Besprechung / Compte rendu

Neuer Regulierungsschub im Datenschutzrecht?

ROLF H. WEBER / FLORENT THOUVENIN (HG.)

Neuer Regulierungsschub im Datenschutzrecht?

Zentrum für Informations- und Kommunikationsrecht, Bd. 54

Schulthess Juristische Medien AG, Zürich 2012, VI+188 Seiten, CHF 62.–, EUR 45.–,

ISBN 978-3-7255-6692-1

Seit die geheimen Abhörprogramme «Prism» und «Tempora» im Juni diesen Jahres bekannt wurden, ist der Daten-schutz wieder einmal in aller Munde. Dass der US-amerikanische Auslandsgeheimdienst NSA seit 2007 massenhaft Zugriff auf Kundendaten von Internetgrössen wie Yahoo, Google, Micro-soft, Apple und Skype erhielt (Prism) und der britische Nachrichten- und Sicherheitsdienst GCHQ über 200 Glasfaserleitungen zur Überwachung des transatlanti-schen Datenverkehrs angezapft haben soll (Tempora), hat sowohl in einer breiten Öffentlichkeit als auch in der Politik die schlimmsten Befürch-tungen bestätigt oder sogar übertroffen. Enthüllungen wie diese sind Wasser auf die Mühlen der Be-fürworter eines effektiveren und stärkeren Datenschutzes. Der von den Proff. Weber (Universität Zü-rich) und Thouvenin (Universität St.Gallen) herausgegebene Sammelband zum Thema «Neuer Regu-lierungsschub im Daten-schutzrecht?» ist nicht erst im Lichte dieser Entwicklungen von grosser Aktua-lität. Der Band bespricht die im Rahmen einer Veranstaltung des Zentrums für Informations- und Kommunikationsrecht der Universität Zürich, der Forschungs-stelle für Informationsrecht der Universi-tät St.Gallen sowie des Schweizer Forums für Kommunikationsrecht behandel-ten Themen vertieft und ermöglicht es dem Leser, die unterschiedlichen Auffassungen zur vielschichtigen Thematik der Frage der Reformbedürftigkeit des Datenschutzrechts zu verstehen und sich eine eigene Meinung darüber zu bilden. Als sehr gelungen zu bezeichnen ist dabei die Wahl der Autoren, welche sich aus Exponenten der Wissenschaft, der Praxis und der Datenschutzbehörden zusammensetzen.

Der Band wird nach den einführenden Worten der Herausgeber eröffnet mit der Analyse der neuen Grundrechts-konzeptionen zum Schutz der Privatheit von ROLF H. WEBER. Nach einer Beschreibung der Gefährdungssituation im Informationszeitalter zeigt er auf, welchen Grundrechtsschutz die schweizerische Bundesverfassung der Privatheit als solcher zukommen lässt; er erwähnt dabei die persönliche Freiheit, das Kommunikationsgeheimnis, den Schutz des Privatlebens sowie den Schutz vor Missbrauch persönlicher Daten. Unter Bezugnahme auf die deutsche Verfassungs-rechtsprechung zeigt er vier neue Schutzrechte auf: Das Recht auf informationelle Selbstbestimmung, das Grundrecht auf Vertraulichkeit und Integrität (sog. Computergrundrecht), das Recht auf Grenzen der Datenaufbe-wahrung sowie das Recht auf Anonymität. Ein Recht auf Anonymität sieht WEBER in der Schweiz durch den Logistep-Entscheid des Bundesgerichts etabliert, soweit IP-Adressen das Schutzgut sind. Soweit die Personenidentifizierung das Schutzgut darstellt, legt er dar, dass die Google-Streetview-Rechtsprechung ein Schutzkonzept etabliert hat, das nicht am konkreten Individuum anknüpft, son-dern am gesamthaft zu würdigenden System. Dies deshalb, weil das Bundesgericht urteilte, dass eine Fehlerquelle bei der Datensicherheit (d.h. der Verpixelung von Gesichtern und Nummernschildern) von unter 2% hinzunehmen ist. Aufgrund der digitalen Grundrechtsgefährdungen kommt WEBER zum Schluss, dass der traditionelle subjektiv-rechtliche Ansatz des Grundrechtsschutzes (wie etwa im schweizerischen Datenschutzgesetz enthalten) nicht mehr ausreiche, um ein angemessenes gesamt-gesellschaftliches Datenschutzniveau zu erreichen. Zusätzlich sei der Staat gefordert; er müsse si-cherstellen, dass die Integrität des Übertragungsprozesses von digitalen Informationen gegenüber staatlichen und privaten Eingriffen geschützt werde.

