Bundesministerium
des Innern

Alexander von Humboldt
INSTITUT FÜR INTERNET
UND GESELLSCHAFT

Panel 2

Angemessene Regelungen für Privatpersonen und „alltägliche Datenverarbeitung“

Datenschutz im 21. Jahrhundert

Konferenz zum Datenschutz im 21. Jahrhundert

Empfehlungen aus dem Workshop 2

Angemessene Regelungen für Privatpersonen und „alltägliche Datenverarbeitung"

Die Teilnehmer des Workshops am 29. August 2012 fordern überwiegend eine **Stärkung des Datenschutzes durch Konzentration** der Gesetzgebung auf die wesentlichen Fragen, d.h. auf die Regeln zur Vermeidung besonderer Risiken für das Persönlichkeitsrecht, die durch Datenverarbeitung entstehen. Sie fordern ferner die **Vereinfachung** des Datenschutzrechts und **sachnähere, rechtssichere und besser durchsetzbare Regelungen**. Das Datenschutzrecht soll das individuelle Persönlichkeitsrecht und andere, ebenfalls grundrechtlich gewährleistete Rechtspositionen des Einzelnen (einschließlich der wirtschaftlichen Entfaltungsfreiheit) schützen. Bei einer Fortsetzung der bisherigen Rechtsentwicklung könnte es sich jedoch zu einem Instrument der Freiheitsbeschränkung entwickeln. Datenschutz darf insbesondere nicht die Meinungs- und Äußerungsfreiheit einengen. Er muss in ein angemessenes Verhältnis zu den anderen Grundrechten der Individuen gesetzt und mit anderen Rechtsmaterien, die sich auf den Umgang mit Informationen beziehen, besser abgestimmt werden.

Daraus folgen Empfehlungen zur Änderung des geltenden Rechts wie auch zur Verbesserung des Entwurfs einer Datenschutz-Grundverordnung der Europäischen Union:

- Verzicht auf die rechtliche Regelung der **Zulässigkeit** solcher Formen der Informationsverarbeitung, die zum normalen „alltäglichen" Zusammenleben der Menschen gehören und keine besonderen Risiken für Persönlichkeitsrechte oder andere Freiheitsrechte mit sich bringen; statt dessen Nutzung der Vielfalt möglicher rechtlicher Regelungen (eingegrenzte Verbote; Sorgfalts- und Vorsichtsmaßnahmen; Verfahrensvorkehrungen usw. im Sinne einer allgemeinen Gefahrenabwehr), die den relevanten Gefahren gezielter entgegengesetzt werden können als das pauschale Unzulässigkeitsurteil.
- Risikoorientierte **Differenzierung** nach *Sachgebieten* und Problemfeldern einerseits, nach *Methoden* der Informationsverarbeitung andererseits (Beispiele im Anhang). Einige allgemeine Regelungen sollten „vor die Klammer gezogen" werden.

Dementsprechend muss der **Anwendungsbereich** der Datenschutznormen eingegrenzt werden. Es ist nicht erforderlich und nicht sinnvoll, sämtliche Formen der Sammlung, Verarbeitung und Verwendung personenbezogener Daten durch Private unter den Vorbehalt einer gesetzlichen Ermächtigung zu stellen. (Der Vorbehalt des

Gesetzes gilt jedoch für alle öffentlichen Stellen; diese sind hier nicht mit gemeint.) Der Ausnahmevorschlag des EU-VO-Entwurfs (Art. 6 Abs. 2 Buchstabe f)) – Verarbeitung durch „natürliche Personen zu ausschließlich persönlichen oder familiären Zwecken ohne jede Gewinnerzielungsabsicht" – bedarf jedoch der Überarbeitung (vgl. Anhang zu 2.).

