

Die Seite des SF / La page du FS

Neuer Regulierungsschub im Datenschutzrecht?

PATRICK EGGIMANN*

Veranstaltung des Zentrums für Informations- und Kommunikationsrecht der Universität Zürich, der Forschungsstelle für Informationsrecht der Universität St. Gallen und des Schweizer Forum für Kommunikationsrecht SF•FS vom 28. Juni 2012

- I. Einführung
- II. Neue Grundrechtskonzeptionen zum Schutz der Privatheit
- III. Neue Regelungsaspekte in der EU-Datenschutzreform
- IV. Gesetzgeberischer Handlungsbedarf in der Schweiz
- V. ACTA und Datenschutz
- VI. Datenaufbewahrungs- vs. Datenlöschungspflichten: Kollision von DSG und BÜPF?
- VII. Datenschutz-Compliance im Unternehmen
- VIII. Diskussion

I. Einführung

Die Tagungsleiter Prof. Dr. ROLF H. WEBER, Ordinarius an der Universität Zürich und Leiter des Zentrums für Informations- und Kommunikationsrecht der Universität Zürich sowie Prof. Dr. FLORENT THOUVENIN, Assistenzprofessor für Immaterialgüter- und Informationsrecht und Direktor der Forschungsstelle für Informationsrecht an der Universität St. Gallen, eröffneten die Tagung in einem vollen Saal des Zunfthauses zur Schmiden in der Zürcher Altstadt.

Prof. Dr. ROLF H. WEBER verwies einleitend auf die nur drei Tage zurückliegende Jahrespressekonferenz des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten sowie auf den entsprechend erst am Vortag veröffentlichten Bericht des kantonalen Datenschutzbeauftragten. Die täglichen Diskussionen um den Datenschutz im Verhältnis zwischen der Schweiz und den USA verdeutlichten die Aktualität des Themas und der Tagung. Die momentane Dynamik der Entwicklung, insbesondere auch in der EU, deutet an, dass die Zeit für allumfassende Lösungen noch – sollte sie denn überhaupt je kommen – nicht reif ist. Gemäss diesen Vorzeichen versprach die Tagung, von Beginn weg ein weites Feld an möglichen Fragen und daran anknüpfenden Antworten aufzutun.

II. Neue Grundrechtskonzeptionen zum Schutz der Privatheit

Prof. Dr. ROLF H. WEBER stellte einleitend fest, dass die neue technische Umgebung weltumspannender Netzwerke und übermittelbarer Code-Schriften eine noch nie dagewesene Herausforderung für die Privatheit darstellt. Das grosse Spektrum an Gefährdungssituationen, die sich grundsätzlich in die staatliche Überwachungstätigkeit und in die private Datensammlung unterteilen lassen, werde von den aktuellen Datenschutzbestimmungen vermutlich zu wenig erfasst. Die Bestandesaufnahme des verfassungsmässigen Grundrechtskatalogs zeige indessen, dass der Schutzbereich einigen Aspekten der digitalen Herausforderung bereits Rechnung tragen könne. Die Konkretisierung der persönlichen Freiheit bleibe bislang jedoch den Gerichten überlassen. Die bundesgerichtliche Bewertung weise dem Persönlichkeitsschutz dabei nur eine Auffangfunktion zu. In Bezug auf den Schutz der Privatsphäre nach Art. 13 BV werde häufig die Anwendung der Sphärentheorie propagiert. Diese könne aber nur beschränkt Anwendung finden, da der Informationsgehalt im Einzelfall zu wenig Beachtung fände. Beim Schutz vor dem Missbrauch persönlicher Daten werde von der Lehre zu Recht kritisiert, dass die informationelle Selbstbestimmung nicht nur Daten umfasse und der Begriff entsprechend zu eng ausgelegt werde.

* MLaw, Doktorand und Geschäftsführer der Forschungsstelle für Informationsrecht der Universität St. Gallen.

Im Weiteren zeigte WEBER die Reaktion der Gerichtspraxis auf die neuen Schutzbedürfnisse auf. Wesentlich sei die Erkenntnis, dass es sich beim Recht auf informationelle Selbstbestimmung nicht um ein Eigentumsrecht an der Information und damit um ein absolutes Recht, sondern um ein subjektives Herrschaftsrecht handle. In Deutschland sei in der digitalen Informationsverarbeitung eine Schutzlücke erkannt worden. Das BVerfG habe aus Art. 2 des Grundgesetzes das Recht auf informationelle Selbstbestimmung entwickelt und ein anerkanntes Grundrecht geschaffen.

