Web gesucht?»* oder *«Meine Zielperson spricht deutsch und hält sich in Pakistan auf; wie kann ich sie ausfindig machen?»*[19].

Die Konzentration der Datensammlung auf Metadaten hat auch einen pragmatischen Grund: Das Internet-Datenvolumen ist letztlich zu gross, um dauerhaft alles zu erfassen. Auch die Heuhaufen-Doktrin erfordert eine Schwerpunktsetzung, und diese liegt bei der Erfassung, Speicherung und Auswertung von Metadaten. Während die mit dem Schleppnetz der NSA erfassten Inhaltsdaten für drei Tage gepuffert werden, werden Metadaten in den beiden Hauptdatenbanken MARINA (Internet) und MAINWAY (Telefonie) bis zu einem Jahr vorge-

Fussnoten

1 Vgl. <http://en.wikipedia.org/wiki/Barack_Obama_%22Hope%22_poster>.
2 Vgl. <http://en.wikipedia.org/wiki/Edward_Snowden>.
3 Vgl. <http://www.heise.de/thema/NSA>.
4 Vgl. <http://apps.opendatacity.de/prism/>.
5 Vgl. <http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html>.
6 Vgl. <http://www.spiegel.de/netzwelt/netzpolitik/neue-dokumente-der-geheime-werkzeugkasten-der-nsa-a-941153.html>.
7 Vgl. <https://www.eff.org/files/2014/01/06/20131230-appelbaum-nsa_ant_catalog.pdf>.
8 Vgl. <http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html>.
9 Vgl. <http://www.heise.de/ct/artikel/NSA-GCHQ-Das-HACIENDA-Programm-zur-Kolonisierung-des-Internet-2292574.html>.
10 Vgl. <http://www.washingtonpost.com/wp-srv/special/national/black-budget/>.
11 Vgl. <http://apps.washingtonpost.com/g/page/world/the-nsas-over collection-problem/517/>.
12 Vgl. <http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013>.
13 Vgl. <http://www.thewire.com/politics/2013/07/nsa-admits-it-analyzes-more-peoples-data-previously-revealed/67287/>.
14 Vgl. <http://www.zeit.de/digital/datenschutz/2014-07/nsa-ueberwachung-90-prozent-unverdaechtige>.
15 Vgl. <http://www.zeit.de/digital/datenschutz/2014-04/vorratsdatenspeicherung-schweiz-daenemark-visualisierung>.
16 Vgl. <http://readwrite.com/2010/04/19/this_is_what_a_tweet_looks_like>.
17 Vgl. <http://www.datenschutz.rlp.de/de/selbstds.php?submenu=datenspuren>.
18 Vgl. <http://www.spiegel.de/fotostrecke/photo-gallery-how-the-nsa-infiltrates-computers-fotostrecke-105339-17.html>.
19 Vgl. <http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation>.
20 Vgl. <http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents>.
21 Vgl. <http://www.heise.de/newsticker/meldung/SPD-will-als-Reaktion-auf-NSA-Skandal-USA-ausspionieren-2106570.html>.
22 Vgl. <http://www.faz.net/aktuell/wirtschaft/unternehmen/schreibmaschinen-als-antwort-auf-die-nsa-13045490.html>.
23 Vgl. Federrath Hannes/Fuchs Karl-Peter/Herrmann Dominik, Schutz vor Überwachung im Internet, digma 2014, 100 ff.
24 Vgl. <http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=dsb&ber=087_elkomm>.
25 Vgl. <http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance>.
26 Vgl. <http://www.sueddeutsche.de/digital/nsa-ueberwachung-deutschland-draengte-microsoft-zur-klage-gegen-e-mail-durchsuchung-1.2056197>.
27 Vgl. <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+IM-PRESS+20140210IPR35501+0+DOC+PDF+V0//EN&language=DE>.
(Alle URL letztmals besucht am 20.8.2014).

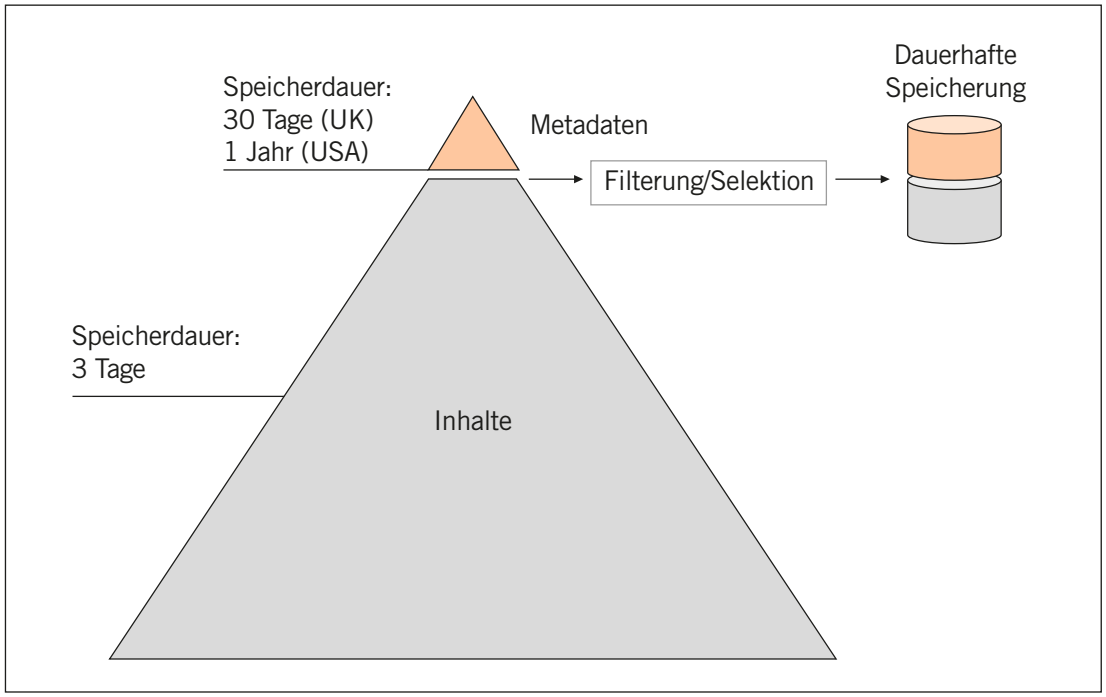


Abb. 2. Inhalts- und Metadaten

halten[20]. Filterungs- und Selektionsprozesse oder aktuelle Anforderungen entscheiden darüber, welche Daten für einen längeren Zeitraum oder dauerhaft gespeichert werden.

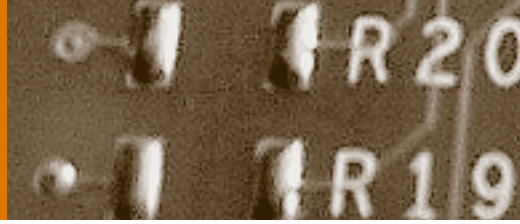
Gegenstrategien

Gründe genug also, um in Resignation zu verfallen? In der Tat, die Internet-Überwachung reicht weit, und wer in den Fokus der NSA gerät, hat wenig Möglichkeiten, sich dieser zu entziehen. Auch Revanchegelüste[21] mögen angesichts einer empfundenen Hilflosigkeit verständlich sein, anzuraten ist beides nicht. Wenngleich manche Ansätze der Gegenwehr eher drollig wirken[22], bestehen auf unterschiedlichen Ebenen doch Möglichkeiten, der massenhaften Ausspähung entgegenzutreten.

- Persönlich haben die Nutzer es in der Hand, auf Instrumente zurückzugreifen, die Vertraulichkeit oder Anonymität bieten[23]. Auch die Empfehlungen der Konferenz der deutschen Datenschutzbeauftragten[24] gehen in diese Richtung. Trotz der technischen Kompetenz der NSA kann man laut Edward Snowden auf den Schutz durch starke Verschlüsselung vertrauen[25]. Mag die NSA auch die eine oder andere Verschlüsselungslösung beherrschen, so lässt ihr Einsatz doch den Aufwand steigen und hilft, die Überwachung als Massenphänomen zurückzudrängen.
- Auf der technischen Ebene sollte daher der Einsatz von Verschlüsselungslösungen zum Regelfall werden. Erste Ansätze hierfür zeigen sich verstärkt auf Anbieterseite. Die Endnutzer wird man jedoch nur gewinnen können, wenn die Lösungen auch handhabbar sind.
- Das teils belächelte und geschmähte «Nationale Routing» stellt einen weiteren Ansatz dar, die Zugriffsmöglichkeiten auf Datenströme zu reduzieren. Dabei geht es nicht um eine «Balkanisierung des Internet», in Zeiten globalisierter Infrastrukturen ein ohnehin schwieriges Unterfangen, sondern um die Rückgewinnung der technologischen Souveränität, zumindest im Bereich der staatlichen Kommunikation.
- Auch auf der politisch-rechtlichen Ebene ist erkennbar, dass ausser Resignation und Revanche mit Reaktion ein dritter Weg beschritten werden kann. Vom sanften Drängen, mit dem die deutsche Bundesregierung offenbar grosse US-Anbieter ermuntert hat, rechtliche Schritte gegen die Überwachungsbegehren der NSA zu ergreifen[26], bis hin zu den Empfehlungen des Ausschusses für bürgerliche Freiheiten des Europaparlaments, das Safe-Harbor- und andere Abkommen auszusetzen[27], bietet sich eine Klaviatur an, auf der zu spielen sich lohnt.

Vieles von dem, was Snowden enthüllt hat, hat seine Wurzeln im «9/11»-Anschlag in New York und vieles geht auf eine blauäugige Unschuld zurück, mit der das Internet als neutrales Kommunikationsmedium betrachtet wurde. Für beides braucht es eine Neubewertung. Nicht resignativ, nicht revanchistisch, sondern vorausschauend, klug und selbstbewusst. Wir können der Massenüberwachung des Internet etwas entgegensetzen und sollten dies auch tun.

Yes, we can! ■



Recht

Auftragsdatenbearbeitung – zum Dritten

Barbara Widmer, lic. iur., LL.M., CIA, Juristische Mitarbeiterin beim Datenschutzbeauftragten des Kantons Basel-Stadt, Basel barbara.widmer@dsb.bs.ch

«Man sieht nur, was man weiss»[1].

In der Praxis fällt auf, dass viele Vertragsparteien nicht wissen, dass der von ihnen abgeschlossene Vertrag eine Auftragsdatenbearbeitung im Sinne von Art. 10*a* DSG[2] enthält. In der Folge übersehen sie die Notwendigkeit zur Aufnahme der entsprechenden datenschutzrechtlichen Regelungen, was sich aufgrund der Verantwortlichkeitsaufteilung nach Art. 10*a* DSG für den Auftraggeber je nach Sachlage unangenehm auswirken kann[3]. Wie im ersten Teil ausgeführt (digma 2014, 24), hat die Auftragsdatenbearbeitung keinen Selbstzweck, sondern steht regelmässig im Zusammenhang mit einer dem Auftraggeber übertragenen Aufgabe/Pflicht (primär öffentliche Organe) oder von diesem bearbeiteten Geschäftsfeld (primär natürliche und juristische Personen). Fehlen dem Auftraggeber die inhaltlichen Kompetenzen oder die zeitlichen und personellen Ressourcen, um eine Aufgabe oder eine Geschäftstätigkeit vollständig selbst durchzuführen, kann er sich durch die Hinzuziehung von Dritten entlasten. Grundlage eines solchen Hinzuzugs bildet in der Regel ein Vertragsverhältnis.

Aufgrund dieser Ausgangslage richtet sich der Fokus nachfolgend im Rahmen eines weiteren Beitrags der Artikelreihe zur Auftragsdatenbearbeitung nach Art. 10*a* DSG auf einige typische Vertragsverhältnisse, die tendenziell oder regelmässig eine Auftragsdatenbearbeitung umfassen. Dabei werden die einzelnen Vertragsverhältnisse jeweils zuerst allgemein und anschliessend unter dem Fokus der Auftragsdatenbearbeitung beleuchtet. Festzuhalten ist, dass diese Übersicht keinen Anspruch auf Vollständigkeit erhebt, sondern lediglich in Anlehnung an das Eingangszitat das «Sehen» erleichtern soll. Der erste Teil der Artikelreihe zum Inhalt und zur Ausgestaltung von Art. 10*a* DSG findet sich in digma 2014.1 und der zweite Teil zum Thema Rechtsbehelfe und Rechtsschutz in digma 2014.2. Der vierte und voraussichtlich letzte Teil folgt in digma 2014.4.

Grundlagen

Verträge lassen sich mitunter nach ihrer charakteristischen Leistung einteilen. Bei diesem Vorgehen findet eine Unterscheidung zwischen Veräusserungsverträgen (z.B. Kauf, Schenkung), Gebrauchsüberlassungsverträgen (z.B. Miete, Leihe), Arbeitsverträgen sowie Dienstleistungsverträgen (z.B. Auftrag, Werkvertrag) statt[4]. Auftragsdatenbearbeitungen im Sinne von Art. 10*a* DSG finden sich verbreitet (wenn nicht ausschliesslich) im Rahmen von Dienstleistungsverträgen. Weshalb dem so ist und welche Konsequenzen sich daraus ergeben, sollen die nachfolgenden Ausführungen veranschaulichen.

Gemäss Literatur gelten als Dienstleistungsverträge jene Verträge, deren charakteristische Leistung ganz oder zu einem wesentlichen Teil ein (unabhängiges) entgeltliches Tätigwerden zum Vorteil eines anderen beinhaltet[5]. Dabei kann es sich um eine einmalige Leistung oder ein Dauerschuldverhältnis handeln. Die gesetzlich geregelten Dienstleistungsverträge umfassen den Auftrag und den Werkvertrag. Daneben findet sich aber auch in einer Vielzahl vom Gesetz nicht geregelter Verträge ein entgeltliches Tätigwerden zum Vorteil eines anderen, wie z.B. beim Factoring, bei Begutachtungs- und Beratungsverträgen oder bei Cloud-Computing-Verträgen[6].