Es ist nicht angemessen, den **Personenbezug** von Daten extensiv zu verstehen. Es sollte vielmehr darauf ankommen, ob der Verarbeiter bzw. Anwender ohne erst aufwendig zu beschaffendes Zusatzwissen auf eine bestimmte Person schließen kann. Die Definition in § 3 Abs. 1 BDSG („bestimmbar") ist entsprechend auszulegen. IP-Adressen sind danach keine personenbezogenen Daten. Sachinformationen dürfen nicht etwa deshalb zu personenbezogenen Daten umgedeutet werden, weil sie notwendigerweise immer auch Urheber und Empfänger haben.

Nach einer anderen Meinung ist es heute überhaupt nicht mehr sinnvoll, zwischen Daten mit und ohne Personenbezug zu unterscheiden. Auch bei schwachem Personenbezug könnten strenge Datenschutzregelungen angebracht sein und umgekehrt.

Die allgemeinen Artikel des Entwurfs der EU-Grundverordnung sind nach vielfach geäußerter Meinung aus dem Workshop zum Teil zu weit gefasst, inhaltlich fragwürdig oder überflüssig:

- Der strenge **Zweckbindungsgrundsatz** (Art. 5 Buchstabe b)) ist im Bereich der privaten Informationssammlung freiheitsfeindlich und daher unangemessen; die dadurch bedingte Mehrfacherhebung vieler Daten ist nicht mehr zeitgemäß.
- Die **allgemeinen Regeln über die Zulässigkeit der Verarbeitung** (Art. 6) sollten wesentlich gestrafft werden. Insbesondere das „principle of legality", das in seiner konsequenten Fassung zum „Verbot mit Erlaubnisvorbehalt" führt, erweckt zwar den Anschein streng rechtsstaatlicher Bedingungen der Informationsverarbeitung, kann diese Funktion aber wegen der zahlreichen unbestimmten Begriffe sowie des komplizierten Systems von Ausnahmen und Gegenausnahmen nicht erfüllen. Die notwendigen **Konkretisierungen** für die verschiedenen „Bereiche und Verarbeitungssituationen" sollen nach dem Entwurf von der *Kommission* beschlossen werden (Art. 6 Abs. 5); damit wird ihr die entscheidende Regelungsmacht übertragen, was auf große Bedenken stößt.
- Teilweise wird auch gefordert, die umfangreichen Vorschriften über **Transparenz** und **Informationspflichten** zu straffen. Transparenz ist wichtig, aber die Ausgestaltung der Informationspflichten in Art. 11 bis 15 des Entwurfs ist teilweise unbestimmt und teilweise unverhältnismäßig, weil für viele Fälle nicht praktikabel. Transparenzpflichten sollten auf solche Datenverarbeitungen beschränkt werden, die besondere Risiken mit sich bringen und mit denen die Betroffenen nicht rechnen müssen.

- Gefordert wird auch, die **Auftragsdatenverarbeitung** zweckmäßiger zu regeln. Sie ist heute die typische Form der Datenverarbeitung und muss praktikabel ausgestaltet sein. Besondere Anforderungen an die Vertragsgestaltung, Kontrolle und Sanktionen sollten nur dort gestellt werden, wo die Risiken dies rechtfertigen.
- Funktion und Stellung der **Aufsichtsbehörden** sind zu überdenken. Sie sind auch bei bester Ausstattung nicht in der Lage, das gesamte riesige Feld der Datenverarbeitung auf Einhaltung aller gesetzlichen Vorschriften zu überwachen, und diese umfassende Kontrolle ist auch nicht notwendig, da die allermeisten Datenverarbeitungsvorgänge gesetzeskonform durchgeführt werden. Es kann auch nicht Aufgabe der Datenschutzbehörden sein, die Ausübung der Meinungs- und Kommunikationsfreiheit zu überwachen. Die unter dem Titel des Datenschutzes verfolgten Interessen können überdies zum Teil sachgerechter als Maßnahmen des *Verbraucherschutzes* durchgesetzt werden. Tatsächlich werden die Aufsichtsbehörden und Beauftragten einerseits vielfach mit Bagatellfällen befasst, sind andererseits aber gegenüber den großen internationalen Konzernen kaum durchsetzungsfähig. Das wird sich auch durch die vom EuGH geforderte „völlige Unabhängigkeit" von den Regierungen nicht ändern. (Die Forderung des EuGH ist ihrerseits unter dem Aspekt der demokratischen Legitimation allen amtlichen Handelns bedenklich.) *Konzentration* auf die wichtigsten Angelegenheiten wäre also auch insofern zu wünschen.
- Ein neuer Ansatz wird auch für die Kontrolle von **Einwilligungen** im Rahmen **Allgemeiner Geschäftsbedingungen** gefordert, die bisher zu lang und unverständlich und damit im Grunde nicht einwilligungsfähig sind. Ein Vorschlag geht dahin, regulierte Standard-Einwilligungsklauseln zu benutzen, die mit individuellen Zusätzen angereichert werden könnten.
- Das in dem VO-Entwurf vorgesehene **Kohärenzverfahren** dürfte nicht ausreichen, um die nötige Rechtssicherheit zu schaffen. Infolge der Unbestimmtheit und Kompliziertheit der vorgesehenen Normen werden zahlreiche Prozesse geführt werden; Klarheit wird dann erst nach Jahren durch den EuGH geschaffen werden.
- Insgesamt ist angesichts der zahlreichen Verbesserungswünsche die Rechtsform der unmittelbar verbindlichen **EU-Verordnung** unangemessen; die Fortentwicklung des Datenschutzes sollte durch eine neue **Richtlinie** bewirkt werden.