JÜRGEN HARTUNG zeigt in seinem umfassenden Artikel neue materielle Regelungsbereiche der geplanten EU-Datenschutzreform auf und bespricht damit vor allem den Entwurf der EU-Kommission für eine Datenschutz-Grundverordnung vom 25. Januar 2012. Er konzentriert sich dabei auf Bereiche,

welche Nicht-EU-Länder wie die Schweiz beeinflussen könnten. Gründe der Reform, welche äusserst umstritten ist und dem Vernehmen nach in Brüssel enorme Lobbying-Bemühungen vonseiten v.a. der grossen US-amerikanischen Internet-Gesellschaften ausgelöst hat, sind die Harmonisierung des EU-Datenschutzrechts, eine Entbürokratisierung sowie die Anpassung an technische Ent-wicklungen. HARTUNG zeigt auf, dass der räumliche Anwendungsbereich ausgeweitet werden soll, sodass ein Unter-nehmen mit Sitz in der Schweiz oder den USA der Grundrechtsverordnung unterstehen würde, wenn dieses Daten über in der EU ansässige Personen entweder beim Angebot von Waren oder Dienstleistungen in der EU verarbeitet oder deren Verhalten «beobachtet» (wozu Targeted Advertising zählen würde). Weitere Reformbereiche betreffen den Begriff des Personendatums (welcher ausgeweitet werden soll), die Ausgestaltung von Einwilligungserklärungen, das Recht auf Vergessenwerden (das erstmals verankert werden soll) und Datenmitnahme sowie die Stärkung der Informationsrechte. Mit der Einführung eines «vorbeugenden Datenschutzes», der vielfach unter dem Mode-Begriff Privacy by Design bzw. Privacy by Default diskutiert wird, soll die Pflicht statuiert werden, vorhandene Voreinstellungen, den möglichen Umfang einer Datenverarbeitung und Löschungsfristen möglichst datenschutzfreundlich auszugestalten, sowie eine Folgenabschätzung vorzunehmen. HARTUNG zeigt illustrativ auf, welche Probleme die Umsetzung einer solchen Regelung hätte, und äussert die Befürchtung, dass die vorgesehene behördliche Konsultationspflicht zu einem «Run» auf die Datenschutzbehörden führen könnte. Insgesamt geben die Ausführungen einen ausgezeichneten Überblick über die möglichen Konsequenzen der geplanten weitreichenden Überarbeitung des EU-Datenschutzrechts und deren Aussenwirkung. Angesichts der Tatsache, dass auch Unternehmen mit Sitz ausserhalb der EU Bussen von bis zu 2% des weltweiten Jahresumsatzes drohen, ist das Lobbying von Gesellschaften, deren Geschäftsmodell auf der Kom-merzialisierung von Daten von Internetnutzern basiert, nachvollziehbar.

PAUL M. SCHWARTZ und DANIEL J. SOLOVE beschäftigen sich mit dem für das Datenschutzrecht zentralen Begriff des Personendatums (personally identifiable information gemäss US-Recht). Die beiden US-amerikanischen Professoren plädieren dafür, unterschiedliche Datenschutzniveaus zu schaffen, je nachdem, ob es sich um «identified data», «identifiable data» oder «non-identifiable data» handelt. Während bei identifizierten (identified) Daten der höchste Schutzstandard gelten müsse – und der betroffenen Person sämtliche Rechte (insbesondere vollständige Notifikations-, Zugriffs- und Änderungsrechte) zustehen sollten –, komme dem Datenschutzrecht bei Daten der letzten Kategorie keine Rolle zu, da kein Personendatum vorliege. Bei bestimmbaren (identifiable) Daten solle ein reduzierter Schutzstandard gelten. Ein solch risikoorientierter Ansatz, den SCHWARTZ/SOLOVE als PII 2.0 bezeichnen, habe auch den Vorteil, dass die datenbearbeitenden Unternehmen einen Anreiz hätten, Daten in möglichst wenig identifizierbarer Art und Weise zu halten.