Da im Rahmen einer Auftragsdatenbearbeitung nach Art. 10*a* DSG ein Dritter mit der Bearbeitung von Personendaten betraut wird, sind Dienstleistungsverträge aufgrund ihrer oben beschriebenen Ausprägung (entgeltliche

Arbeit zum Vorteil eines anderen) besonders geeignet, eine Auftragsdatenbearbeitung zu beinhalten. Allerdings enthält längst nicht jeder Dienstleistungsvertrag auch eine Auftragsdatenbearbeitung. Neben der Qualifikation als Dienstleistungsvertrag sind immer auch der konkrete Vertragstypus sowie die Umstände des Einzelfalls massgebend (z.B. umfasst die Auftragsdatenbearbeitung Personendaten).

Nachfolgend finden einige ausgewählte Dienstleistungsverträge aufgrund ihrer übergeordneten Bedeutung mit Bezug auf Auftragsdatenbearbeitungen nach Art. 10*a* DSG eine eingehendere Betrachtung. Es handelt sich dabei um den Auftrag, das Factoring, kollektive Taggeldversicherungsverträge, Begutachtungs- und Beratungsverträge, Softwareentwicklungs- und Softwarepflegeverträge sowie Cloud-Computing-Verträge.

Vertragsverhältnisse

Auftragsverhältnisse

Vertragstypische Elemente: Im Rahmen eines Auftragsverhältnisses verpflichtet sich der Beauftragte gegenüber dem Auftraggeber, ein ihm übertragenes Geschäft vertragsgemäss zu besorgen (Art. 394 Abs. 1 OR). Dabei erbringt der Beauftragte seine Arbeitsleistung mit Blick auf ein bestimmtes vertraglich vereinbartes Ziel, wobei lediglich das Tätigwerden im Hinblick auf dieses Ziel, nicht aber die Zielerreichung Vertragsgegenstand bildet. Inhalt eines Auftrags kann jede mögliche, nicht widerrechtliche Tätigkeit sein. Welche Dienstleistungen durch den Beauftragten im Einzelfall konkret zu erbringen sind, sollte sich aus der vertraglichen Vereinbarung ergeben. Wurde der Auftragsumfang nicht ausdrücklich bezeichnet, bestimmt sich dieser nach der Natur des zu besorgenden Geschäfts (Art. 396 Abs. 1 OR). Der Auftragnehmer haftet dem Auftraggeber für getreue und sorgfältige Ausführung der vereinbarten Leistungen (Art. 398 Abs. 2 OR)[7].

Im Gegenzug für die Auftragserbringung bezahlt der Auftraggeber dem Auftragnehmer eine Vergütung. Obwohl der Auftrag von Gesetzes wegen auch unentgeltlich erbracht werden kann (Art. 394 Abs. 3 OR), spricht aufgrund der heutigen Bedeutung der Dienstleistungsgesellschaft regelmässig eine faktische Vermutung für die Entgeltlichkeit des Auftrags. Wurde die Höhe der Vergütung des Auftrags nicht vereinbart, ist eine übliche, angemessene Vergütung geschuldet[8].

Der Auftrag kann sowohl eine einmalige Leistung beinhalten als auch als Dauerschuldverhältnis ausgestaltet sein und von beiden Parteien jederzeit widerrufen oder gekündigt werden (Art. 404 Abs. 1 OR). Findet der Widerruf oder die Kündigung allerdings zur Unzeit statt, hat der zurücktretende Teil der anderen Partei einen dadurch entstanden Schaden zu ersetzen (Art. 404 Abs. 2 OR)[9].

Enthaltene Auftragsdatenbearbeitung: Entsprechend der oben beschriebenen Inhaltsvielfalt von Auftragsverhältnissen können diese eine Auftragsdatenbearbeitung nach Art. 10*a* DSG umfassen, müssen aber nicht. Voraussetzung ist, dass der Auftragnehmer als Dritter zur Erfüllung des Auftrags Personendaten (im Sinne von Art. 3 lit. a, c und d DSG) im Besitz oder Eigentum des Auftraggebers bearbeitet. Zu den Auftragsverhältnissen, in deren Rahmen dieses Erfordernis regelmässig erfüllt ist, gehören die Auslagerung der Lohnbuchhaltung, die Auslagerung des Personalwesens (inkl. Auftragsverhältnisse zur Durchführung von Assessments, Outplacements und Ähnlichem) sowie die Auslagerung der Kundenbewirtschaftung und -befragung oder des Case Managements. Bearbeitet der Auftragnehmer zwar Daten, die sich im Besitz oder Eigentum des Auftraggebers befinden, enthalten diese aber keine Personendaten, liegt keine Auftragsdatenbearbeitung nach Art. 10*a* DSG vor.

Factoring

Vertragstypische Elemente: Mittels eines Factoring-Vertrags werden das Risiko der Zahlungsunfähigkeit sowie die administrativen Debitorenumtriebe gegen eine Factoring-Gebühr an ein Factoring-Un-

Kurz&bündig

Dienstleistungsverträge enthalten aufgrund ihrer charakteristischen Leistung verbreitet Auftragsdatenbearbeitungen im Sinne von Art. 10a DSG. Innerhalb der Dienstleistungsverträge finden sich diese insbesondere in folgenden Vertragstypen: Dem Auftrag, dem Factoring, kollektiven Taggeldversicherungsverträgen, Begutachtungs- und Beratungsverträgen, Softwareentwicklungs- und Softwarepflegeverträgen sowie Cloud-Computing-Verträgen. In der Praxis wird das Vorliegen von Auftragsdatenbearbeitungen oft übersehen und die Verträge werden in der Folge nicht datenschutzkonform ausgearbeitet. Dies kann aufgrund der Verantwortlichkeitsaufteilung von Art. 10*a* DSG für den Auftraggeber unangenehme Auswirkungen zeitigen.

ternehmen übertragen (zediert). Dabei findet eine Unterscheidung in unechtes und echtes Factoring statt: Beim *unechten* Factoring übernimmt das Factoring-Unternehmen gegen ein entsprechendes Entgelt für den Klienten die Führung der Debitorenbuchhaltung, die Rechnungsstellung, das Mahnwesen, das Inkasso sowie die Bevorschussung der offenen Forderungen. Beim *echten* Factoring kommt zu diesen Dienstleistungen die Übernahme des Delkredererisikos hinzu[10].

Da im Rahmen eines Factoring-Vertrags vornehmlich Elemente von Nominatverträgen kombiniert werden, wird dieser in der Literatur den gemischten Verträgen zugeordnet. Je nach Ausgestaltung des konkreten Vertrags kommen insbesondere Kauf, Zession, Auftrag und/oder Darlehen infrage. Der Factoring-Vertrag stellt ein Dauerschuldverhältnis dar und erlischt entsprechend nicht durch einmalige Erfüllung. Vielmehr ist dieser zu erfüllen, bis er durch Zeitablauf oder aus einem anderen Grund (primär Kündigung) beendigt wird[11].

Enthaltene Auftragsdatenbearbeitung: Soll der Factoring-Vertrag den ihm zugedachten Zweck erfüllen, wird der Factoring-Nehmer stets Personendaten (in Form von Debitorendaten) im Besitz oder Eigentum des Auftraggebers bearbeiten müssen. Diese Bearbeitung kann dabei neben normalen Personendaten in Form von Debitorenpersonalien auch besonders schützenswerte Personendaten und/oder Persönlichkeitsprofile umfassen. Entsprechend dieser Ausgangslage findet sich in Factoring-Vereinbarungen regelmässig eine Auftragsdatenbearbeitung im Sinne von Art. 10*a* DSG.

Insbesondere bei Factoring-Vereinbarungen im Gesundheitsbereich umfasst die Auftragsdatenbearbeitung stets besonders schützenswerte Personendaten. Der Grund dafür liegt in der Art der Rechnungsstellung. So umfasst im ambulanten Gesundheitsbereich die Rechnungsstellung nach TARMED-Tarifsystem neben der Angabe des Taxpunktes und des Taxpunktwerts immer auch eine Kurzbeschreibung der damit verbundenen medizinischen Indikation[12]. Im stationären Bereich werden die verbreitet verwendeten Diagnosecodes (z.B. die DRG-Fallpauschalen) jeweils mit einer Kurzbeschreibung des damit verbundenen Vorfalls ergänzt (z.B. der DRG-Code A02Z mit der Beschreibung «Transplantation von Niere und Pankreas»)[13]. Im Weiteren weist jede Rechnung die Patientenpersonalien sowie die Personalien und den Fachbereich des behandelnden Arztes auf.

Kollektive Taggeldversicherungsverträge

Da im Rahmen von kollektiven Taggeldversicherungsverträgen verschiedene gesetzliche Grundlagen zusammenspielen (OR[14], VVG[15], UVG[16] und KVG[17]) und das Versicherungsverhältnis entweder durch Vertrag oder von Gesetz wegen entstehen kann, finden diese nachfolgend eine ausführlichere Betrachtung.

Grundlagen: Nach Art. 324a Abs. 1 OR hat der Arbeitgeber den Lohn für eine beschränkte Zeit weiterzubezahlen, wenn der Arbeitnehmer aus Gründen, die in seiner Person liegen, insbesondere Krankheit oder Unfall, an der Arbeitsleistung ohne sein Verschulden verhindert wird. Art. 324a Abs. 2 OR präzisiert diese Regelung dahingehend, dass wenn durch Abrede, Normal- oder Gesamtarbeitsvertrag nicht längere Zeitabschnitte bestimmt sind, der Arbeitgeber im ersten Dienstjahr den Lohn für drei Wochen und nachher für eine angemessene längere Zeit zu bezahlen hat. Aus der Regelung des zweiten Absatzes ergibt sich, dass es sich bei den angegebenen Zeitabschnitten lediglich um Minimalvorgaben handelt, die zugunsten des Arbeitnehmers abgeändert werden können. Da Arbeitsverhinderungen wegen Krankheit oder Unfall länger dauern können, liegt es im Interesse beider Vertragsparteien, ihr jeweiliges Risiko zu minimieren. Deshalb schliessen die Arbeitgeber dort, wo der Versicherungsschutz nicht von Gesetz wegen entsteht, regelmässig kollektive Taggeldversicherungen ab, die in der Regel eine weit über die Vorgaben von Art. 324a Abs. 2 OR hinausreichende Lohnfortzahlungspflicht vorsehen[18].

Vertragstypische Elemente: Im Rahmen eines Versicherungsvertrags übernimmt der Versicherer gegen Leistung einer Prämienzahlung ein Risiko[19]. Im Fall von kollektiven Taggeldversicherungsverträgen besteht dieses für den Fall, dass der Arbeitnehmer aufgrund von Unfall oder Krankheit unverschuldet an der Arbeitsleistung verhindert wird in der Lohnfortzahlungspflicht (vonseiten Arbeitgeber) und im Lohnausfall (vonseiten Arbeitnehmer)[20]. Da somit von einem entsprechenden Versicherungsvertrag sowohl der Arbeitgeber als auch der Arbeitnehmer profitieren, tragen diese die Prämienbeiträge teilweise gemeinsam[21]. Versicherungsnehmer ist jeweils der Arbeitgeber. Der Versicherungsvertrag ist ein Dauerschuldverhältnis und wird in der Regel durch die Kündigung einer der Parteien beendet.[22]

Im Bereich der *Unfallversicherung* ergeben sich die

Vorgaben für die inhaltliche Ausgestaltung der Versicherungsverhältnisse aus dem Bundesgesetz über die Unfallversicherung (UVG). Bei Personen, die bei der Suva[23] unfallversichert sind, entsteht das Versicherungsverhältnis im obligatorischen Bereich von Gesetz wegen und im freiwilligen Bereich mittels Vereinbarung (meist in Form von durch die Arbeitgeber abgeschlossenen Kollektivverträgen) (Art. 59 Abs. 1 UVG). Für alle anderen Versicherten schliessen die Arbeitgeber sowohl im Bereich der obligatorischen als auch der freiwilligen Unfallversicherung Kollektivverträge mit privaten Versicherungsgesellschaften ab (Art. 59 Abs. 2 UVG)[24]. Das UVG regelt, dass der Anspruch auf ein Taggeld am dritten Tag nach dem Unfalltag entsteht und bis zur Wiedererlangung der vollen Arbeitsfähigkeit, dem Beginn einer Rente oder dem Tod des Versicherten dauert (Art. 16 Abs. 2 UVG). Er beträgt 80 Prozent des versicherten Lohnes (Art. 17 Abs. 1 UVG).

Im Bereich der *Krankentaggeldversicherungen* kann ein Vertragsabschluss entweder nach dem Bundesgesetz über die Krankenversicherung (KVG) oder nach dem Bundesgesetz über den Versicherungsvertrag (VVG) erfolgen. Im Rahmen der *kollektiven* Krankentaggeldversicherung haben die Versicherungsverhältnisse nach VVG allerdings jene nach KVG weitgehend abgelöst[25]. Entsprechend beziehen sich die nachfolgenden Ausführungen lediglich auf Versicherungsverhältnisse nach VVG. In deren Rahmen ergeben sich die inhaltlichen Vorgaben nicht wie bei der Unfallversicherung aus einem spezifischen, die Krankentaggeldversicherung regelnden Gesetz, sondern diese stellen, soweit sie über Art. 324*a* OR hinausgehen, Teil der Privatautonomie dar[26]. Ergeben sich aus einem allfällig bestehenden Gesamtarbeitsvertrag keine weiterführenden Vorgaben, sehen entsprechende Versicherungsverträge regelmässig Lohnfortzahlungspflichten von mindestens 80 Prozent des versicherten Lohnes während einer Zeitdauer von 730 Tagen (abzüglich allfällig vereinbarter Wartefristen) vor[27].