Anhang: Ansätze zur Abgrenzung der „besonders riskanten" von der „alltäglichen" Informationsverarbeitung

1. Zum Verfahren:

Wird auf den allgemeinen Grundsatz verzichtet, dass jede Form der Informations-(Daten)-verarbeitung einer gesetzlichen Grundlage bedarf, so brauchen zunächst nur die „riskanten" Vorgänge geregelt zu werden; was nicht geregelt ist, ist jedenfalls nicht ausdrücklich verboten (sondern u.U. durch Richterrecht oder Gewohnheitsrecht oder punktuell durch Spezialvorschriften geregelt). Für die nicht riskante „alltägliche" Informationsverarbeitung genügen dann allgemeine Bestimmungen etwa zur Transparenz.

Für die Beibehaltung des bisherigen Regelungsprinzips – **generelles Verbot und zahlreiche Erlaubnisnormen** – sprechen die (freilich recht kurze) Tradition und das Argument, dass dabei keine Regelungslücke entsteht. Dagegen ist einzuwenden, dass der Regelungsbereich viel zu groß ist, als dass durchgängig sachgerechte Normen zur Anwendung kommen können. Es entsteht immer wieder Rechtsunsicherheit und letztlich sogar das Gefühl vieler Bürger, das Datenschutzrecht werde nicht beachtet. Der Neuansatz wäre eine Chance für das Parlament, auf konkrete Sorgen und Ängste der Bürger konkret einzugehen und es nicht bei allgemeinen Sympathiebekundungen zu belassen.

Es wäre daher angebracht, die verschiedenen Formen der Informationsverarbeitung in zwei oder mehr **Stufen** zu regeln: auf der einen Stufe die „schweren Fälle" von Persönlichkeitsgefährdung und auf der oder den anderen die leichteren, bei denen entsprechend weniger Überwachung erforderlich ist. Ob die einen als Ausnahme der anderen angesehen werden sollen, ist nur eine Formulierungsfrage.

2. Kriterien der Abgrenzung

Art. 2 Abs. 2 Buchstabe d) des EU-Entwurfs stellt einen nützlichen Ansatz für die „Entbürokratisierung" der **privaten bzw. familiären Informationsverarbeitung** dar. Das Tatbestandsmerkmal „ohne jede Gewinnerzielungsabsicht" sollte gestrichen werden, denn auch bei Bestehen dieser Absicht ist es nicht zwingend, das gesamte Datenschutzrecht anzuwenden. Die Sanktionierung etwaiger Beeinträchtigungen fremder Persönlichkeitsrechte durch private Informationsvorgänge i.S. von Art. 2 Abs. 2 kann nach Deliktsrecht (§ 823 BGB) erfolgen (einschließlich Beseitigungs- und Unterlassungsansprüche gemäß § 1004 BGB). Zu erwägen ist auch eine Anknüpfung an § 14 BGB („Unternehmer"-Begriff).