Das Recht der Datenaufbewahrung sei in der EU durch die Richtlinie 2006/24 über die Vorratsdatenspeicherung kodifiziert worden. Die Schweiz verfüge auf Gesetzesebene über keine spezifische Regelung. In diesem Zusammenhang wies WEBER auf die Diskussion um das Recht auf Vergessen hin und meinte, dass das heute nicht mehr nur Schwerverbrecher, sondern uns alle interessiere. Die Anonymität sei ein wesentliches Anliegen, das zeige beispielsweise die Diskussion um Google Street View. In seinem Urteil 1C_230/2011 vom 31. Mai 2012 habe das Bundesgericht auch das Interesse der Öffentlichkeit an der Nutzung der Dienste und die wirtschaftlichen Interessen von Google in Erwägung gezogen. Vor diesem Hintergrund sei diesbezüglich wohl auch in Zukunft keine Nulltoleranz zu erwarten. Vielmehr werde eine Risikominimierung im Rahmen des technisch Machbaren zu fordern sein. Ein Anhaltspunkt für die Konkretisierung dieser Anforderung könne die vertragsrechtliche Frage nach der zulässigen Fehlerhaftigkeit von Softwareprodukten bieten.

Bei der Grundrechtskonzeption sei die Anerkennung ungeschriebener Menschenrechte in Anlehnung an die deutsche Rechtsprechung kein Tabu. Ebenfalls denkbar sei eine Einbindung in Art. 13 BV in Form eines unbenannten Menschenrechts. Die Grundrechtswirkung könne zudem auf den Schutz der Funktionsfähigkeit digitaler Systeme ausgeweitet werden. Eine so verstandene Grundrechtsfunktion würde nicht nur der Missbrauchsabwehr, sondern dem Vertrauen in den Prozess des Informationsaustausches als Ganzes dienen.

III. Neue Regelungsaspekte in der EU-Datenschutzreform

Dr. JÜRGEN HARTUNG, Rechtsanwalt in Köln, informierte über die Regulierungsvorhaben in der Europäischen Union. Von Interesse sei v.a. der Entwurf der EU-Kommission vom 25. Januar 2012 für eine Datenschutz-Grundverordnung, über die der Ministerrat und das Parlament voraussichtlich innerhalb der nächsten zwei Jahre abstimmen würden. Das Ziel der Verordnung bestehe in der Harmonisierung des uneinheitlichen Rechtsraumes. Aus diesem Grund erfolge die Regulierung durch eine Verordnung und nicht durch eine Richtlinie. Das Problem der unterschiedlichen Auslegung und Durchsetzung werde aber vermutlich dennoch bestehen bleiben. Zudem sei in Teilbereichen eine nationale Umsetzung vorgesehen. Konflikte mit dem jeweiligen nationalen Recht und im Zusammenhang mit der vorrangigen E-Privacy-Richtlinie 2002/58/EU seien entsprechend vorprogrammiert. Ein weiteres Ziel, der Abbau bürokratischen Volumens, stehe in Anbetracht des zu erwartenden Umfangs der Verordnung sowie der Vielzahl weiterer ausführender Akte, Formulare, usw. allerdings bereits jetzt in Frage.

Die Grundprinzipien und die Grundsystematik würden aus deutscher Sicht kaum verändert. Für deutsche Unternehmen wären aber einige Punkte zu beachten. Insbesondere der Rechtsschutz würde neu durch den EuGH und nicht mehr durch das BVerfG sichergestellt. Es sei zu erwarten, dass der EuGH den wirtschaftlichen Aspekten im Allgemeinen und der Wirtschaftsfreiheit im Besonderen stärkere Bedeutung zumessen werde. Der Fokus des BVerfG richte sich stärker am Individuum aus. Im Hinblick auf den räumlichen Anwendungsbereich sei eine Abkehr vom rein sitztechnischen Territorialitätsprinzip hin zum Ort der Datenverarbeitung zu erwarten. Die EU-Verordnung werde dadurch zu grossen Teilen auf Nicht-EU-Unternehmen anwendbar. Wie sich das durchsetzen lasse, sei aber bisher unklar.