Enthaltene Auftragsdatenbearbeitung: Da es sich bei der Lohnfortzahlung aufgrund von Art. 324*a* OR um eine Pflicht des Arbeitgebers handelt und dieser zu deren Erfüllung eine Versicherungsgesellschaft beizieht, lässt er einen Dritten Personendaten bearbeiten, die sich in seinem Besitz oder Eigentum befinden. Spätestens wenn sich ein Unfall ereignet oder eine Krankheit eintritt, wird der Arbeitgeber seinem Taggeldversicherer die Personalien der verunfallten oder erkrankten Person, allfällige bereits von dieser erhaltene Arztzeugnisse sowie weitere im Zusammenhang mit dem Fall stehende Informationen weiterleiten. Anschliessend übernimmt der Versicherer alle weiteren Abklärungen sowie die Berechnung und Auszahlung der Taggelder. Da sich das Bearbeiten von Personendaten aufgrund von Art. 10*a* Abs. 1 DSG sowohl durch Vereinbarung als auch Gesetz einem Dritten übertragen lässt, spielt es für das Vorliegen einer Auftragsdatenbearbeitung keine Rolle, ob das Verhältnis zur Versicherungsgesellschaft durch Gesetz (wie bei Suva versicherten Personen im Bereich der obligatorischen Unfallversicherung) oder mittels Vereinbarung (in allen anderen Fällen) begründet wird. Entsprechend liegt im Rahmen von kollektiven Taggeldversicherungsverhältnissen stets eine Auftragsdatenbearbeitung im Sinne von Art. 10*a* DSG vor.

Begutachtungs- und Beratungsverträge

Vertragstypische Elemente: Im Rahmen eines *Begutachtungsvertrags* verpflichtet sich der Berater zur Durchführung einer Analyse und zur Erstellung eines Gutachtens über die im Zusammenhang mit der Analyse bearbeiteten Sachfragen. Dazu muss er sich in einem ersten Schritt zur konkret bestehenden Problemstellung Informationen beschaffen, diese in einem zweiten Schritt analysieren und die daraus gewonnenen Erkenntnisse interpretieren sowie die Erkenntnisse abschliessend in einem schriftlichen Analysebericht (dem Gutachten) festhalten. Im Gegenzug bezahlt ihm der Beratene ein Entgelt und gewährt dem Berater im Sinne von Obliegenheiten Einsicht in die benötigten Unternehmenstatsachen und wirkt soweit notwendig aktiv mit[28].

Bei einem *Beratungsvertrag* kommen zusätzlich zu den Elementen des Begutachtungsvertrags die Ausarbeitung von Lösungsvorschlägen, die Auswahl der optimalen Lösungsvariante sowie deren Präsentation (meist) in Form eines Berichts hinzu. Entsprechend hat der Beratene die gleichen Pflichten wie beim Begutachtungsvertrag, welche insbesondere in der Pflicht zur Bezahlung eines Entgelts besteht. Je nach Sachlage kann ein Beratungsvertrag auch als Dauerschuldverhältnis ausgestaltet sein[29].

Die rechtliche Qualifizierung dieser beiden Vertragsarten gestaltet sich in der Tendenz schwierig. Das Bundesgericht hat dazu ausgeführt, entsprechende Verträge könnten sehr unterschiedliche Fragestellungen enthalten, was

eine Differenzierung der rechtlichen Einordnung erfordere. Namentlich technische Gutachten führten regelmässig zu einem Resultat, das sich nach objektiven Kriterien überprüfen und als richtig oder falsch qualifizieren lasse. Die Richtigkeit des Gutachtensergebnisses sei somit objektiv gewährleistungsfähig und könne als Erfolg versprochen werden. Deshalb stehe in Bezug auf diese Art von Gutachten einer Anwendung der werkvertraglichen Regelungen an sich nichts entgegen. Würden dagegen objektive Kriterien für die Beurteilung der Richtigkeit des Gutachtensergebnisses fehlen, könne diese weder vom Gutachter gewährleistet noch vom Auftraggeber überprüft werden. Die objektive Richtigkeit lasse sich in diesem Fall nicht als Werk versprechen, womit der Gutachter nicht einen Arbeitserfolg, sondern (lediglich) ein sorgfältiges Tätigwerden im Interesse des Vertragspartners schulde. Ein solcher Vertrag erfülle daher die Merkmale des Auftrags[30].

Die Frage nach der Qualifikation dieser Verträge hier abschliessend beantworten zu wollen, würde sowohl die umfangmässigen als auch die thematischen Vorgaben des vorliegenden Beitrags sprengen. Dessen Absicht besteht nach wie vor darin, einen Überblick über jene Vertragstypen zu geben, in deren Rahmen Auftragsdatenbearbeitungen regelmässig oder verbreitet zu finden sind. Speziell unter diesem Fokus sind die bundesgerichtlichen Darlegungen jedoch, wie sich den nachfolgenden Ausführungen entnehmen lässt, durchaus von Interesse.

Enthaltene Auftragsdatenbearbeitung: Die Ausführungen des Bundesgerichts zur Qualifikation von Begutachtungs- und Beratungsverträgen hat gezeigt, dass entsprechende Verträge eine Vielzahl an Begutachtungs- und Beratungsinhalten aufweisen können. Diese reichen von rein technischen bis zu wirtschaftlichen, rechtlichen, sozialen, medizinischen und anderen Fragestellungen. Mit Bezug auf die Auftragsdatenbearbeitung ist es somit bei Gutachten über rein technische, mathematische und ähnliche Fragestellungen, in deren Rahmen allenfalls auch ein Erfolg geschuldet sein kann, durchaus denkbar, dass der Gutachter zwar als Dritter Daten des Auftraggebers bearbeitet, dass diese aber keine Personendaten enthalten und entsprechend kein Fall einer Auftragsdatenbearbeitung im Sinne von Art. 10*a* DSG vorliegt. Dagegen ist es im Rahmen anderer Gutachtertätigkeiten, die sich z.B. auf wirtschaftliche, rechtliche, soziale, medizinische oder vergleichbare Fragestellungen beziehen und in deren Zusammenhang vonseiten des Gutachters primär ein sorgfältiges Tätigwerden im Interesse des Auftraggebers geschuldet ist, verbreitet vorstellbar, dass zur Erfüllung der vertraglichen Pflichten eine Bearbeitung von Personendaten des Auftraggebers stattfindet. In der Folge dürften Begutachtungs- und Beratungsverträge mit dieser Art von Inhalten verbreitet eine Auftragsdatenbearbeitung nach Art. 10*a* DSG aufweisen.

Softwareentwicklungs- und Softwarepflegevertrag

Vertragstypische Elemente: Gegenstand eines *Softwareentwicklungsvertrags* ist in der Regel die Entwicklung von individuellen Softwareprogrammen (Individualsoftware) für einen bestimmten Anwen-

Literatur

- Borges Georg/Schwenk Jörg (Hrsg.), Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce, Heidelberg 2012 (zit. Autor/-in in: Borges/Schwenk).
- Engels Thomas, Datenschutz in der Cloud – Ist hierbei immer eine Auftragsdatenverarbeitung anzunehmen? in: Kommunikation & Recht 9/2011, 548 ff.
- Fröhlich-Bleuler Gianni, Softwareverträge, Bern 2004.
- Fuhrer Stephan, Schweizerisches Privatversicherungsrecht, Zürich 2011.
- Hilber Marc (Hrsg.), Handbuch Cloud Computing, Köln 2014 (zit. Autor/-in in: Hilber).
- Honsell Heinrich/Vogt Nedim/Wiegand Wolfgang (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1–529 OR, 5. Auflage, Basel 2011 (zit. BSK-OR-Autor/-in).
- Honsell Heinrich, Schweizerisches Obligationenrecht, Besonderer Teil, 9. Auflage, Bern 2010.
- Huguenin Claire, Obligationenrecht, Besonderer Teil, 3. Auflage, Zürich 2008 (zit. Huguenin OR BT).
- Huguenin Claire, Obligationenrecht: Allgemeiner und besonderer Teil, Zürich 2012.
- Leuenberger Christoph, Dienstleistungsverträge in: ZSR, Band 106/2, 1987, 1 ff.
- Lutz Stefan, Vertragsrechtliche Fragen des Cloud Computing, München 2010.
- Maurer Alfred, Schweizerisches Unfallversicherungsrecht, Bern 1985.
- Maurer-Lambrou Urs/Blechta Gabor, Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 3. Auflage, Basel 2014 (zit. BSK-DSG-Autor/-in).
- Müller-Chen Markus/Girsberger Daniel/Furrer Andreas, Obligationenrecht, Besonderer Teil, Zürich 2011.
- Riemer-Kafka Gabriela, Schweizerisches Sozialversicherungsrecht, 4. Auflage, Bern 2014.
- Rusch Arnold, Erfolgsbezug bei Werkvertrag und Auftrag in: BJM 6/2013, 285 ff.
- Schmid Jörg/Stöckli Hubert, Schweizerisches Obligationenrecht, Besonderer Teil, Zürich 2010.
- Schmidt-Bens Johanna, Cloud Computing Technologien und Datenschutz, Edewecht 2012.
- Schweizerischer Fachverband für Cloud Computing, Leitfaden Cloud Computing, Risk & Compliance, Version März 2012 (zit. Leitfaden Cloud Computing), zu finden unter: <http://www.eurocloudswiss.ch/index.php/publikationen/leitfaden> (besucht am 8.8.2014).
- Straub Wolfgang, Cloud Verträge – Regelungsbedarf und Vorgehensweise in: AJP 7/2014, 905 ff.
- Tercier Pierre/Favre Pascal, Les contrats spéciaux, 4e édition, Genève 2009.
- von Kaenel Adrian (Hrsg.), Krankentaggeldversicherung: Arbeits- und versicherungsrechtliche Aspekte, Zürich 2007 (zit. Autor/-in in: von Kaenel).

der. Neben der eigentlichen Entwicklung der Software werden dabei oft zusätzliche Leistungen wie Beratung, Projektmanagement, Installation, Schulung und Ähnliches erbracht. Allerdings treten diese Leistungen gegenüber der Softwareentwicklung zurück. Ebenfalls Teil von Softwareentwicklungsverträgen stellt die lizenzrechtliche Ausgestaltung der Weiterentwicklung der Software und die Modifikation des Programmcodes durch den Anwender dar. Entsprechend handelt es sich bei Softwarepflegeverträgen in der Regel um Werkverträge mit lizenzvertrags- und auftragsrechtlichen Elementen[31].

Mit einem *Softwarepflegevertrag* soll die Gebrauchstauglichkeit sowie die Weiterentwicklung des Softwareprodukts (Individual- oder modifizierte Standardsoftware) sichergestellt werden. Der Softwarepflegevertrag kann unterschiedliche Leistungen enthalten. Diese reichen von Supportleistungen in Verbindung mit der Behebung von Softwarefehlern bis zur Anpassung und Weiterentwicklung der Software. Ein Softwarepflegevertrag wird in der Regel auf unbestimmte Zeit abgeschlossen und stellt daher ein Dauerschuldverhältnis dar. Je nach vorhandenen Leistungen weist er werkvertragliche, auftragsrechtliche und/oder lizenzvertragsrechtliche Elemente auf[32].

Enthaltene Auftragsdatenbearbeitung: Die im Rahmen von *Softwareentwicklungsverträgen* erstellte Individualsoftware wird jeweils mit Blick auf die Bedürfnisse (Geschäftsabläufe) des Anwenders massgeschneidert. Damit dies möglich ist, bedarf der Entwickler eines vertieften Einblicks in die der zu entwickelnden Software zugrunde liegenden Geschäftsprozesse. Zu diesem Zweck überlässt der Anwender dem Entwickler nicht selten ganze Datensammlungen, anhand oder aufgrund welcher dieser die Individualsoftware anschliessend entwickelt. Da diese Datensammlungen in der Regel (auch) Personendaten und/oder Persönlichkeitsprofile enthalten und der Entwickler diese zur Vertragserfüllung bearbeitet, dürften Softwareentwicklungsverträge verbreitet eine Auftragsdatenbearbeitung im Sinne von Art. 10*a* DSG beinhalten.

Bei einem *Softwarepflegevertrag* gestaltet sich die Sachlage vergleichbar. Im Rahmen der Erbringung von Supportleistungen in Verbindung mit der Behebung von Softwarefehlern sowie der Anpassung und Weiterentwicklung von Software wird sich der Dienstleistungsnehmer regelmässig vertieft mit den jeweils zugrunde liegenden Geschäftsprozessen und den damit verbundenen Datensammlungen auseinandersetzen müssen. Da diese Datensammlungen in der Regel (auch) Personendaten enthalten dürften, bearbeitet der Dienstleistungsnehmer zur Erfüllung des Softwarepflegevertrags entsprechend mitunter Personendaten, womit eine Auftragsdatenbearbeitung im Sinne von Art. 10*a* DSG vorliegt.

Cloud Computing-Verträge

Vertragstypische Elemente: Da eine einheitliche (juristische) Definition von Cloud Computing fehlt, muss der Begriff umschrieben werden. In einem umschriebenen Sinne lassen sich unter diesem unterschiedliche Erscheinungsformen von computergestützten Dienstleistungen, die über ein Netzwerk zur Verfügung gestellt werden, zusammenfassen[33]. Diesen Dienstleistungen liegt verbreitet eine komplexe Lieferkette zugrunde, an der eine Reihe rechtlich unabhängiger Leistungserbringer in Form von Subunternehmern des Hauptanbieters beteiligt sind. Oft ist es für den Anwender wenig transparent, wer welche Leistung erbringt[34].