Als Kriterien für die Abgrenzung „harmloser" von „gefährlichen" Verarbeitungsweisen kommen ferner in Betracht: die **Sensibilität** der Informationen (vgl. Art. 9 des VO-Entwurfs; die Datenart reicht aber zur Beurteilung des Informationsvorgangs nicht aus!), die **Heimlichkeit** bzw. Offenheit ihrer Erhebung oder Verwertung (Intransparenz als Grund für Misstrauen), der notwendige Schutz von **Vertrauensbeziehungen** (besondere Berufsgeheimnisse), das Gewicht der befürchteten **Nachteile** u.ä.

3. Beispiele für regelungsbedürftige Vorgänge

- Systematische **Auswertung** von Datensammlungen durch „Unternehmer" (im Unterschied zur deutlich weniger riskanten bloßen Sammlung und Speicherung von Daten). Die Erstellung von **„Profilen"** ist häufig, aber nicht immer eine Persönlichkeitsgefährdung. Sie ist regelungsbedürftig, wenn eine Mehrzahl von (insbesondere sensiblen) Dateien oder von solchen Dateien ausgewertet wird, die ursprünglich unterschiedlichen Zwecken dienten. Hier könnten auch Transparenzpflichten ein „Gegenmittel" darstellen.
- Grundsätzlich „riskant" ist die **Veröffentlichung** persönlicher Daten im Internet. Aber gerade diese Form der Informations-„verarbeitung" muss um der *Kommunikationsfreiheit* willen grundsätzlich zulässig sein und darf nicht unter eine behördliche (Vor-)Zensur fallen. Die „Medienfreiheit" begünstigt nicht nur die wirtschaftlich organisierte Presse, sondern umfasst auch ein *„Laienprivileg"*.
- Nach dem Beispiel des schwedischen Datenschutzrechts könnte darauf abgestellt werden, ob eine Datensammlung so **strukturiert** ist, dass die Gefahren der automatisierten Verarbeitung sich ohne weiteres verwirklichen können oder nicht (dies war aber unter den Teilnehmern strittig).
- **Videoüberwachung** ist in so vielen Zusammenhängen üblich, dass eine allgemeine Regelung sinnvoll erscheint (Hinweispflicht, Löschungsfristen, Auskunftsrecht? Vgl. § 6b BDSG).

4. Beispiele für zu behandelnde Sach- und Problembereiche (zu prüfende Maßnahmen)

- **Arbeitswelt**: Leistungskontrollen; unmittelbare Überwachung der Tätigkeit durch technische Mittel; „Rasterfahndung" bei großen Teilen der Beschäftigten;
- **Kreditauskunfteien**: richtige Auswahl der Datenarten, laufende Richtigkeitskontrolle, Verbot nachteiliger Entscheidungen allein aufgrund automatisierter Datenverarbeitung (§ 6a BDSG, wird zu wenig beachtet), *Scoring* als umstrittene Grundlage wirtschaftlicher Entscheidungen (Weiterentwicklung von § 29b BDSG);
- **Mitgliedschaftsverwaltung:** allgemeine Regelung der Zweckentfremdung von Mitgliederdaten von Vereinen etc.;

- **Auswertung von Kundendaten** („Data Mining“ usw.) zu Zwecken der **Direktwerbung und Marktforschung:** Vereinfachung der geltenden Regelung, Klärung unbestimmter Vorschriften;
- **Soziale Netzwerke:** mehr Transparenz, insbesondere verständliche AGB und Erläuterungen; automatische Löschung nach bestimmten Fristen; Verbot der Nachverfolgung (tracking), datenschutzfreundliche Voreinstellungen u.ä.;
- **E-Mail-Systeme**: strenge Abschottung von anderen Systemen;
- **„Internet der Dinge“** (RFID, „smart meter“ usw.): Einwilligung der jeweils Betroffenen wäre unmöglich, also „objektive“ Regelung notwendig. Welche Gefahren bestehen wirklich für Persönlichkeitsrechte? Die Regelung über „mobile personenbezogene Speicher- und Verarbeitungsmedien“ in § 6c BDSG überprüfen;
- **Umgang mit Gesundheitsdaten:** Harmonisierung und Vereinfachung der verschiedenen Regelungen im und außerhalb des Sozialgesetzbuches.