Der sachliche Anwendungsbereich der Datenschutz-Grundverordnung sei ebenfalls noch umstritten. So sei insbesondere nicht geklärt, ob IP-Adressen und weitere technische Kennungen bereits personenbezogene Daten darstellten. Im Hinblick auf die Verantwortlichkeit würden sich insbesondere für Anbieter verschiedener Internet-Dienste wichtige Fragen stellen. Sofern die Daten gespeichert werden, sei die EU-Verordnung anwendbar. Aus Unternehmenssicht wenig erfreulich sei ferner die vorbeugende Datenschutz-Folgenabschätzung. Ähnlich wie im Kartellrecht räche sich hier eine schlechte Recherche. Abschliessend kritisierte HARTUNG die Starrheit der vorgesehenen Lösung und verwies auf Kanada als positives Beispiel. Dort bestehe Freiheit in der Umsetzung und in der Suche des

bestmöglichen individuellen Lösungswegs. Die Dokumentation diene nicht der Erfüllung eines starren Pflichtprogramms, sondern der Legitimation der individuell gewählten Lösung.

Das Recht auf Vergessen oder was noch davon übrig sei, werde hauptsächlich die Transparenz und die Einflussmöglichkeiten für die Betroffenen verbessern. Die Umsetzung im unmittelbaren Verhältnis zwischen Verantwortlichen und Betroffenen erscheine relativ unproblematisch. Schwierig gestalte sich nebst technischen Fragen hingegen die Umsetzung für Daten, die Dritte rechtmässig veröffentlicht hätten, und das Verhältnis zu anderen Rechtsgebieten, beispielsweise gegenüber dem Presserecht oder dem Recht auf freie Meinungsäusserung.

IV. Gesetzgeberischer Handlungsbedarf in der Schweiz

HANSPETER THÜR, Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, stellte vorweg fest, dass die Schweiz vor ähnlichen Herausforderungen wie die EU stehe. Im Hinblick auf die lokalen Probleme müsse die Schweiz aber auch selbst aktiv werden. Eine bessere Übereinstimmung mit dem europäischen Recht sei indessen wünschenswert. Die Evaluation des DSG habe dessen Wirksamkeit seit der Inkraftsetzung bestätigt, die Bedrohungslage habe sich jedoch gewandelt und insbesondere verschärft. Das sei namentlich auf die technische Entwicklung, die Quantität der Datenbearbeitungen und deren Globalisierung zurückzuführen. Entsprechend sei von der Notwendigkeit der Anpassung des DSG auszugehen. Ein Prüfungsauftrag für eine Revision solle dem EJPD bis 2014 unterbreitet werden.

Der Fokus für Anpassungen liege auf dem früheren Greifen des Datenschutzes (z.B. mittels Privacy by Design resp. Privacy Enhancing Technologies), in der Verbesserung der Datenherrschaft und Transparenz, der Sensibilisierung und dem Schutz Minderjähriger sowie auf der Stärkung der Aufsicht. Insbesondere bei der Aufsicht müsse ein rascheres Handeln ermöglicht werden. Nebst einer Vereinfachung der Sachverhaltsabklärung müsse der nicht angekündigte Zugang zu Lokalitäten im Rahmen vorsorglicher Massnahmen ermöglicht werden.

In Bezug auf den Anwendungsbereich sei eine Ausdehnung auf sämtliche Datenbearbeitungen zu favorisieren. Unverständlich sei beispielsweise, weshalb öffentliche Register ausgeschlossen sein sollten, und auch die Anwendung gleicher Bestimmungen für den privaten und den öffentlichen Sektor sei fragwürdig. Ein einheitliches Gesetz für Bund und Kantone dagegen stelle einen klaren Vorteil dar.

Bei den Rechten der Betroffenen gehe es nicht darum, Neues zu schaffen, sondern Bestehendes zu akzentuieren. Von der Förderung der Übertragbarkeit von Daten verspricht sich THÜR auch eine Stärkung des Wettbewerbs unter den Anbietern. Brisant sei zudem die ständige Beschattung von Internetnutzern. So dürfe es nicht sein, dass soziale Netzwerke vom Nutzer unbemerkt nebenher erfassen, welche Artikel einer Onlinezeitung gelesen würden. Unklarheit bestehe v.a. in Bezug auf die Kausalhaftung des Datenbearbeiters. Hinsichtlich dessen Verpflichtungen hob THÜR diejenige zur Errichtung eines Geschäftssitzes in der Schweiz hervor. Es könne nicht sein, dass man für ein einfaches Löschungsgesuch von Pontius zu Pilatus geschickt werde.