In technischer Hinsicht finden sich drei verschiedene Formen von Cloud Computing: *Software as a Service* (SaaS), *Platform as a Service* (PaaS) und *Infrastructure as a Service* (IaaS). Entsprechend der oben dargelegten Begriffsumschreibung ist diesen drei Arten gemeinsam, dass jeweils ein Anbieter einem Anwender gegen ein Entgelt IT-Dienstleistungen über ein Netzwerk zur Verfügung stellt. Die Unterscheidung in die genannten drei Formen ergibt sich anschliessend durch die Vereinbarung der Art und Güte der Dienstleistungen.

- Bei «Software as a Service» handelt es sich um die verbreitetste Form von Cloud-Computing. Diese baut auf dem PaaS und dem IaaS auf und stellt entsprechend jene Cloud-Form dar, die dem Anwender den grössten Nutzen bringt. In deren Rahmen stellt der Anbieter dem Anwender ein in sich geschlossenes Leistungspacket zur Verarbeitung von Daten mitunter mittels Internetbrowser zur Verfügung. In der Regel erfolgt dabei beim Anwender weder eine lokale Installation von Software noch eine lokale Speicherung von Daten[35].
- Bei «Platform as a Service» stellt der Anbieter dem Anwender IT-Komponenten (bzw. eine Plattform) zur Verfügung, die zur Interaktion und Kommunikation genutzt werden können. Mit diesen kann der Anwender beispielweise eigene SaaS-Lösungen (siehe oben) entwickeln und betreiben lassen[36].
- Bei «Infrastructure as a Service» stellt der Anbieter dem

Anwender über ein Netzwerk IT-Infrastruktur zur Verfügung. Dabei kann diese Dienstleistung z.B. Ressourcen zum Betrieb eines virtuellen Systems, Speicherplatz und/oder Netzwerkbandbreite je einzeln oder in Kombination umfassen. Die Verantwortung für den Betrieb der IT-Infrastruktur verbleibt beim Anbieter. Die Installation und Nutzung des Betriebssystems sowie allfälliger Anwendungskomponenten liegt dagegen in der Verantwortung des Anwenders[37].

Enthaltene Auftragsdatenbearbeitung: Die Anwender verarbeiten im Rahmen von Cloud-Angeboten mittels der durch den Anbieter zur Verfügung gestellten IT-Dienstleistungen Daten. Der Anbieter steuert dadurch, dass er die Hoheit über die angebotenen Dienstleistungen hat, die Datenverarbeitungen und bearbeitet dadurch als Dritter Daten, die sich im Besitz oder Eigentum des Anwenders befinden. Wie im ersten Teil ausgeführt[38], ist der Begriff des Bearbeitens nach Art. 3 lit. e DSG äusserst weit gefasst und es ist dabei auch nicht von Bedeutung, ob die Personendaten während der Bearbeitung von Menschen zur Kenntnis genommen werden oder ob die Bearbeitung vollständig durch eine Maschine erfolgt. Werden zur Erfüllung einer gesetzlichen Aufgabe oder im Rahmen einer Geschäftstätigkeit somit zur Bearbeitung von Personendaten Cloud Services in Anspruch genommen, umfasst das entsprechende Cloud-Angebot eine Auftragsdatenbearbeitung im Sinne von Art. 10*a* DSG.[39].

In der Literatur finden sich Meinungen, die mit Bezug auf das Vorliegen einer Auftragsdatenbearbeitung (neben den vorgenannten Voraussetzungen) differenzieren möchten,

Fussnoten

1 Zitat von Johann Wolfgang von Goethe (1749–1832).
2 Bundesgesetz vom 19. Juni 1992 über den Datenschutz, SR 235.1.
3 Siehe dazu die Ausführungen im zweiten Teil in digma 2014, 76 ff.
4 Tercier/Favre, § 9 Rz. 428 ff.
5 Leuenberger in: ZSR 106/2, 1987, 13; Tercier/Favre, § 9 Rz. 432.
6 Siehe dazu Leuenberger in: ZSR 106/2, 1987, 13.
7 Siehe für diesen Abschnitt Honsell, 315 und 322 f; Müller-Chen/Girsberger/Furrer, Kapitel 8, Rz. 2 ff.; Schmid/Stöckli, Rz. 1877 ff.
8 Siehe für diesen Abschnitt Müller-Chen/Girsberger/Furrer, Kapitel 8, Rz. 64 f.; Schmid/Stöckli, Rz. 1952 ff.
9 Siehe für diesen Abschnitt Honsell, 337 ff.; Schmid/Stöckli, Rz. 1959 ff.
10 Siehe für diesen Abschnitt BSK-OR-Amstutz/Schluep, Einl. vor Art. 184 ff. Rz. 112 ff.; Huguenin OR BT, Rz. 1573 ff.; Müller-Chen/Girsberger/Furrer, Kapitel 12, Rz. 106 ff.
11 Siehe für diesen Abschnitt BSK-OR-Amstutz/Schluep, Einl. vor Art. 184 ff. Rz. 116 und 125; Huguenin, Rz. 3921 und 3942.
12 Siehe dazu <http://www.tarmedsuisse.ch> (besucht am 8.8.2014).
13 Siehe dazu <http://www.swissdrg.org> (besucht am 8.8.2014).
14 Bundesgesetz vom 30. März 1911 betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht), SR 220.
15 Bundesgesetz vom 2. April 1908 über den Versicherungsvertrag (VVG), SR 221.229.1.
16 Bundesgesetz vom 20. März 1981 über die Unfallversicherung (UVG), SR 832.20.
17 Bundesgesetz vom 18. März 1994 über die Krankenversicherung (KVG), SR 832.10.
18 Siehe dazu auch Müller Hans-Rudolf in: von Kaenel, 20 f. und 25.
19 Fuhrer, § 2 Rz. 2.6 f.
20 Siehe dazu auch Fierz Roland in: von Kaenel, 5.
21 Müller Hans-Rudolf in: von Kaenel, 25.
22 Fuhrer, § 2 Rz. 2.15.
23 Schweizerische Unfallversicherungsanstalt; siehe zu dieser Art. 61 ff. UVG sowie Riemer-Kafka, 335 ff.
24 Siehe zur Entstehung des Versicherungsverhältnisses in der Unfallversicherung auch Maurer, 131 ff.
25 Siehe dazu auch Eugster Gebhard in: von Kaenel, 65, sowie Müller Hans-Rudolf in: von Kaenel, 24.
26 Eugster Gebhard in: von Kaenel, 50.
27 Siehe dazu Müller Hans-Rudolf in: von Kaenel, 25, sowie als Anschauungsbeispiel die Krankentaggeldversicherung bei der AXA Winterthur unter: <https://www.axa-winterthur.ch/de/unternehmenskunden/angebote/krankentaggeldversicherung/seiten/default.aspx> (besucht am 8.8.2014).
28 Siehe für diesen Abschnitt BSK-OR-Amstutz/Schluep, Einl. vor Art. 184 ff. Rz. 304 f.; Huguenin OR BT, Rz. 1733 ff.
29 Siehe für diesen Abschnitt BSK-OR-Amstutz/Schluep, Einl. vor Art. 184 ff. Rz. 306 f.; Huguenin OR BT, Rz. 1733 ff.
30 BGE 127 III 328 E. 2c bestätigt in BGE 134 I 159 E. 3; siehe zu dieser Fragestellung auch Rusch in: BJM 6/2013, 296 f.
31 Siehe für diesen Abschnitt Fröhlich-Bleuler, Rz. 45, sowie im Weiteren Huguenin OR BT, Rz. 1667.
32 Siehe für diesen Abschnitt Fröhlich-Bleuler, Rz. 1168 ff.
33 Siehe dazu Straub in: AJP 2014, 905; Weiss Andreas in: Hilber, Teil 1A Rz. 1, sowie im Weiteren Borges Georg/Brennscheidt Kirstin in: Borges/Schwenk, 46, und Lutz, 1.
34 Siehe dazu Weiss Andreas in: Hilber, Teil 1A Rz. 39.
35 Siehe für detaillierte Ausführungen Kittlaus Hans-Bernd in: Hilber, Teil 1B Rz. 38 ff., sowie im Weiteren Schmidt-Bens, 16, und Leitfaden Cloud Computing, 14.
36 Siehe für detaillierte Ausführungen Kittlaus Hans-Bernd in: Hilber, Teil 1B Rz. 38 ff., sowie im Weiteren Schmidt-Bens, 17.
37 Siehe für detaillierte Ausführungen Kittlaus Hans-Bernd in: Hilber, Teil 1B Rz. 27 ff. sowie im Weiteren Schmidt-Bens, 17 f.
38 digma 2014, 23.
39 Siehe zu diesem Abschnitt auch Borges Georg/Brennscheidt Kirstin in: Borges/Schwenk, 62 f.; Hartung Jürgen/Storm Nicholas in: Hilber, Teil 4 Rz. 42 ff., sowie im Weiteren, aber undifferenziert BSK-DSG-Bühler/Rampini, Rz. 22d.
40 Siehe dazu Engels in: Kommunikation & Recht, 549 f.; Meinung übernommen von Hansen Marit in: Borges/Schwenk, 87 f., sowie für das schweizerische Recht, aber in der Sache unklar: Straub in: AJP 7/2014, 912 f.

ob der Einsatz von Cloud-Anwendungen allein durch den Anwender erfolgt, ohne dass der Anbieter eigene Aufgaben (die über die Bereitstellung und Aufrechterhaltung der IT-Dienstleistungen hinausgehen) übernimmt, oder ob der Anbieter eigene (weiter gehende) Leistungen wie etwa das Anfertigen und Aufbewahren von Sicherheitskopien erbringt. Nach dieser Auffassung liegt eine Auftragsdatenbearbeitung nur im zweiten Fall vor[40]. Diese Idee erscheint jedoch aus zweierlei Gründen nicht zielführend. Einerseits dürften sich bei einem solchen Vorgehen im Einzelfall regelmässig Abgrenzungsschwierigkeiten ergeben. Andererseits bearbeitet der Anbieter, wie oben ausgeführt, dadurch, dass er die Hoheit über die zur Verfügung gestellten IT-Dienstleistungen hat und damit die Datenverarbeitungen steuert (inkl. der in deren Rahmen stattfindenden Bearbeitung von Personendaten), in jedem Fall Daten, die sich im Besitz oder Eigentum des Nutzers befinden. Entsprechend kann auch im ersten Fall das Vorliegen einer Auftragsdatenbearbeitung bejaht und auf eine Differenzierung im dargelegten Sinne verzichtet werden.

Besseres Sehen durch besseres Wissen

Wie die obigen Ausführungen zeigen, finden sich im Rahmen von Dienstleistungsverträgen aufgrund ihrer inhaltlichen Ausgestaltung verbreitet Auftragsdatenbearbeitungen im Sinne von Art. 10*a* DSG. Entsprechend wichtig ist es, dass sich die Parteien einerseits bewusst sind, dass sie in einem konkreten Fall einen Dienstleistungsvertrag abschliessen und andererseits, dass sich im Rahmen von Dienstleistungsverträgen verbreitet Auftragsdatenbearbeitungen finden. Die datenschutzkonforme Vertragsausgestaltung hängt im Einzelfall somit entscheidend davon ab, dass die Vertragsparteien entsprechend dem Eingangszitat aufgrund von Wissen sehen und ihr Handeln in der Folge danach ausrichten.

Liegt ein Dienstleistungsvertrag, der eine Auftragsdatenbearbeitung umfasst, vor, gilt es in Bezug auf dessen inhaltliche Ausgestaltung gewisse risikotreibende Faktoren zu beachten. Worin diese bestehen und welche Auswirkungen sich daraus für die Vertragsgestaltung ergeben, bildet Gegenstand des nächsten Beitrags der Artikelreihe zur Auftragsdatenbearbeitung in digma 2014.4. ■

Rechtsprechung

Öffentlichkeitsprinzip oder Auskunftsrecht?

Dominika Blonski, MLaw, Auditorin beim Datenschutzbeauftragten des Kantons Zürich, Zürich
dominika.blonski@dsb.zh.ch

Urteil des Bundesgerichts vom 4. März 2014 (1C_780/2013) sowie Urteil des Verwaltungsgerichts des Kantons Zürich vom 4. September 2013 (VB.2012.00510). Einsichtsrecht in ein Protokoll des Spitalrats (Art. 13 und 16 BV, Art. 10 und 17 KV/ZH, §§ 20 und 23 IDG/ZH)

Sachverhalt

Der Oberarzt X. wurde von der Spitaldirektion des Universitätsspitals Zürich (USZ) im Amt eingestellt und schliesslich freigestellt. Die dagegen erhobenen Rechtsmittel hiess der Spitalrat des USZ und danach auch das Verwaltungsgericht des Kantons Zürich gut. In der Folge ersuchte X. um Zugang zu seinen eigenen Personendaten. Er erhielt dabei Einsicht in ein Sitzungsprotokoll des Spitalrats vom 15. Dezember 2010. In erwähnter Sitzung wurde unter anderem die Situation betreffend X. sowie das Vorgehen für künftige vergleichbare Fälle besprochen. Für die Einsichtsgewährung waren die Namen der an der Sitzung beteiligten Personen eingeschwärzt und somit für X. nicht erkennbar. Darauf verlangte X., dass ihm vollständige Einsicht in das Protokoll ohne Unkenntlichmachung der Namen und mit allen Beilagen gewährt werde. Ausserdem solle ihm mitgeteilt werden, wer das Protokoll erstellt habe, wer für dessen Richtigkeit und Vollständigkeit verantwortlich sei, welche Personen an der Sitzung anwesend gewesen seien und wer das Protokoll mit den Beilagen erhalten habe. Der Spitalrat wies dieses Begehren mit der Begründung ab, seine Aufsichtsfunktion werde mit der Offenlegung gefährdet. Zudem stünden Interessen Privater entgegen, denen die Vertraulichkeit ihrer Auskünfte zugesichert worden war. Das Verwaltungsgericht des Kantons Zürich hiess die dagegen erhobene Beschwerde teilweise gut. Damit wurde der Spitalrat angewiesen, X. vollständig Einsicht in das Sitzungsprotokoll zu gewähren mit der Ausnahme eines Namens, weil entsprechende Person Personenschutz beantragt hatte und ihr daher vorgängig die Gelegenheit zur Stellungnahme einzuräumen sei. Zudem müsse er X. mitteilen, wer an fraglicher Sitzung anwesend war. Die weiteren Rechtsbegehren wurden wegen Gegenstandslosigkeit abgeschrieben, weil ihnen bereits nachgekommen worden war. Gegen diesen Entscheid wandte sich der Spitalrat ans Bundesgericht, welches auf die Beschwerde in öffentlich-rechtlichen Angelegenheiten mangels Beschwerdelegitimation des Spitalrats nicht eintrat. Das Bundesgericht sprach dem Entscheid insbesondere die präjudizielle Bedeutung ab.