Kontrollfrage: Was wäre anders, wenn die allgemeinen Vorschriften wie das „Verbotsprinzip“ oder Art. 5 ff. der EG-VO wegfielen und nur sachgerechte bereichsspezifische Regelungen in Kraft wären, wie sie hier zu 3. und 4. vorgeschlagen werden (und evtl. ergänzt werden müssten)?

Zusammenstellung: Hans Peter Bull

Fragen für Panel 2
Angemessene Regelungen für Privatpersonen und „alltägliche Datenverarbeitung“

I. Reformbedarf

- Sind die Regelungen zur Ausnahme von Privatpersonen[1] im Lichte der Lindqvist-Entscheidung im Zeitalter des Internets noch angemessen?
- Welche Folgen hätte es, wenn man das Datenschutzrecht auf Privatpersonen und „alltägliche Datenverarbeitungen“ konsequent anwenden würde? Müssten die Datenschutz-Aufsichtsbehörden z.B. die Nutzer sozialer Netzwerke und die von ihnen eingestellten Inhalte kontrollieren? Wäre eine „konsequente Anwendung“ überhaupt umsetzbar? (Stichpunkt: Vollzugsdefizit)
- Müssen wir unterscheiden zwischen Datenverarbeitungen, die weniger und stärker regelungsbedürftig sind?
- Bedarf es eines speziellen Erlaubnistatbestandes zur Veröffentlichung von personenbezogenen Daten im Internet? Wäre ein allgemeines Verbot mit Erlaubnistatbestand bei Veröffentlichungen mit den überkommenen Grundsätzen des Äußerungs-, Presse- und Medienrechts sowie Art. 5 GG vereinbar?

II. Reformmöglichkeiten

1. Abgrenzungskriterien

- Ist die Person des Verarbeitenden (z.B. Privatpersonen im Gegensatz zu Unternehmen) der geeignete Anknüpfungspunkt für die Unterscheidung?
- Ist der Gesichtspunkt der Gewinnerzielungsabsicht ein geeignetes Kriterium?
- Wäre die Größe des Empfängerkreises bei Veröffentlichungen ein geeignetes Abgrenzungskriterium?
- Sollte man zwischen gefährlichen und weniger gefährlichen („alltäglichen“) Datenverarbeitungen unterscheiden? Passt für diese Unterscheidung der Begriff der „alltäglichen Datenverarbeitung“ („ordinary processing“)?
- Welche weiteren Kriterien könnten herangezogen werden, um eine eher geringe Gefährdung der Privatsphäre bzw. von Persönlichkeitsrechten zu beschreiben?
    - Inhalte der Verarbeitung bzw. der Kommunikation?
    - Struktur bzw. Zielrichtung der Datenverarbeitung? (Ansatz Schweden)
    - Kontext, Zweck der Verarbeitung bzw. der Kommunikation?
    - Eingriffsintensität/Risiken des konkreten Verarbeitungsvorgangs?
    - „Informationelles Machtgefälle“ zwischen Datenverarbeiter und Betroffenen?

---

[1] Art. 3 Abs. 2 2. Spiegelstrich Richtlinie 95/46, § 1 Absatz 3 BDSG sowie Art. 2 Abs. 2 Buchstabe d Entwurf Datenschutz-Grundverordnung.