HANSPETER THÜR, der eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB), erörtert in seinem Beitrag, ob das über 20-jährige eidgenössische Datenschutzgesetz (DSG) den heutigen Anforderungen noch gewachsen ist. Nach einer kurzen Besprechung des bundesrätlichen Berichts über die Evaluation des DSG vom 9. Dezember 2011 und hängiger parlamentarischer Vorstösse bespricht er diejenigen 6 Gebiete, die aus seiner Sicht bei einer Totalrevision (die er anregt) genauer zu betrachten seien: Objekt und Geltungsbereich des Gesetzes (gewisse Ausnahmen vom Geltungsbereich seien aufzuheben), Definition (Angleichung der Terminologie an EU, etwa hinsichtlich «Controller»-Begriff), Grundprinzipien des Datenschutzes (u.a. Ergänzung des Bearbeitungsgrundsatzes «Datensparsamkeit»), Rech-te der betroffenen Personen (u.a. Einführung von Recht auf Vergessenwerden und der Datenübertragung), Verpflich-tungen von Datenbearbeitern (u.a. neue Verpflichtung zu Privacy by Design, Datenschutzfolgeabschätzung, Daten-schutzverantwortlichem), Aufsicht (zusätzliche Kompetenzen von Datenschutzaufsichtsbehörden, Sicherstellung mate-rieller Unabhängigkeit). Wenig überraschend orientiert sich THÜR stark am laufenden Reformprojekt der EU (vgl. die Zusammenfassung von HARTUNGs Aufsatz). Angesichts der «schweizerischen Realität der kleinen Schritte», welche einer Totalrevision im Wege stehen könnte, bezeichnet THÜR die drei letztgenannten Bereiche als die vordringlichsten Reformpunkte, auf welche nicht verzichtet werden solle. Mit einer solchen Reform bestehe die Hoffnung, dass der Schutz der Privatsphäre kein überholtes Auslaufmodell sei.

BRUNO BAERISWYL, der Datenschutzbeauftragte des Kantons Zürich, nimmt sich der populären sozialen Netzwerke an. Diese sind für ihn die besten Taktgeber für die aktuellen Reformbestrebungen; eine Reform des Datenschutzrechts müsse sich daran messen, wie Garantien für die Privatheit in den sozialen Medien gewährleistet werden. BAERISWYL argumentiert, dass das geltende Datenschutz-

gesetz den Schutz der Privatsphäre der Nutzer von sozialen Netzwerken nicht hinreichend sicherstelle, weshalb neue rechtliche Instrumente notwendig seien. Nach Ausführungen zur grundrechtlichen Natur des Datenschutzes zeigt er auf, welche Datenbearbeitungen in sozialen Netzwerken stattfinden, bevor er sich den Allgemeinen Geschäftsbedingungen (AGB) widmet. Diese verunmöglichten ein Vorgehen gegen die Betreiber faktisch aufgrund ihrer Bestimmungen zum anwendbaren Recht, dem Gerichtsstand und den Haftungsbeschränkungen. BAERISWYL geht danach den seiner Ansicht nach notwendigen Konsequenzen für die schweizerische Rechtsetzung nach: Er schlägt, inspiriert von den europäischen Reformprojekten, unter anderem vor, dass zwingend das Recht und der Gerichtsstand am Wohnsitz der betroffenen Person gelten müssten sowie ein Recht auf Vergessenwerden sowie auf Portierbarkeit von Daten zu schaffen sei. Die Ausführungen von BAERISWYL schliessen mit dem Hinweis, dass es mit der Nutzung von sozialen Medien zu einem «Trade Off» mit der Privatsphäre gekommen sei, was es zu korrigieren gelte.