Erwägungen des Verwaltungsgerichts

Das Verwaltungsgericht des Kantons Zürich hielt im vorinstanzlichen Entscheid zunächst fest, dass das Protokoll der Spitalratssitzung Angaben zur Person des X. und somit Personendaten im Sinne des § 3 [Abs. 3] IDG/ZH[1] enthalte. Als Anstalt des kantonalen öffentlichen Rechts mit eigener Rechtspersönlichkeit, die mit der Erfüllung öffentlicher Aufgaben betraut ist (§§ 1 und 3 USZG/ZH[2]), stelle das USZ ein öffentliches Organ im Sinne von § 2 Abs. 1 Satz 1 i.V.m. § 3 [Abs. 1] lit. c IDG/ZH dar. Das IDG/ZH sei folglich anwendbar (E. 3.1 und 3.2).

Weiter führte es aus, dass der Anspruch auf Zugang zu den eigenen Personendaten gemäss § 20 Abs. 2 IDG/ZH auch die Information darüber umfasse, woher die Daten stammen. Im konkreten Fall bestehe folglich grundsätzlich Anspruch auf Bekanntgabe der im Sitzungsprotokoll festgehaltenen Namen der über X. sprechenden Personen (E. 3.3). Eine Verweigerung oder Aufschiebung der Informationsbekanntgabe sei gemäss § 23 Abs. 1 IDG/ZH möglich, wenn eine rechtliche Bestimmung, ein überwiegendes öffentliches oder privates Interesse entgegenstehe.

Das Verwaltungsgericht prüfte die im erwähnten Artikel festgehaltenen möglichen Einschränkungsgründe und kam zum Schluss, dass erstens das Organisationsregle-

ment des Spitalrats des USZ (OR SR) als bloss internes Reglement keine ausreichende rechtliche Bestimmung im Sinne von § 23 Abs. 1 IDG/ZH darstelle und daher die in dessen § 13 geregelte Verschwiegenheitspflicht der Spitalratsmitglieder und Sitzungsteilnehmer der Einsicht nicht entgegenstehe (E. 3.5).

Bezüglich des Vorliegens von überwiegenden öffentlichen Interessen hielt das Verwaltungsgericht zweitens fest, dass weder der Meinungsbildungsprozess des öffentlichen Organs (§ 23 Abs. 2 lit. b IDG/ZH) noch die zielkonforme Durchführung konkreter behördlicher Massnahmen (§ 23 Abs. 2 lit. e IDG/ZH) beeinträchtigt werde (E. 3.6). Es liege hier kein direkter Zusammenhang mit einem noch nicht abgeschlossenen Meinungsbildungsprozess vor. Zudem könne X. die Aussagen über seine Person nur zuordnen, wenn er auch wisse, von wem sie stammen. Der Argumentation des Spitalrats, die Sitzungsteilnehmer seien vor rechtlichen Angriffen aufgrund ihrer Äusserungen zu schützen, folgte das Verwaltungsgericht nicht, denn die Beratungen dürften nicht zu rechtsfreiem Raum erklärt werden. Hier überwiege das verfassungsmässige Recht von X. Im Ergebnis liege folglich kein überwiegendes öffentliches Interesse vor, das der Bekanntgabe der Namen im Protokoll entgegenstehen würde.

Im Hinblick auf das überwiegende private Interesse kam das Verwaltungsgericht drittens zum Schluss, dass die Spitalratsmitglieder nicht in ihrer Privatsphäre betroffen seien, wenn ihre Namen bekannt gegeben werden (E. 3.7). Sie würden sich im Rahmen ihrer Funktion äussern. Daher komme § 23 Abs. 3 IDG/ZH nicht zum Zug. Das Verwaltungsgericht äusserte sich zudem zu zwei Spezialfällen. In einem Fall wurde das Gefahrenpotenzial von X. bezüglich einer der im Protokoll mit Namen erscheinenden Person abgeklärt. In diesem Fall gelte dasselbe wie für die anderen Sitzungsteilnehmer und es bestehe kein Grund zur Einschränkung. Zu einem anderen Ergebnis kam das Gericht in Bezug auf die Person, die Personenschutz für ihre Familie beantragt hatte, was im Sitzungsprotokoll erwähnt wird. Diese Information sei geeignet, die Privatsphäre zu beeinträchtigen. Daher müsse der betroffenen Person vor Bekanntgabe ihres Namens Gelegenheit zur Stellungnahme gemäss § 26 Abs. 1 IDG/ZH eingeräumt werden. Damit stehen im Ergebnis auch keine überwiegenden privaten Interessen entgegen und der Spitalrat müsse X. Einsicht in das Protokoll mit erkennbaren Namen gewähren, mit Ausnahme des Namens der Person, die Personenschutz beantragt hatte.

Den Rechtsbegehren, X. sei Einsicht in sämtliche Beilagen zum Protokoll zu gewähren, es sei ihm mitzuteilen, wer das Protokoll erstellt hat, wer für dessen Richtigkeit und Vollständigkeit zuständig ist und wer davon Kenntnis erhalten hat, wurde nachgekommen, weshalb sie wegen Gegenstandslosigkeit abzuschreiben seien (E. 4 und 5). Der Spitalrat müsse X. jedoch gestützt auf § 18 Abs. 3 lit. b IDV/ZH[3] bekannt geben, wer an der Sitzung anwesend war (E. 5).

Erwägungen des Bundesgerichts

Das Bundesgericht trat aufgrund mangelnder Beschwerdelegitimation des Spitalrats als Beschwerdeführer nicht auf die Beschwerde in öffentlich-rechtlichen Angelegenheiten ein. Es ging von der Anwendbarkeit der allgemeinen Norm in Art. 89 Abs. 1 des Bundesgerichtsgesetzes[4] aus und stellte in Frage, ob der Spitalrat gestützt auf diese Norm zur Beschwerde legitimiert sei. Dies wäre der Fall, wenn er durch den angefochtenen Entscheid besonders berührt ist und ein schutzwürdiges Interesse an dessen Aufhebung oder Änderung hat (Art. 89 Abs. 1 lit. b und c BGG). Obwohl diese Norm vordergründig auf Privatpersonen Anwendung finde, können auch Gemeinwesen gestützt darauf beschwerdeberechtigt sein, wenn sie «durch einen Entscheid gleich oder ähnlich wie ein Privater oder aber in spezifischer Weise in der Wahrung [ihrer] hoheitlichen Aufgaben betroffen [werden] und nicht bloss das allgemeine Interesse an der richtigen Rechtsanwendung geltend [machen]» (E. 3). Weil der Spitalrat nicht wie eine Privatperson betroffen sei, prüfte das Bundesgericht, ob der Entscheid eine erhebliche Betroffenheit für den Beschwerdeführer in wichtigen öffentlichen Interessen bewirke. Dies werde bejaht, wenn «einem Entscheid präjudizielle Be-

Kurz&bündig

Der Spitalrat des USZ muss die Namen der an einer Sitzung sprechenden Personen der davon betroffenen Person bekannt geben. Auch die Namen der an der Sitzung anwesenden Personen müssen mitgeteilt werden. Dieser Anspruch ergibt sich aus dem datenschutzrechtlichen Zugangsrecht zu eigenen Personendaten. Der Vergleich der Spitalratsmitglieder mit Richtern missglückt, da das Justizöffentlichkeitsprinzip nicht auf das Protokoll der Spitalratssitzung anwendbar ist. Der Spitalrat handelt nicht als Spruch-, sondern als Führungsorgan, womit kein Gerichtsurteil vorliegt. Das Justizöffentlichkeitsprinzip sichert die Kenntnis des Spruchkörpers als Ganzes und gewährt nicht die Zuteilung der einzelnen Aussagen zur sprechenden Person.

deutung für die öffentliche Aufgabenerfüllung zukommt» (E. 3).

Dabei stellte das Bundesgericht zunächst fest, dass die Art und Weise, wie das Öffentlichkeitsprinzip gemäss Art. 17 der Kantonsverfassung[5] in der Spitalaufsicht verwirklicht werde, wichtige öffentliche Interessen im Bereich der hoheitlichen Staatstätigkeit betreffe. Zudem sei für die Bejahung der Legitimation vorausgesetzt, dass der angefochtene Entscheid den Beschwerdeführer bei der Aufgabenerfüllung in erheblicher Weise berühre. Der Spitalrat argumentierte, die Bekanntgabe der anonymisierten Namen störe seinen Meinungsbildungsprozess, weil unsachlicher Druck von aussen auf die Mitglieder entstehe und die Gefahr von unbegründeten zivil- und strafrechtlichen Klagen bestünde sowie noch hängige oder zu erwartende Rechtsstreitigkeiten mit dem Beschwerdegegner erschwert würden. Dem entgegnete das Bundesgericht, dass das Öffentlichkeitsprinzip dies naturgemäss mit sich bringe und keine legitimationsbegründende besondere Betroffenheit darstelle. An dieser Stelle nahm das Bundesgericht auf seine neuere Rechtsprechung zu Richterinnen und Richtern Bezug und hielt fest, dass für die Mitglieder des Spitalrats dasselbe gelte. «[D]ie mit dem Öffentlichkeitsgrundsatz verbundene Kontrollfunktion durch die Rechtsgemeinschaft [wäre] massgeblich beeinträchtigt oder gar illusorisch […], wenn die an einem Entscheid beteiligten Richter unbekannt bleiben könnten. Richter und Richterinnen übten ein öffentliches Amt aus und hätten für die von ihnen gefällten Urteile einzustehen und sich allfälliger Kritik zu stellen. […] [D]ie Sitzungsteilnehmer [bewegten sich] nicht im rechtsfreiem Raum […] und [bedürften] keines besonderen Schutzes vor allfälligen rechtlichen Schritten der von den Äusserungen betroffenen Personen […]. […] Behördenmitglieder [sollten sich] nicht von unsachlichem Druck von aussen beeinflussen lassen» (E. 3). Die Bekanntgabe der Namen der Sitzungsteilnehmer könne folglich die Funktionsfähigkeit des Spitalrats nicht ernsthaft beeinträchtigen. Aufgrund des Präjudizes fehle es im Ergebnis deshalb an der erheblichen Betroffenheit des Spitalrats, weshalb das Bundesgericht nicht auf die Beschwerde eintrete.

Obwohl das Bundesgericht aus formellen Gründen nicht auf die Beschwerde eintrat, hielt es damit im Ergebnis materiell fest, dass die Vorinstanz zu Recht die Bekanntgabe der Namen der Sitzungsteilnehmer angewiesen hat. Nach diesem bundesgerichtlichen Entscheid ist das Urteil des Verwaltungsgerichts[6] rechtskräftig.

Bemerkungen

Die sich stellende Frage im vorliegenden Verfahren und damit der Streitgegenstand betrifft den Umfang der Einsicht in das Protokoll der besagten Spitalratssitzung. Reicht eine Einsicht in das Protokoll mit abgedeckten Namen der jeweils sprechenden Personen oder müssen die Namen auch bekannt gegeben werden?

Grundlage des Zugangsanspruchs

Sowohl das Verwaltungsgericht als auch das Bundesgericht kommen richtigerweise zum Schluss, dass die Namen der an der Sitzung des Spitalrats sprechenden Personen dem X. bekannt gegeben werden müssen. Die Begründung ist jedoch eine unterschiedliche. Das Verwaltungsgericht ging vom Zugangsanspruch zu eigenen Personendaten gemäss § 20 Abs. 2 IDG/ZH aus, prüfte die Zulässigkeit der Einschränkung dieses Rechts und sah keinen Einschränkungsgrund (§ 23 IDG/ZH: rechtliche Bestimmung, überwiegendes öffentliches oder privates Interesse) gegeben. Das Bundesgericht zog hingegen bei der Prüfung der Beschwerdeberechtigung das Öffentlichkeitsprinzip bei, dessen Kernstück der Anspruch auf Zugang zu bei einem öffentlichen Organ vorhandenen Informationen gemäss § 20 Abs. 1 IDG/ZH darstellt.