2. Rechtssystematische Umsetzung der Unterscheidung

- Sollte man die „alltägliche Datenverarbeitung" oder Privatpersonen gänzlich aus dem Datenschutzrecht herausnehmen („Ausnahme-Lösung") und auf andere Rechtsgebiete verweisen (z.B. bürgerliches Recht, Schadensersatz- und Unterlassungsansprüche)?
- Ist eine „positive" Definition von alltäglichen, weniger gefährlichen Datenverarbeitungen überhaupt sinnvoll oder sollte man sich darauf konzentrieren, die gefährlicheren bzw. risikoreicheren Datenverarbeitungen gesetzlich näher zu beschreiben?
- Wären z.B. Veröffentlichungen weniger oder stärker gefährdende Datenverarbeitungen? Wie können Wertungswidersprüche zum Äußerungs- und Presserecht bzw. Medienrecht aufgelöst werden, wenn z.B. der Grundsatz gilt, dass es keine behördliche Kontrolle von Inhalten gibt? Sollte für Veröffentlichungen insgesamt auf das Äußerungs-, Presse und Medienrecht verwiesen werden?
- Sollte man die „alltägliche" Datenverarbeitung als allgemeine Datenverarbeitung voll in das Datenschutzrecht aufnehmen, dafür aber ein „vereinfachtes Schutzregime" mit leichter Handhabbarkeit schaffen („Regelungs-Lösung")?
- Könnten ein vereinfachtes Schutzregime den „Allgemeinen Teil" des Datenschutzrechts bilden und Datenverarbeitungen, die das Persönlichkeitsrecht stärker gefährden, in einem „Besonderen Teil" geregelt werden?

3. Regelungen für gering gefährdende (allgemeine) Datenverarbeitungen

- Wie könnte die Ausgestaltung eines „vereinfachten Schutzregimes" aussehen?
- Sollte man vom Verbot mit Erlaubnisvorbehalt abweichen und stattdessen allgemeine Gebote regeln, aus denen sich Schutzrechte der Betroffenen ableiten (z.B. „Wer automatisiert Daten verarbeitet, hat dabei die Persönlichkeitsrechte des Betroffenen zu achten")?
- Wie ließe sich sonst eine allgemeine Zulässigkeit der Datenverarbeitung regeln, wenn schutzwürdige Interessen des Betroffenen offensichtlich nicht beeinträchtigt werden?
- Wie könnten die Abwägungen mit anderen Rechten bzw. schutzwürdigen Interessen bei „alltäglichen Datenverarbeitungen" ausgestaltet werden?
- Sollte es anlassunabhängige Kontrollen und Sanktionen bei „objektiven" Verstößen geben oder das Antrags- bzw. Beschwerdeprinzip gelten?
- Sollten Sanktionen auf einer ersten Stufe (allgemeine Prävention) oder erst auf einer zweiten Stufe (Missbrauch und tatsächliche Verletzungen von Persönlichkeitsverletzungen) ansetzen?
- Sollte die Beweislast beim Betroffenen liegen?
- Sollte es ein anderes Haftungsregime im Vergleich zu gefährlicheren Datenverarbeitungen geben?
- Sollten z.B. Informations- und Nachweispflichten bei alltäglichen Datenverarbeitungen gelockert werden?

Teilnehmer des Workshops 2 am 29. August 2012

Angemessene Regelungen für Privatpersonen und „alltägliche Datenverarbeitung“

Rechtsanwalt

Universität Hamburg

Ruhr-Universität Bochum

1&1

Landesminister a.D., Universität Hamburg

Humboldt Universität zu Berlin

Verband Deutscher Zeitschriftenverleger e.V.

Infino - Institut für Informationsordnung e.V.

Rechtsanwalt

Landesbeauftragter für den Datenschutz Baden-Württemberg

Humboldt Universität zu Berlin

Bayerisches Landesamt für Datenschutzaufsicht

Universität Regensburg

Humboldt Universität zu Berlin

Universität Bielefeld

Berliner Datenschutzrunde

ISOC, Internet Society German Chapter e.V.

Stockholm University

Rechtsanwalt

Ministry of Justice, Sweden

The Danish Ministry of Justice

GSM Association London

Council of Europe

Latham & Watkins LLP Frankfurt/Main