FLORENT THOUVENIN widmet sich in seinem Beitrag dem Spannungsverhältnis zwischen dem Urheberrecht und dem Datenschutzrecht am Beispiel der Bekämpfung des unautorisierten Filesharings über das Internet. Das Interesse der Rechteinhaber an der Durchsetzung ihrer Schutzrechte online steht dem Anliegen der Nutzer auf Wahrung ihrer Privatsphäre gegenüber. Als Ausgangspunkt dient ihm dabei das Anti-Counterfeiting Trade Agreement (ACTA), das schliesslich gemäss dem Autoren zumindest teilweise auch am erwähnten Spannungsverhältnis – und der nicht hinrei-chenden Berücksichtigung von Datenschutzanliegen – scheiterte. THOUVENIN gibt zunächst einen konzisen Überblick über die Entstehungsgeschichte von ACTA und die Gründe des Scheiterns, wobei er freilich die Vermutung äussert, dass einzelne Anliegen wie die recht weit gehenden Rechtsdurchsetzungsinstrumente in anderen Handelsabkommen (wie. z.B. das Trans-Pacific Partnership Agreement [TPP]) Eingang finden könnten. In der Folge beleuchtet er verschiedene Ansätze zur Durchsetzung von Urheberrechten im Internet: Ein Vorgehen gegen Rechtsverletzer selber, über Access-Provider, Graduated-Response-Modelle, technische Massnahmen (DRM) sowie Informationen für die Wahrnehmung von Rechten (z.B. digitale Wasserzeichen). Seine Analyse kommt zum Schluss, dass diese Ansätze (zumeist) aufgrund entgegenstehender Vorgaben des geltenden Datenschutzrechts wenig erfolgversprechend sind. Als Ausweg aus diesem Dilemma sieht THOUVENIN drei Lösungsmöglichkeiten, denen im Wesentlichen ein Ersatz des Verbotsrechts der Rechteinhaber durch pauschalisierte Vergütungsansprüche zugrunde liegt: eine Weiterentwicklung des gegenwärtigen Systems der kollektiven Verwertung, eine Content- bzw. Kultur-Flatrate und ein Pay-per-Use-/Pay-per-Volume-Modell. In all diesen Systemen könne ein angemessener Schutz der Privatsphäre gewährleistet werden.

NICOLE BERANEK ZANON geht in ihrem ausführlichen Aufsatz der Frage nach, ob die Datenaufbewahrungspflich-ten des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) mit den Datenlö-schungspflichten des DSG kollidierten. Nach allgemeinen Ausführungen zur Konzeption des BÜPF und des DSG zeigt sie den rechtlichen Rahmen der Überwachung des Fernmeldeverkehrs gemäss Strafprozessordnung und BÜPF genauer auf, wobei sie sich auch dem Datenschutz im Fernmeldegesetz widmet. BERANEK ZANON diskutiert sodann detailliert die gemäss BÜPF zu sammelnden Daten und geht dabei auch auf den Vorentwurf für eine Änderung des BÜPF ein (ein Gesetzesentwurf und die Botschaft wurden im Februar dieses Jahres an das Parlament überwiesen). Die Frage der Not-wendigkeit der vor allem in Deutschland kontrovers beurteilten Vorratsdatenspeicherung (d.h. der rückwirkenden Überwachung) sei berechtigt, und die Autorin zeigt die Vorgaben an dieselbe gemäss dem Urteil des deutschen Bun-desverfassungsgerichts vom 2. März 2010 auf. Betreffend Datenschutz und insbesondere Datensicherheit bestehe Handlungsbedarf am Vorentwurf. Schliesslich konstatiert BERANEK ZANON ein Seilziehen zwischen Fernmeldedienstanbieter, dem Dienst ÜPF und den Staatsanwaltschaften: Während Erstere in Gesetz und Verordnung nur diejenigen Überwachungsarten festhalten möchten, die derzeit technisch möglich seien, plädierten der Dienst ÜPF und die Staatsanwaltschaften für möglichst offene Generalklauseln. Der Gesetzgeber müsse klare rechtliche Grundlagen und ein austariertes Modell schaffen, welche den Grundrechtseingriff ins Fernmeldegeheimnis und den Datenschutz im Allgemeinen rechtfertigten, womit ein Gleichgewicht zwischen den widerstrebenden Interessen gewahrt bleibe.