V. ACTA und Datenschutz

Prof. Dr. FLORENT THOUVENIN eröffnete sein Referat mit der Anmerkung, dass man sich wohl frage, was er überhaupt noch zu sagen hätte. Erst vor einer Woche sei in den Zeitungen zu lesen gewesen, dass das ACTA (Anti-Counterfeiting Trade Agreement) mindestens in Europa und wohl auch in der Schweiz nie in Kraft treten werde. Die Geschichte sei aber gerade hinsichtlich Transparenz und Datenschutz ein Lehrstück, dessen nähere Betrachtung sich lohne.

Aus Sicht der Schweiz lasse sich feststellen, dass bereits im Verhandlungsmandat des Bundes ein gesetzlicher Umsetzungsbedarf ausgeschlossen werden konnte. Die mit dem ACTA angestrebte Harmonisierung habe entsprechend vor allem auf die für den Transit von sogenannten Piraterieprodukten wesentlichen Drittstaaten, wie Marokko oder Mexiko abgezielt. Trotzdem seien in der Schweiz und in der EU mehrere zehntausend Menschen auf die Strasse gegangen. Auslöser der Proteste seien die intransparenten Verhandlungen über das Vorhaben und die Sorge um die Privatsphäre gewesen. So sei in einer weniger einschneidenden Endfassung des ACTA zwar kein direkter Datenaustausch zwischen Internet Service Providern und Rechteinhabern, aber noch immer eine rasche Übermittlung von identifizierenden Informationen auf behördliche Anordnung hin enthalten. Aus den Protesten gegen ACTA lasse sich schliessen, dass der Datenschutz im Internet für bestimmte Kreise

stark an Bedeutung gewonnen habe und die Strategie, die Öffentlichkeit möglichst lange nicht über die Verhandlung von Staatsverträgen zu informieren, heute kaum mehr tragbar sei. Die Zukunft des ACTA bleibe u.a. in den USA ungewiss. Ferner sei unklar, ob auch ohne Staatsvertrag die Rechtsdurchsetzungsmechanismen nicht auf anderem Weg eingeführt würden.

Im Weiteren ging THOUVENIN hinsichtlich der Durchsetzung von Urheberrechten vor allem auf die technischen Massnahmen und auf die Informationen für die Wahrnehmung von Rechten ein. Technische Massnahmen umfassen Zugangs- und Kopierkontrollen sowie Verschlüsselungs-, Verzerrungs- und Umwandlungstechniken, die es den Inhabern von Urheberrechten ermöglichen, die Nutzung von Werken in digitaler Form mit technischen Mitteln einzuschränken und zu kontrollieren, sog. Digital Rights Management (DRM). Ein rechtlicher Schutz gegen die Umgehung technischer Massnahmen sei auch in ACTA vorgesehen. Im Wesentlichen werde wiederholt, was bereits im US-amerikanischen Digital Millennium Copyright Act (DMCA) vorgesehen war und über den WIPO Copyright Treaty und den WIPO Performances and Phonograms Treaty international umgesetzt worden sei. Als Folge der Umsetzung dieser beiden Staatsverträge im Rahmen der letzten URG-Revision seien entsprechende Regeln seit 2008 auch in der Schweiz geltendes Recht (URG 39a ff.). Der Schutz werde im ACTA aber konkretisiert und teilweise verstärkt. Aus Sicht des Datenschutzes erscheine der Einsatz technischer Massnahmen jedoch als wenig problematisch, da ihr Einsatz entweder die Bearbeitung von Personendaten nicht umfasse oder die Datenbearbeitung zumindest erkennbar sei.

Da die mit dem Einsatz von DRM verbundenen Nutzungsrestriktionen in weiten Kreisen auf Ablehnung stossen würden, seien die Rechtsinhaber dazu übergegangen, ihre in digitaler Form verbreiteten Werke mit Informationen für die Wahrnehmung von Rechten zu versehen. THOUVENIN führt hier insbesondere die Verwendung von digitalen Wasserzeichen als Beispiel für das Spannungsverhältnis zwischen der Durchsetzung von Urheberrechten und dem Datenschutz im digitalen Kontext an. Wie im Fall «Logistep» (BGE 136 II 508) seien die fraglichen Personen indessen auch mit dieser Technik normalerweise nur durch die Mitwirkung Dritter bestimmbar. Aus datenschutzrechtlicher Sicht seien hier insbesondere die fehlende Erkennbarkeit und die Verhältnismässigkeit der Datenbearbeitung problematisch.