Die beiden erwähnten Zugangsansprüche zu Informationen sind zu unterscheiden. Einerseits ergibt sich der allgemeine Zugangsanspruch zu Informationen gemäss § 20 Abs. 1 IDG/ZH aus dem verfassungsrechtlich verankerten Öffentlichkeitsprinzip (Art. 17 KV/ZH), welcher der Transparenz des Handelns der öffentlichen Organe dient. Das Ziel des Öffentlichkeitsprinzips ist die Förderung der freien Meinungsbildung, die Förderung der Wahrnehmung der demokratischen Rechte sowie die Erleichterung der Kontrolle staatlichen Handelns. Neben der proaktiven Informationstätigkeit des öffentlichen Organs (gemäss § 14 IDG/ZH) besteht somit auch eine reaktive Informationstätigkeit, das heisst die Information auf Verlangen einer beliebigen Person (gemäss § 20 Abs. 1 IDG/ZH). Der allgemeine Zugangsanspruch umfasst alle (fertiggestellten) Informationen, die bei einem öffentlichen Organ vorhanden sind[7]. Andererseits ist auch der Zugangsanspruch zu den eigenen Personendaten gemäss § 20 Abs. 2 IDG/ZH bereits auf Verfassungsstufe verankert (Art. 13 Abs. 2 BV[8], Art. 10 KV/ZH) und stellt als

Verwirklichung grundrechtlicher Garantien den eigentlichen datenschutzrechtlichen Anspruch dar. Grundlage der Ausübung des informationellen Selbstbestimmungsrechts ist die Kenntnis um die Bearbeitung eigener Personendaten. Der Zugangsanspruch zu eigenen Personendaten soll den Schutz der betroffenen Person in ihren Persönlichkeits- und Grundrechten gewährleisten. Er umfasst den Zugang zu allen Personendaten über die gesuchstellende Person und ist insofern enger, als er nur von der betroffenen Person geltend gemacht werden kann[9]. Die beiden Zugangsansprüche unterscheiden sich insbesondere im Ausgang der Interessenabwägung gemäss § 23 IDG/ZH in einem konkreten Fall.

In der Sitzung des Spitalrats wurde über X. gesprochen. Damit enthält das Sitzungsprotokoll Angaben, die sich auf X. beziehen, und folglich Personendaten. Weil sich die Angaben auf ihn selber beziehen, handelt es sich um seine eigenen Personendaten, womit vor dem Verwaltungsgericht zu Recht der Anspruch auf Zugang zu den eigenen Personendaten gemäss § 20 Abs. 2 IDG/ZH Gegenstand war. Als Grundlage für die Ausübung des informationellen Selbstbestimmungsrechts sowie für den Schutz der betroffenen Person in ihren Persönlichkeits- und Grundrechten muss X. zugänglich gemacht werden, wer was über ihn gesagt hat. Die an der Sitzung gemachten Aussagen über ihn lassen sich nur einordnen, wenn ihm auch bekannt ist, von wem sie stammen. Erst daraus ergibt sich für X. die Möglichkeit, allenfalls weitere Rechte wie Berichtigungsansprüche geltend zu machen. Wäre das Zugangsgesuch von einem Dritten und damit gestützt auf das allgemeine Zugangsrecht (gemäss § 20 Abs. 1 IDG/ZH) gestellt worden, hätte die Interessenabwägung wohl zu einem anderen Ergebnis geführt. Dabei wären wahrscheinlich die Passagen des Protokolls, in denen über X. gesprochen wurde, abgedeckt worden, weil die privaten Interessen des X. überwogen hätten. Dies zeigt auf, dass je nach Grundlage – allgemeiner Zugangsanspruch oder Zugangsanspruch zu eigenen Personendaten – die Interessenabwägung zu verschiedenartigen Ergebnissen führen und daher ein unterschiedlicher Umfang der Einsichtsgewährung resultieren kann. Auf diese bedeutende Unterscheidung der beiden Zugangsrechte ist das Bundesgericht nicht eingegangen.

Spitalratsmitglieder als Richter?

Das Bundesgericht zieht ein kürzlich ergangenes Urteil (BGE 139 I 129) über die Bekanntgabe der Zusammensetzung des Spruchkörpers als Präjudiz bei und verneint damit die besondere Betroffenheit und hiermit die Beschwerdelegitimation des Spitalrats. Gegenstand des Urteils, worauf sich das Bundesgericht bezieht, war die Frage, ob einem Journalist vollständige Einsicht einschliesslich der namentlichen Nennung der Zusammensetzung des Spruchkörpers in ein nur auszugsweise publiziertes Urteil der ehemaligen Asylrekurskommission gewährt werden solle. Das Bundesgericht prüfte dies auf der Grundlage des gemäss Art. 30 Abs. 3 BV vorgesehenen Prinzips der Justizöffentlichkeit.

Das zu den verfassungsrechtlichen Verfahrensgarantien gehörende Prinzip der Justizöffentlichkeit soll den Einblick in die Rechtspflege sowie die Transparenz von gerichtlichen Verfahren sicherstellen. Es geht einerseits um den Schutz der Parteien bezüglich ihrer korrekten Behandlung und gesetzmässigen Beurteilung. Andererseits wird die Nachvollziehbarkeit der Führung von Verfahren, der Verwaltung des Rechts sowie der Ausübung der Rechtspflege für nicht am Verfahren beteiligte Dritte ermöglicht, womit schliesslich die demokratische Kontrolle durch die Rechtsgemeinschaft sichergestellt wird (BGE 139 I 129 E. 3.3). Weil die rechtmässige Zusammensetzung des Spruchkörpers (gemäss Art. 30 Abs. 1 BV, der besagt, dass jede Person einen Anspruch auf ein durch Gesetz geschaffenes, zuständiges, unabhängiges und unparteiisches Gericht habe) zudem nur mit dessen Namensnennung nachvollzogen werden könne (BGE 139 I 129 E. 3.6), hält das Bundesgericht im Ergebnis fest, dass dem Journalisten vollständige Einsicht in das Urteil einschliesslich der Zusammensetzung des Spruchkörpers gewährt werden müsse.

Das Bundesgericht kam im Urteil bezüglich Spitalrat zum Schluss, dass dasselbe für die Mitglieder des Spitalrats gelte und dass das Öffentlichkeitsprinzip entsprechend im Bereich der Spitalaufsicht zu verwirklichen sei. Dieser Argumentation ist aus zwei Gründen nicht zu folgen.

Das Justizöffentlichkeitsprinzip gemäss Art. 30 Abs. 3 BV ist auf Gerichtsurteile anwendbar[10]. Darin liegt der erste Unterschied zum Sitzungsprotokoll des Spitalrats, welches kein Urteil darstellt. Der Spitalrat handelte in der fraglichen Sitzung nicht als Spruchorgan.

Der Spitalrat erfüllt verschiedene Aufgaben, die im USZG/ZH umschrieben und

im Statut des Universitätsspitals[11] konkretisiert werden. Der Spitalrat ist oberstes Führungsorgan und verantwortlich für die Erfüllung der kantonalen Leistungsaufträge (§ 11 Abs. 1 und 2 USZG/ZH). Dabei ist er unter anderem zuständig für Verträge der Zusammenarbeit mit Hochschulen, den Entwicklungs- und Finanzplan, den Geschäftsbericht, die Unternehmensstrategie sowie die Ernennung der Spitaldirektion und von Klinikdirektoren (§ 11 Abs. 3 Ziff. 2, 4, 5, 8, 10 und 11 USZG/ZH). Er übt ausserdem die Aufsicht über die mit der Geschäftsführung betrauten Personen aus und ist Rekursinstanz gegen Anordnungen der Spitaldirektion (§ 11 Abs. 3 Ziff. 12 und 13 i.V.m. § 29 Abs. 1 USZG/ZH, § 21 USZ-Statut/ZH). Zudem hat der Spitalrat unter anderem ein Personalreglement[12] erlassen (§ 5 lit. d Ziff. 1 USZ-Statut i.V.m. § 11 Abs. 3 Ziff. 7 USZG/ZH), womit ihm auch rechtssetzende Befugnisse zustehen. Bezüglich personalrechtlicher Fragen ist der Spitalrat zuständig für die Ernennung und Entlassung von bestimmtem Personal (Mitglieder Spitaldirektion sowie Klinik- und Institutsdirektoren) sowie die Anstellung von seinem eigenen Personal (§ 2 lit. a, b und d PR-USZ/ZH). Diese Zusammenstellung zeigt die Vielfalt der Aufgaben des Spitalrats und damit seine unterschiedlichen Funktionen als Führungsorgan, rechtssetzendes Organ, Aufsichtsorgan als auch als Spruchkörper im Sinne einer Rekursinstanz auf.

Der Spitalrat nahm im vorliegenden Fall die Sitzung vom 15. Dezember 2010 als Führungsorgan wahr, indem er über personelle Grundsatzfragen betreffend X. und das Vorgehen in ähnlichen Fällen diskutierte. Unter diesen Umständen ist die Aufgabenerfüllung des Spitalrats im konkreten Fall nicht mit jener eines Richtergremiums vergleichbar. Wäre vorliegend ein Entscheid, den der Spitalrat in seiner Funktion als Rekursinstanz gegen Entscheide der Spitaldirektion gefällt hätte, Gegenstand des Verfahrens gewesen, könnte die Rechtsprechung zur Öffentlichkeit der Namen der an einem Entscheid beteiligten Richterinnen und Richter analog auf die Spitalratsmitglieder angewandt werden. Damit handelte der Spitalrat entgegen der Argumentation des Bundesgerichts nicht als Spruchorgan. Das Bundesgericht lässt ausser Acht, dass dem Spitalrat verschiedene Aufgaben zukommen und daher kein pauschaler Vergleich der Spitalratsmitglieder mit Richtern möglich ist.

Aus dem Justizöffentlichkeitsprinzip ergibt sich der Anspruch auf Kenntnis des Spruchkörpers als Gremium. Darin findet sich der zweite Unterschied zum Einsichtsbegehren des X. in das Sitzungsprotokoll des Spitalrats, weil er nicht nur die Zusammensetzung des Spitalrats und damit die Sitzungsteilnehmer wissen, sondern auch die genaue Zuordnung der Aussagen zur jeweils sprechenden Person erfahren möchte. Sein Hauptbegehren, zu erfahren, wer was über ihn gesagt hat, unterscheidet sich von der Kenntnisnahme eines Richtergremiums, welches als Kollegium einen Entscheid gefällt hat. Aus dem Justizöffentlichkeitsprinzip ergibt sich kein Anspruch darauf, die einzelnen Voten der beteiligten Richter zu erfahren, weil die Beratungen des Gerichts nicht darunter fallen[13]. Die verfassungsrechtliche Verfahrensgarantie geht insofern weniger weit. Folglich kann die beigezogene Rechtsprechung auf das Hauptbegehren des X. nicht angewandt werden. Das Präjudiz kommt somit nur in Bezug auf das Begehren des X. zur

Fussnoten

1 Gesetz (des Kantons Zürich) vom 12. Februar 2007 über die Information und den Datenschutz (IDG), LS 170.4 (zitiert: IDG/ZH).
2 § 1 und 3 des Gesetzes (des Kantons Zürich) vom 19. September 2005 über das Universitätsspital Zürich, (USZG), LS 813.15 (zitiert: USZG/ZH).
3 Verordnung (des Kantons Zürich) vom 28. Mai 2008 über die Information und den Datenschutz (IDV), LS 170.41 (zitiert: IDV/ZH).
4 Bundesgesetz vom 17. Juni 2005 über das Bundesgericht (Bundesgerichtsgesetz, BGG), SR 173.110.
5 Verfassung des Kantons Zürich vom 27. Februar 2005, LS 101 (zitiert: KV/ZH).
6 Urteil des Verwaltungsgerichts des Kantons Zürich vom 4. September 2013 (VB.2012.00510).
7 Beat Rudin in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich IDG, Zürich/Basel/Genf 2012, § 20 N 7 ff.
8 Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV), SR 101.
9 Beat Rudin (Fn. 7), § 20 N 22 ff.
10 Ulrich Häfelin/Walter Haller/Helen Keller, Schweizerisches Bundesstaatsrecht, 8. Aufl., Zürich/Basel/Genf 2012, Rn. 856; Gerold Steinmann in: Bernhard Ehrenzeller/Philippe Mastronardi/Rainer J. Schweizer/Klaus A. Vallender (Hrsg.), Die Schweizerische Bundesverfassung. Kommentar, 2. Aufl., Zürich/Basel/Genf/St. Gallen 2008, Art. 30 Rn. 30; Jörg Paul Müller/Markus Schefer, Grundrechte in der Schweiz. Im Rahmen der Bundesverfassung, der EMRK und der UNO-Pakte, 4. Aufl., Bern 2008, 966 f.
11 Statut des Universitätsspitals Zürich vom 10. Februar 2010 (USZ-Statut/ZH), LS 813.151 (zitiert: USZ-Statut/ZH).
12 Personalreglement des Universitätsspitals Zürich vom 19. November 2008 (PR-USZ/ZH), LS 813.152 (zitiert: PR-USZ/ZH).
13 Ulrich Häfelin/Walter Haller/Helen Keller (Fn. 10), Rn. 856; Gerold Steinmann (Fn. 10), Art. 30 Rn. 32; Jörg Paul Müller/Markus Schefer (Fn. 10), 970.

Anwendung, die Sitzungsteilnehmer zu kennen.

Zusammenfassend lässt sich festhalten, dass sowohl das Verwaltungsgericht wie auch das Bundesgericht zu Recht die Bekanntgabe der Namen der an der Sitzung des Spitalrats über X. sprechenden Personen im Sitzungsprotokoll bejahten. Dabei ergibt sich dieser Anspruch gemäss Verwaltungsgericht richtigerweise aus dem datenschutzrechtlichen Zugangsrecht zu eigenen Personendaten. Beim Vergleich der Spitalratsmitglieder mit Richtern durch das Bundesgericht stellt sich heraus, dass das Justizöffentlichkeitsprinzip nicht ohne Weiteres auf das Protokoll der Spitalratssitzung anwendbar ist. Erstens handelt der Spitalrat nicht als Spruch-, sondern als Führungsorgan, womit kein Gerichtsurteil vorliegt. Zweitens sichert das Justizöffentlichkeitsprinzip die Kenntnis des Spruchkörpers als Ganzes und gewährt nicht die im vorliegenden Fall geforderte Zuteilung der einzelnen Aussagen zur Person, die sie jeweils gemacht hat. Damit können Spitalratsmitglieder nicht Richterinnen und Richtern gleichgestellt werden. ■

Der Blick nach Europa und darüber hinaus

Im Notfall «eCall» und alles wird gut!