DAVID ROSENTHALs Beitrag zur Datenschutz-Compliance im Unternehmen, der den Vortragsstil beibehält, rundet diesen Band würdig ab. Nach einer Einleitung, in welcher er aufzeigt, dass Datenschutzverletzungen im Alltag von jedermann zig-fach begangen werden, legt ROSENTHAL praxisnah und fachkundig dar, was von Unternehmen realisti-scherweise verlangt werden kann, um den Vorgaben des DSG nachzukommen. Er schlägt u.a. vor, dass Unternehmen eine Anlaufstelle für Daten-

schutzbelange schaffen, ein Verzeichnis von Datensammlungen erstellen, Datenbearbeitun-gen sorgfältig dokumentieren, sowohl unternehmensinterne als auch grenzüberschreitende Datenflüsse regeln und auf Vorfälle und Anfragen von betroffenen Personen zeitnah reagieren. Von grossem Interesse ist schliesslich der zweite Teil von ROSENTHALs Beitrag, der die derzeitigen Regulierungstrends (vgl. hiezu die Beiträge von HARTUNG, THÜR und BAERISWYL) kritisch hinterfragt. ROSENTHAL zieht zunächst die weitverbreitete These in Zweifel, dass die betroffenen Personen (deren Daten bearbeitet werden) unter der geltenden Rechtslage litten. Offenbar liege ihnen schlicht die Nut-zung der neuen Informationstechnologien mehr am Herzen als das Risiko eines Missbrauchs ihrer Daten. Dass dies auf Unwissen zurückzuführen sei, sei angesichts der Medienberichterstattung zweifelhaft. Schärfere Sanktionen bei Daten-schutzverstössen erachtet ROSENTHAL als nicht notwendig; sie verbesserten den Datenschutz für die betroffenen Perso-nen nicht, verursachten jedoch erhöhte Compliance-Kosten. Er plädiert weiter auch gegen schärfere formale Vorschrif-ten des DSG. Auch diese führten einzig zu höheren Kosten, ohne dass sie das Niveau des materiellen Datenschutzes steigerten. Wenig überraschend plädiert ROSENTHAL schliesslich auch gegen schärfere materielle Vorschriften des DSG. Es bestehe die Gefahr, dass diese zu starr und innert Kürze überholt seien, sodass sie dem Technologie- und Wer-tewandel nicht mehr gerecht werden könnten; auch seien sie vielfach überschiessend, wie er u.a. anhand des neuen Art. 3 Abs. 1 lit. u UWG illustriert. Im Übrigen werde es immer einzelne Unternehmen geben, welche die Grenzen des Er-laubten auszureizen versuchten; diese sollten nicht den Anlass für die Schaffung von schärferen Regeln sein.

Es ist zu hoffen, dass sich der Gesetzgeber zumindest seriös mit dem Argumentarium von ROSENTHAL auseinan-dersetzt und nicht ausschliesslich den Stimmen Gehör schenkt, die einen schärferen Datenschutz fordern. Angesichts der Popularität von Datenschutzanliegen in Teilen der Bevölkerung und den europäischen Reformbestrebungen ist jedenfalls davon auszugehen, dass das DSG zumindest punktuell in den nächsten Jahren revidiert werden wird. Der Gesetzgeber hat die diffizile Aufgabe, hier nicht über das Ziel hinauszuschiessen und insbesondere nicht die Falschen zu treffen. Ansonsten könnte, wie ROSENTHAL befürchtet, ein verschärftes DSG lediglich zu höheren Compliance-Kosten führen, ohne dass damit tatsächlich ein höheres Datenschutzniveau etabliert würde.

Philipp Frech, Dr. iur., LL.M., Rechtsanwalt, Zürich