Abschliessend zeigte THOUVENIN drei mögliche Szenarien für die digitale Werknutzung auf: Das ökonomisch ideale, personalisierte Pay per use Modell, den grobkörnigen, teilweise anonymisierten Status quo und die ökonomisch wenig präzise, für den Schutz der Privatsphäre hingegen vorteilhafte Lösung der Flatrate.

VI. Datenaufbewahrungs- vs. Datenlöschungspflichten: Kollision von DSG und BÜPF?

NICOLE BERANEK ZANON, Legal Counsel Switch, zeigte aktuelle und potentielle Probleme aus der Praxis auf. Switch sei als Internet Service Anbieter mit einer Vielzahl unterschiedlicher Daten konfrontiert. Am Beispiel von Geodaten und weiterer Informationen aus dem Telekommunikationsbereich zeigte BERANEK ZANON auf, wie sich annähernd sämtliche Handlungen im Alltag einer Person nachvollziehen lassen. Dies sei in Anbetracht einer möglichen Weitergabe sensibler Daten an Dritte besonders beunruhigend. Ein solcher Fall liege momentan bei der Genfer Staatsanwaltschaft; in Frage stehe der Verkauf vertraulicher Daten durch Mitarbeiter von grossen Telekommunikationsunternehmen an ein Detektivbüro.

IP-Adressen könnten durch Fernmeldediensteanbieter bestimmten Personen zugeordnet werden, sofern die Daten noch vorhanden seien. Momentan bestehe eine Pflicht zur Datenspeicherung während sechs Monaten. Die vorgesehene Gesetzesänderung des BÜPF sehe neu 12 Monate vor, was in Anbetracht der grossen Datenmengen viel zu lang sei. Generell könne von einer Steigerung der Identifizierbarkeit ausgegangen werden. Dies sei auch auf die vermehrte Nutzung internetfähiger Geräte zurückzuführen, wozu ja bereits der moderne Kühlschrank gehöre. Jedes dieser Geräte verfüge über eine MAC-Adresse (Media-Access-Control-Adresse), die der Identifizierung des Geräts diene.

Im Schnittbereich von Telekommunikations- und Internetdaten werde momentan diskutiert, ob die neuen Technologien zum Abhören von Gesprächen über das Internet noch von Art. 280 StPO gedeckt seien. Anders als das Bundesgericht stellte BERANEK ZANON fest, dass die Möglichkeiten der Überwachung durch internetbasierte Lösungen wesentlich einschneidender seien. Eine ausreichende gesetzliche Grundlage böte hingegen der neue Art. 270bis StPO. Ebenfalls beachtenswert seien biometrische Authentifizierungstechniken und Gesichtserkennungsprogramme. Der Schutz für Personen, z.B. in Zonen mit Spitälern, müsse gewährleistet werden können.

Abschliessend wies BERANEK ZANON auf inhaltliche Unterschiede von VÜPF und BÜPF hin. Wo das Gesetz noch Fernmelde- und Internetanbieter in die Pflicht nahm, werde der Anwendungsbereich der Verordnung begrifflich auf Internetzugangsanbieter ausgeweitet. Ein Zielkonflikt bestehe grundsätzlich im Interesse an der Verfolgung schwerer Delikte und dem Schutz der Privatsphäre. Hier sei Augenmass gefordert.

VII. Datenschutz Compliance im Unternehmen

DAVID ROSENTHAL, Rechtskonsulent in Zürich, beschrieb die Diskrepanz zwischen dem gelebten Datenschutz im Unternehmen und dem normativen Sollzustand: Ein Reality Check. Vorweg stellte ROSENTHAL fest, dass vieles entgegen dem Gesetz nicht gemacht werde. Das sei aber in zweifacher Hinsicht zu relativieren. Einerseits könne man das DSG so oder so nicht vollumfänglich einhalten. Andererseits sei der Weg das Ziel; damit sei man in der Schweiz bis anhin generell gut gefahren.

Die Situation in den Unternehmen präsentiere sich weitgehend einheitlich. In Bezug auf die Einsetzung einer für Datenschutzfragen verantwortlichen Person lasse sich sagen, dass viele bestimmt worden seien, die Aufgabe aber nur von wenigen tatsächlich erfüllt werde. Das Problem liege dabei nicht in der fehlenden Bereitschaft, sondern im mangelnden Bewusstsein um die relevanten Fragen.