Barbara Widmer, lic. iur., LL.M., CIA, Juristische Mitarbeiterin beim Datenschutzbeauftragten des Kantons Basel-Stadt, Basel barbara.widmer@dsb.bs.ch

Stellen Sie sich vor, es geschieht ein Autounfall und keiner geht hin. Genau dies soll es, geht es nach der Europäischen Union (EU), in Zukunft nicht mehr geben. Sie hat zu diesem Zweck eine neue Verordnung[1] ausgearbeitet, wonach ab Oktober 2015 alle neuen Fahrzeuge der Klassen «Personenkraftwagen» und «leichte Nutzfahrzeuge» mit einem bordeigenen eCall-System ausgerüstet werden müssen. Dieses soll bei einem schweren Unfall, der sich auf dem Gebiet der Union ereignet, automatisch einen eCall-Notruf über die europaweite Notrufnummer 112 auslösen[2]. Zu diesem Zweck wird das eCall-System mit verschiedenen Sensoren und Sicherheitstechniken des Fahrzeugs (z.B. dem Airbag) verbunden. Erfährt das Fahrzeug einen Aufprall einer gewissen Stärke, sendet dieses automatisch den Unfallzeitpunkt, den Standort, die Fahrtrichtung sowie den Fahrzeugtyp an eine Zentrale und stellt eine Sprechverbindung über die Notrufnummer 112 her[3]. Das System soll sich gemäss der aktuellen Verordnungsregelung nur im Fall, dass ein Unfall eintritt, aktivieren und Daten aufzeichnen. Der Notruf kann auch von Hand ausgelöst werden, jedoch soll es keine Möglichkeit geben, diesen auszuschalten[4]. Die Nutzung des eCall-Systems wird somit von Rechts wegen vorgeschrieben.

Die EU erhofft sich, durch das eCall-System eine Verringerung der Schwere der Verletzungen und der Todesopfer sowie der durch Verkehrsunfälle verursachten Staukosten und der strasseneigenen Notrufinfrastrukturkosten zu erreichen. Im Weiteren soll dieses zu einer Erleichterung der Arbeit der Notrufdienste und einer erhöhten Sicherheit der Rettungskräfte führen[5].

Personendaten

Obwohl die Idee eines solchen eCall-Systems auf den ersten Blick bestechend wirkt, darf sie nicht darüber hinwegtäuschen, dass ein solches System aus datenschutzrechtlicher Sicht problematisch ist. Erstens, weil die im Notfall gesendeten Daten spätestens mit der Herstellung der Sprechverbindung über die Notrufnummer 112 zu personenbezogenen Daten werden, zweitens, weil die Gefahr besteht, dass das System mehr Daten aufzeichnet, als für den Notfall notwendig sind, und drittens, weil sich eine Verwendung der gespeicherten Daten zu anderen als den angegebenen Zwecken (z.B. zur Auswertung des Fahrverhaltens im Hinblick auf den Abschluss von Versicherungsverträgen oder zur Auswertung des Unfallhergangs) nicht ausschliessen lässt[6].

Grundrechtseingriff

Da das eCall-System somit zu einer datenschutzrechtlich relevanten Bearbeitung von Personendaten führt, ist zu prüfen, inwiefern diese Bearbeitung allenfalls einen unzulässigen Eingriff in das Grundrecht des Schutzes der eigenen Personendaten (Art. 8 GRCh[7]) darstellt. Nach diesem hat jede Person das Recht auf Schutz der sie betreffenden Daten.

Zulässig ist ein entsprechender Eingriff, wenn die von der Datenbearbeitung betroffenen Personen in die Datenbearbeitung eingewilligt haben (Art. 8 Abs. 2 GRCh). Ansonsten ist ein Eingriff nur zulässig, wenn dieser

- gesetzlich vorgesehen ist,
- den Wesensgehalt dieser Rechte und Freiheiten achtet,
- verhältnismässig ist und
- den von der Union anerkannten, dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entspricht (Art. 52 Abs. 1 GRCh)[8].

Zum Erfordernis der Verhältnismässigkeit hat der europäische Gerichtshof in ständiger Rechtsprechung festgehalten, die Handlungen

der Unionsorgane dürften die Grenzen dessen, was zur Erreichung der mit der fraglichen Regelung zulässigerweise verfolgten Ziele geeignet und erforderlich sei, nicht überschreiten. Stünden mehrere geeignete Massnahmen zur Auswahl, sei zudem die am wenigsten belastende zu wählen und die dadurch bedingten Nachteile müssten in einem angemessenen Verhältnis zu den angestrebten Zielen stehen[9].

Auf das eCall-System angewendet, bedeutet dies Folgendes: Ist die Nutzung desselben freiwillig und setzt eine Person dieses im Notfall ein, hat sie durch dessen Gebrauch in die Datenbearbeitung eingewilligt und es liegt kein Grundrechtsverstoss vor. Ist die Nutzung desselben dagegen *nicht* freiwillig (wie vorgesehen), stellt die mit diesem verbundene Bearbeitung von Personendaten nur dann keinen unzulässigen Grundrechtseingriff dar, wenn sie die vier oben genannten Voraussetzungen von Art. 52 Abs. 1 GRCh erfüllt. Nachdem die von diesem geforderten gesetzlichen Grundlagen mitunter mit der vorgenannten Verordnung geschaffen wurden und der Wesensgehalt von Art. 8 Abs. 1 GRCh geachtet sein dürfte, stellt sich die Frage nach der Verhältnismässigkeit. Während die Geeignetheit eines obligatorischen eCall-Systems zur Erreichung der oben dargelegten Ziele weitgehend bejaht werden kann, dürfte es an der Erforderlichkeit fehlen. Dies insbesondere deshalb, weil es alternative (weniger belastende) Massnahmen gibt, mit denen die vom eCall-System verfolgten Ziele ebenso gut erreicht werden können. Zu denken ist z.B. an die vermehrte Förderung von computergesteuerten Bordelementen oder von an die konkreten Umstände angepassten Verkehrsleitsystemen sowie die Entwicklungsförderung von unfallsicheren Karosserie-Materialien oder die Nutzung der bereits vorhandenen privaten Smartphones. In der Folge ist die Verhältnismässigkeit eines *nicht* freiwilligen eCall-Systems zu verneinen, womit es an einer der für einen rechtmässigen Grundrechtseingriff erforderlichen Voraussetzungen fehlt. In diesem Zusammenhang ist darauf hinzuweisen, dass der Gerichtshof vor kurzem die EU-Richtlinie zur Vorratsdatenspeicherung[10] mangels Vereinbarkeit mit dem Verhältnismässigkeitsgrundsatz aufgehoben hat[11].

Und die Schweiz …?

Für die Schweiz präsentiert sich die rechtliche Sachlage weitgehend gleich. Auch in der Schweiz erfordert der Eingriff in das von Art. 13 Abs. 2 BV[12] vorgesehene Grundrecht auf Schutz vor Missbrauch der persönlichen Daten eine gesetzliche Grundlage. Im Weiteren muss ein entsprechender Eingriff verhältnismässig und angemessen (durch ein öffentliches Interesse oder den Schutz von Grundrechten Dritter gerechtfertigt) sein (Art. 36 BV). Mit Blick auf einen obligatorischen Einsatz eines eCall-Systems im oben genannten Sinn dürfte es in der Schweiz zurzeit bereits an der rechtlichen Grundlage fehlen. Aber selbst wenn eine solche geschaffen würde, kollidierte ein obligatorisches eCall-System auch hier mit dem Erfordernis der Verhältnismässigkeit. Auch in der schweizerischen Rechtsordnung erfordert der Grundsatz der Verhältnismässigkeit, dass die gewählte Massnahme zur Zielerreichung geeignet und erforderlich ist und dass bei mehreren gleich geeigneten Massnahmen, die jeweils mildeste gewählt wird[13].

Im Sinn eines Fazits lässt sich somit fragen, ob hier weniger (nämlich ein freiwilliges eCall-System) für alle Beteiligten nicht mehr wäre? ■

Fussnoten

1 Vorschlag für eine Verordnung des europäischen Parlaments und des Rates über Anforderungen für die Typengenehmigung zur Einführung des bordeigenen eCall-Systems in Fahrzeuge und zur Änderung von Richtlinie 2007/46/EG/COM/2013/0316 final (VO eCall), EUR-Lex 52013PC316-DE.

2 VO eCall, Eingangserläuterungen Ziff. 3.3, Art. 2, 4 und 5.

3 Hecking Claus, Spiegel Online vom 25.2.2014, zu finden unter: <http://www.spiegel.de/auto/aktuell/ecall-eu-will-automatisches-notrufsystem-fuer-alle-neuwagen-a-955359.html> (besucht am 7.8.2014).

4 VO eCall, Eingangserläuterungen Ziff. 3.3, Art. 2, 4 und 5.

5 Siehe für diesen Abschnitt VO eCall, Eingangserläuterungen Ziff. 1 und 2.2.1.

6 Siehe für diesen Abschnitt auch Hecking Claus, Spiegel Online vom 25.2.2014, Fundort siehe Fn. 3.

7 Charta der Grundrechte der Europäischen Union, ABl. C 83/389 vom 30.3.2010.

8 Siehe dazu auch Jarass Hans, Charta der Grundrechte der Europäischen Union, Kommentar, 2. Auflage, München 2013 (Art. 8 Rz. 11 ff.).

9 EuGH, Vorab. C-343/09, 2010, Rz. 45 (England); verb. Vorab. C-581/10, 2012, Rz. 71 (Deutschland und England); Vorab. C-101/12, 2013, Rz. 29 (Deutschland); Vorab. C-283/11, 2013, Rz. 50 (Österreich); siehe für weitere Ausführungen dazu Cornils Matthias in: Grabenwarter Christoph (Hrsg.), Europäischer Grundrechteschutz, Baden-Baden 2014, § 5 Rz. 107 ff.

10 Richtlinie 2006/24/EG über die Vorratsdatenspeicherung von Daten, ABl. L 105/54 vom 13.4.2006.

11 EuGH, Vorab. C-293/12, 2014, Rz. 69 ff. (Irland und Österreich).

12 Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101.

13 Häfelin Ulrich/Haller Walter/Keller Helen, Schweizerisches Bundesstaatsrecht, 8. Aufl., Zürich 2012, Rz. 320 ff.

ISSS

Big Data – Chancen und Risiken

Ursula Widmer, Dr., Präsidentin Information Security Society Switzerland (ISSS), Dr. Widmer & Partner, Rechtsanwälte, Bern
ursula.widmer@widmer.ch

Die Menge der gespeicherten Daten verdoppelt sich ca. alle 2 Jahre. Gleichzeitig zeichnet sich ab, dass zunehmend weder physische Produkte wie Maschinen oder Produktionsstrassen noch Software für den Erfolg im Wettbewerb massgeblich sind, sondern das Wissen über Kunden, Märkte und Produkte. Solches Wissen lässt sich mit neuen mathematischen Hilfsmitteln, mit denen beinahe beliebig grosse Datenmengen aus verschiedensten Quellen analysiert und ausgewertet werden können, immer präziser gewinnen. Dies sind die treibenden Faktoren von Big Data und der Hintergrund, dass dieses als «neues Öl» oder «Goldmine» bezeichnet wird.

Der Einsatz von Big Data erlaubt Auswertungen für die Produktentwicklung, die Prognose von Marktentwicklungen und Kundenwünschen, für die Erfüllung von regulatorischen Anforderungen, indem z.B. verdächtige Finanztransaktionen erkannt werden können und vermutlich auch immer präzisere Persönlichkeits- und Verhaltensanalysen von uns allen. Schliesslich erlaubt Big Data die Nutzung von Daten als Geschäftsmodell, indem grosse Datenmengen für Analyse und Auswertung zur Verfügung gestellt werden.

Somit stellen sich auch neue Herausforderungen an das Datenmanagement und die Datensicherheit. Es besteht die Gefahr, dass die Kontrolle über die Daten und deren Kopien verloren geht. Auch ist die Frage nach der Richtigkeit der Informationen schwieriger zu beantworten, wenn diese aus einer Vielzahl unterschiedlicher Quellen stammen. Andererseits lässt sich Big Data für die ICT-Sicherheit nutzen, z.B. zur Erkennung von komplexen, über eine längere Zeit andauernde Angriffe in Netzwerken.