Festzustellen sei auch, dass, bedingt durch den grossen Aufwand, kaum ein Unternehmen ein vollständiges Verzeichnis seiner Datensammlungen erstelle. Wie man so das DSG befolgen könne, sei offensichtlich unklar. Zur Beruhigung vieler Teilnehmer merkte ROSENTHAL hier an, dass durch die fehlenden Verzeichnisse die Daten in einigen Unternehmen dann tatsächlich verloren gingen.

Ein sehr wichtiger Punkt sei auch das Bewusstsein über die Wahrnehmung der Kunden. Der beste Datenschutz in Theorie und Praxis bringe wenig, wenn den Kunden nicht das Gefühl von Sicherheit vermittelt werden könne. Dazu sei v.a. eine gute Kommunikation und Transparenz nötig. Diesem Ansatz komme das DSG mit seinen offenen Formulierungen entgegen. Gerade den Juristen falle es jedoch schwer, die sich daraus ergebenden Werturteile zu fällen. Tendenziell werde restriktiv ausgelegt, um auf der sicheren Seite zu sein.

Angesichts dieser Tatsachen stellte ROSENTHAL die rhetorische Frage, ob wir denn wirklich vor einem Problem stünden. Dass dem allenfalls nicht so sei, lasse sich auch daran erkennen, dass viele Unternehmen gar nicht mit Auskunfts- und Berichtigungsbegehren konfrontiert seien. Hinsichtlich der denkbaren Handlungsoptionen merkte ROSENTHAL an, dass Regeln immer zu wenig weit oder zu weit gehen würden. Entscheidend seien die sich verändernden sozialen Realitäten. Die gesellschaftlichen und damit die gesetzlichen Wertungen würden einer grossen Dynamik unterliegen. Vorzuziehen seien daher weniger und offenere Bestimmungen, die diese Wertungen zulieszen; dies auch auf Kosten der Rechtssicherheit.

VIII. Diskussion

Dr. BRUNO BAERISWYL, Datenschutzbeauftragter des Kantons Zürich, merkte einleitend an, dass eine Revision des DSG bestimmte Punkte in den Fokus rücken sollte, die dann eingehend überarbeitet werden. Prof. Dr. HANS RUDOLF TRÜEB, Rechtsanwalt in Zürich, wies auf bestehende Unsicherheiten in der Praxis hin. Die Probleme reichten von einfachen grenzüberschreitenden Telefonverzeichnissen im Intranet bis hin zu GPS-Chips für diebstahlgefährdete Bagger. In Bezug auf die Regulierung warf TRÜEB die Frage auf, weshalb man nicht wieder zu den Grundsätzen zurückkehre. THÜR sah das ähnlich, merkte jedoch an, dass die durch die technische Entwicklung entstehenden Lücken geschlossen werden müssten. Gerade aufgrund der technischen Entwicklung sei aber eine Regulierung bis ins Detail wenig sinnvoll. Dr. BRUNO GLAUS, Rechtsanwalt in Zürich, sah den Handlungsbedarf nicht bei den Grundsätzen, sondern bei der Rechtsdurchsetzung. Diese sei für den Normalbürger momentan zu aufwändig.

Einen anderen zentralen Punkt zeigte HARTUNG in der Zuordnung der Verantwortlichkeit auf. ROSENTHAL knüpfte hier an und stellte fest, dass in der Schweiz jeder, der an der Datenbearbeitung mitwirke, verantwortlich sei. Damit gehe die Schweiz weiter als die EU. Überhaupt sei das DSG sehr gut austariert. Partielle Anpassungen im Rahmen von Harmonisierungsbestrebungen mit der EU wären daher der falsche Weg.

Im Bereich des Urheberrechts sprach BAERISWYL den Aspekt der Gratiskultur und das öffentliche sowie die wirtschaftlichen Interessen an. Bezüglich der Letzteren verwies THOUVENIN auf die Leer-



trägervergütung, die so auszugestalten sei, dass ein angemessener Ertrag resultiere. Das öffentliche Interesse wäre nur tangiert, wenn zu wenig Literatur und Kunst geschaffen würden. Momentan lasse sich jedoch eher das Gegenteil beobachten.