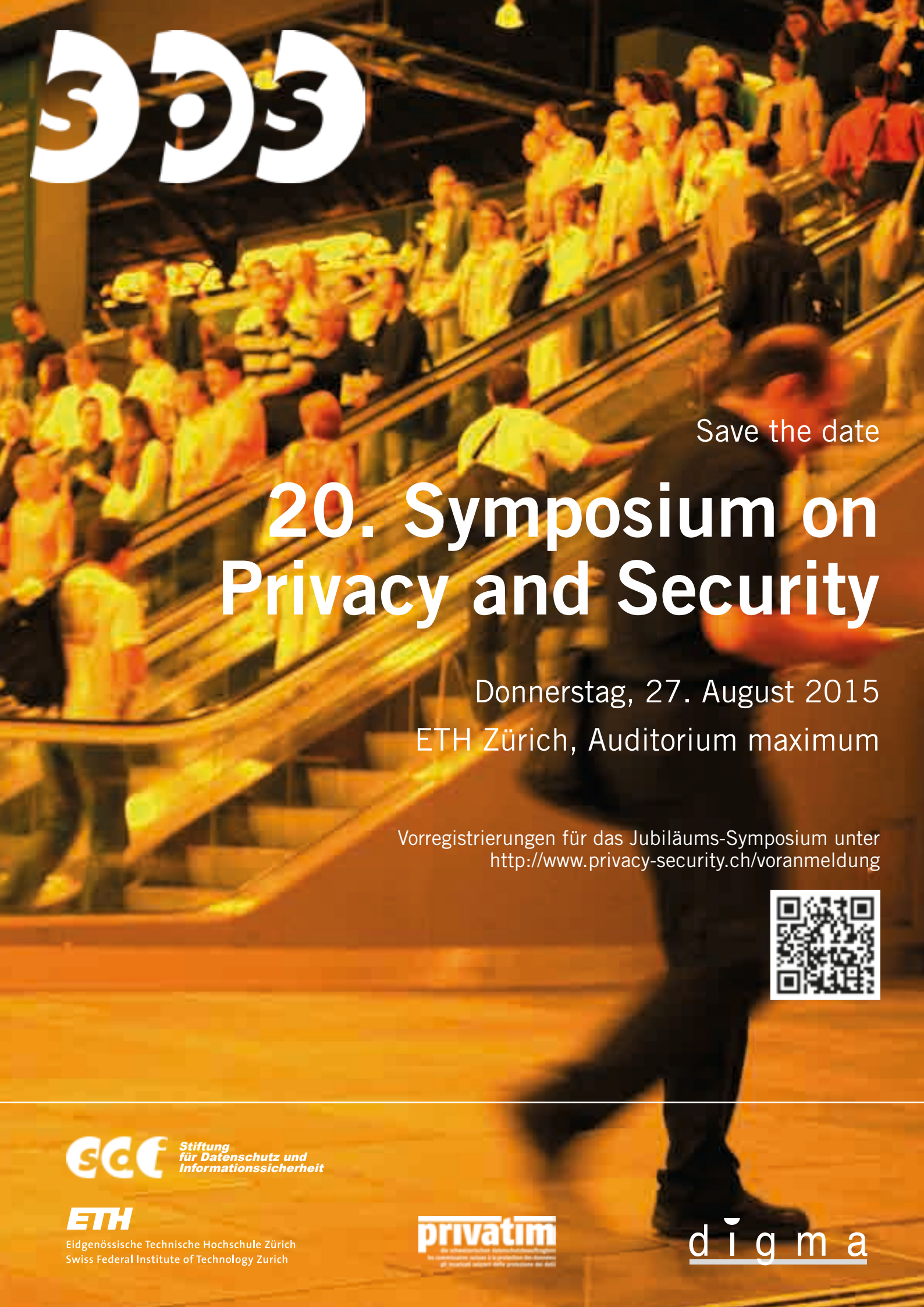
Grundlegende Fragen wirft Big Data im Zusammenhang mit dem Datenschutz auf. Verlangt der Datenschutz, dass nur diejenigen Daten erhoben werden, welche für einen bestimmten Zweck notwendig sind, und dass die Daten gelöscht werden, wenn dieser Zweck erreicht ist, so ist es aus der Sicht von Big Data wünschenswert, dass möglichst viele Daten aus möglichst langen Zeiträumen verfügbar sind, die von zahlreichen Interessenten zu den unterschiedlichsten Zwecken analysiert und ausgewertet werden können. Damit ist auch die datenschutzrechtliche Zielsetzung, dass die Betroffenen jeweils wissen, welche Daten von wem und zu welchem Zweck bearbeitet werden, nicht mehr aufrechtzuerhalten.

Werden für Big Data anonymisierte Daten genutzt, findet das Datenschutzrecht zwar keine Anwendung, da kein Personenbezug der Daten besteht. Die Problematik liegt jedoch darin, dass sich nicht immer eindeutig beurteilen lässt, ob die Anonymisierung genügt. Es ist möglich, dass Daten, die in einem bestimmten Kontext genügend anonymisiert sind, wenn sie mit anderen Daten kombiniert werden, die Anonymisierung wieder verlieren. Es entsteht die paradoxe Situation, dass die gleichen Daten kontextabhängig einmal vom Datenschutzrecht ausgenommen sind und ein anderes Mal nicht.

Die Fragestellungen bezüglich der Informationssicherheit und des Datenschutzes im Zusammenhang mit Big Data sind neu und verlässliche Lösungen müssen weltweit erst noch gefunden werden. Einen Beitrag hierzu wird die nächste ISSS Berner Tagung «Big Data – Chancen und Risiken in der Praxis» vom 26. November 2014 leisten. Anlässlich dieser Veranstaltung sollen Fragestellungen, wie oben skizziert, mit Fachexperten beleuchtet und erste Antworten und Lösungsansätze aufgezeigt werden. ■

Link

Weiterführende Informationen zur Berner Tagung finden Sie auf der Website der Information Security Society Switzerland ISSS (<http://www.isss.ch>).



Save the date

20. Symposium on Privacy and Security

Donnerstag, 27. August 2015

ETH Zürich, Auditorium maximum

Vorregistrierungen für das Jubiläums-Symposium unter
http://www.privacy-security.ch/voranmeldung

Stiftung für Datenschutz und Informationssicherheit

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

privatim

digma

Aus den Datenschutzbehörden

Herzlich willkommen zu den News aus den Datenschutzbehörden.

Kanton Basel-Stadt

■ Am 6. Juli 2014 ist § 30a des baselstädtischen Aufenthaltsgesetzes vom 16. September 1998[1] in Kraft getreten. Die Bestimmung erlaubt es der Einwohnerkontrolle, die zur Kontaktaufnahme für ein bestimmtes Forschungs- oder Präventionsprojekt notwendigen Adressdaten ausgewählter Bewohnerinnen und Bewohner bekannt zu geben an «a) öffentliche und private Stellen und Organisationen, die vom Bund, vom Kanton oder einer Gemeinde mit der Durchführung eines bestimmten Forschungs- oder Präventionsprojektes beauftragt worden sind oder b) öffentlich-rechtliche Forschungseinrichtungen für ihre Forschungsprojekte»[2].

■ Der Datenschutzbeauftragte hat ein Merkblatt zur Anonymisierung von Word- und pdf-Dokumenten auf seiner Homepage veröffentlicht: <http://www.dsb.bs.ch/taetigkeitsbereiche/querschnittsthemen/anonymisierung.html>.

Kanton Zug

Am 6. September 2014 ist das Gesetz über die Videoüberwachung im öffentlichen und im öffentlich zugänglichen Raum in Kraft getreten[3].

■ Neben zahlreichen positiven Punkten (der Einsatz von Videoüberwachung ist in einem Gesetz ausdrücklich und klar geregelt, für kantonale Organe ist der Regierungsrat Bewilligungsinstanz, für kommunale der Gemeinderat [§ 5], wobei diese Kompetenzen nicht delegiert werden dürfen [§ 5 Abs. 2], rechtskräftige Bewilligungen hat der Datenschutzbeauftragte unter Einschluss des Aufnahmeperimeters [im Internet] zu veröffentlichen etc.), hat der Zuger Datenschutzbeauftragte jedoch auch einige der getroffenen Lösungen zu beanstanden. Ein Auszug:

■ Der Zweck der Videoüberwachung ist viel zu umfassend – Videoüberwachung kann letztlich für alles und jedes eingesetzt werden (§ 3).

■ Die Erforderlichkeit der Überwachung müsste vertieft nachgewiesen werden.

■ Bezüglich der Zuständigkeit müsste das Territorialitätsprinzip gelten: zuständig für die Überwachung müsste somit sein, wer die Hoheit über die zu überwachenden Örtlichkeit hätte. Das Gesetz definiert jedoch die Zuständigkeit nach der Zuständigkeit für «Ruhe und Ordnung» (Zuständigkeit: Gemeinde bzw. übrige Organe) bzw. «Sicherheit» (im ganzen Kanton: Polizei) (§ 4). Es ist daher (wohl) davon auszugehen, dass damit die Zuger Polizei in der Praxis sämtliche Videokameras im Kanton betreiben wird. Diese Zentralisierung ist (jedenfalls) heikel.

■ Bei Verlängerungsgesuchen hätte die Erforderlichkeit der Weiterführung mit einem Evaluationsbericht nachgewiesen werden müssen.

■ Echtzeitüberwachung sollte höchstens in Ausnahmesituationen zulässig sein (§ 8).

■ Das Bildmaterial sollte im 4-Augen-Prinzip durch das verantwortliche Organ und eine für Sicherheit zuständige Stelle ausgewertet werden (§ 9). ■

Sandra Husi-Stämpfli, Dr. iur. LL.M., Stv. Datenschutzbeauftragte des Kantons Basel-Stadt, Basel
sandra.husi@dsb.bs.ch

Fussnoten

1 SG 122.200.

2 Ausführlich dazu Sandra Husi, § 30a AufenthG, in: Beat Rudin/Bruno Baeriswyl (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt, Zürich 2013.

3 Videoüberwachungsgesetz, VideoG, BGS 159.1.

Nächste Nummer

Die nächste Ausgabe von digma erscheint im Dezember 2014 und widmet sich schwerpunktmässig dem Thema **«Der ‹betreute› Mensch».**

Mein Auto, meine Nanny

Beat Rudin, Herausgeber, beat.rudin@unibas.ch

Der Mensch ist ein soziales Wesen. Die meisten haben es gern, wenn jemand zu ihnen schaut. Nicht jemand, der alles besser weiss, sondern Freunde, die uns sanft ansprechen, wenn wir aus der Spur zu geraten drohen. Nicht jemand, der wie «Helikoptereltern» alle Gefahren und Risiken von uns fernhält, sondern Freunde, die uns in unserer Selbstständigkeit unterstützen.

Nun bekommen wir neue solche Freunde, die uns bewahren vor all dem Bösen, das uns droht: unsere Autos. Sie blinken und piepsen schon heute, wenn wir die Sicherheitsgurten nicht umlegen – am Anfang noch zurückhaltend, dann penetrant. Und nun kündigt General Motors (GM) die nächste Wohltat an: Ein System analysiert die Augenbewegungen der Fahrerin (Männer sind selbstverständlich mitgemeint), um ihre Müdigkeit frühzeitig zu erkennen.

Super – schon wieder jemand, der es gut mit uns meint! Keine Gefahr eines verheerenden Sekundenschlafs mehr! Wir müssen nicht mehr auf die Signale unseres Körpers achten – das Auto sagt uns, wenn wir nicht mehr fahren können. Nur – wenn wir trotz Müdigkeit noch irgendwohin fahren müssen, dann nervt die Stimme gewaltig. Auch wenn sie noch so nett tönt.

Viel mehr Fragen habe ich aber zu dem, was hinter der Stimme läuft. Was passiert mit den Daten? Gehen die an den Autohersteller? GM sagt: ja, aber anonymisiert – nur: Was heisst im Zeitalter von Big Data anonymisiert noch? Kann die Polizei die Daten auslesen, wenn sie mich kontrolliert? Gehen sie an meine Versicherung? Werden sie im Schadensfall verwendet, um über die Haftung zu entscheiden? Und wie steht's mit dem Ausbaupotenzial? Wenn wir schon die Augen vermessen – damit kann man auch feststellen, ob die Fahrerin (Männer sind immer noch mitgemeint) unter Alkoholeinfluss steht. Wohin fliessen diese Daten dann?

Ich habe Verständnis dafür, dass sich die Fahrerin beobachtet fühlt. Brauchen wir wirklich das ganze Leben eine Nanny? Sollen all die Geräte um uns herum die Über-Sorge der «Helikoptereltern» fortsetzen?

Freiheit sieht anders aus. Es wäre wohl wichtiger, dass wir lernen, mit der Freiheit verantwortungsbewusst umzugehen.

PS aus aktuellem Anlass: Wie interpretiert wohl das System das Augenverdrehen der Fahrerin, die soeben erfahren hat, dass GM schon wieder über 200 000 Autos wegen eines Defekts zurückrufen muss – zusätzlich zu den bisher rund 30 Mio. in diesem Jahr? (www.wirtschaftsblatt.at, 21.9.2014)


Wenn Ihre Daten missbraucht wurden: Besorgen Sie sich eine neue Identität!
Beratung Datenschutz
Fontana

FB
FACH
HAND
BUCH

Expertenwissen für die Praxis

Verwaltungsrecht

Das Fachhandbuch richtet sich an praktische Rechtsanwender mit hohem fachlichem Anspruch. Der Aufbau ist stark an den Problemen der Praxis orientiert. Beispiele, Checklisten und Praxistipps erleichtern den Überblick. Alle praxisrelevanten Aspekte einschliesslich prozessualer Hinweise werden abgedeckt, Schnittstellen und Nebengebiete sind erläutert.

Fachhandbuch Verwaltungsrecht

Expertenwissen für die Praxis

Fachhandbuch

Herausgeberschaft:

Giovanni Biaggini
Isabelle Häner
Urs Saxer
Markus Schott

Erscheint im November 2014

ca. 1450 Seiten, gebunden
ISBN 978-3-7255-6748-5
ca. CHF 298.00

Das Fachhandbuch Verwaltungsrecht vereinigt über 30 Expertenbeiträge namhafter Autorinnen und Autoren aus Advokatur, Justiz, Verwaltung und Universitäten. Es verbindet wissenschaftliche Qualität mit ausgeprägter Praxisrelevanz und deckt verschiedenste Bereiche des Verwaltungsrechts ab: Einerseits die Regelungen einzelner Wirtschaftszweige wie der Banken- und Finanzwelt, der Medien, des Verkehrs, der Energie oder des Gesundheitswesens; anderseits die sektorübergreifenden Grundfragen wie Bewilligungen und Konzessionen, die Staatshaftung oder das Aufsichtsrecht. Die einzelnen Beiträge verarbeiten umfassend die relevante Praxis von Verwaltungsbehörden und Gerichten. Dadurch ist das Werk auf dem neuesten Stand.

Schulthess Juristische Medien AG Zwingliplatz 2 8001 Zürich www.schulthess.com

Schulthess §
Der Verlag zu Recht