Bundesministerium
des Innern

Alexander von Humboldt
INSTITUT FÜR INTERNET
UND GESELLSCHAFT

Panel 1

Stärkere Regelungen für besondere Gefährdungen des allgemeinen Persönlichkeitsrechts

Datenschutz im 21. Jahrhundert

Konferenz zum Datenschutz im 21. Jahrhundert

Empfehlungen aus dem Workshop 1

Stärkere Regelungen für besondere Gefährdungen des allgemeinen Persönlichkeitsrechts

Die Experten des vorbereitenden Workshops am 28. August 2012 regen an, im Rahmen der Europäischen Gesetzgebung einer Datenschutz-Grundverordnung folgende Aspekte in Erwägung zu ziehen:

I. Reformbedarf

Das Datenschutzrecht im 21. Jahrhundert muss den Herausforderungen der Informationsgesellschaft angepasst werden. Wie bisher im deutschen Recht üblich, sollte der Anwendungsbereich eines modernen Datenschutzrechts breit definiert werden. Es erscheint nach wie vor sinnvoller, Einzelprobleme durch Ausnahmeregelungen zu lösen, als Vorfestlegungen über einen zu engen Anwendungsbereich zu treffen, die man später nur schwer korrigieren kann. Die vorhandenen Fundamente müssen allerdings weiterentwickelt werden:

- Hierfür bietet sich das in der Datenschutzliteratur diskutierte **Schutzzielkonzept** an. Datenverarbeitende Unternehmen sind heute weniger an Kausalitäten als an Korrelationen interessiert. Aus diesem Grund gibt es ein großes wirtschaftliches Interesse, große Datenpools zu erstellen („Big Data"). Umstritten blieb, ob auch die Datenvermeidung als legitimes Schutzziel anerkannt bleiben sollte.

- Ein weiterer Reformbaustein kann mit **System- und Selbstdatenschutz** umschrieben werden. Insbesondere eine Pflicht zur **Anonymisierung** und **Pseudonymisierung** sollten in den Entwurf der DS-GVO Eingang finden, weil sie eine differenzierte Anwendung des Datenschutzrechts auf bestimmte Datenkategorien erlauben. Dabei sollten auch Vorgaben für die Bedingungen der Aufhebung von Pseudonymen gemacht werden.

- Flankiert werden könnten Schutzzielkonzept und Systemdatenschutz durch Zertifizierungsansätze, etwa in Form von **Datenschutzsiegeln**.

- Wünschenswert erscheint eine Konkretisierung der Voreinstellungen, so dass etwa als Regel: "keine Weitergabe" festgelegt wird (Ergänzung zu Art. 23 des Entwurfs der DS-GVO).

- Der durch den Entwurf befürchteten Abwertung der Einwilligung könnte mit im Verbraucherschutzrecht diskutierten Lösungsmodellen entgegengetreten werden. Zu denken ist etwa an eine **Ampellösung**; auch eine Kurzzusammenfassung der einwilligungsrelevanten Informationen wäre begrüßenswert.

- Der Katalog des Art. 33 Abs. 2 DS-GVO bietet bereits sinnvolle Anknüpfungspunkte für die Regelung **risikoreicher Datenverarbeitung**. Allerdings könnte dieser Katalog noch ergänzt werden um folgende Kriterien:
  - Heimlichkeit der Datenerhebung und -verarbeitung
  - Besondere Vertrauenserwartung

  Ggf. könnten diese besonderen Kriterien auch als Abwägungsleitlinien rechtlich fruchtbar gemacht werden.

- Die **Videoüberwachung** könnte als gesonderte Gefährdung in einen gesonderten Tatbestand aufgenommen werden.

II. Zusätzliche Reformmöglichkeiten

- Diskussionsbedarf besteht weiterhin hinsichtlich der **besonderen Kategorien von personenbezogenen Daten** (Art. 9 Abs. 1 DS-GVO). Die im Entwurf genannten Datenarten sollten zwar beibehalten werden, sie können jedoch die Gefährdungen nicht abschließend und zukunftsoffen erfassen. (1) Für eine Öffnung spricht, dass sich gesellschaftlich gesehen verändert, was als sensitives Datum betrachtet wird. (2) Dagegen wurde vorgebracht, dass ein offener Katalog zu mehr Rechtsunsicherheit führen könnte. (3) Allerdings haben wir, etwa bei den Regelbeispielen im Strafrecht, Erfahrungen mit offenen Katalogen gemacht, an die harte Rechtsfolgen geknüpft werden. (4) Bei einer Öffnung wäre freilich die Frage zu klären, wer darüber entscheiden soll, ob neue Gefährdungen mit den gegenwärtig genannten Katalogdaten des Art. 9 DS-GVO gleichzusetzen sind. Dies sollten die unabhängigen Datenschutzbehörden in einem europaweit abgestimmten Verfahren tun.

- Das Verhältnis zwischen dem besonderen Schutz des Art. 9 DS-GVO und dem allgemeinen Art. 6 DS-GVO ist klarzustellen.

Zusammenstellung: Anna-Bettina Kaiser
Alexander Dix

Fragen für Panel 1
Stärkere Regelungen für besondere Gefährdungen des allgemeinen Persönlichkeitsrechts

I. Reformbedarf

- Wo liegen aktuell die größten Gefahren für die Persönlichkeitsrechte (z.B. Profiling durch Cookies oder Hinzuziehung sämtlicher – auch im dark web – verfügbarer Daten)?
- Wie kann ein risikoadäquater Datenschutz rechtlich realisiert werden? Ist es zutreffend, dass nach geltendem Recht die Risikoeinschätzung regelmäßig erst im Rahmen der Verhältnismäßigkeitsprüfung vorgenommen wird? Wenn ja, welches sind hierfür die Maßstäbe?
- Soll die Einschätzung des Risikos im Wesentlichen den Datenschutzaufsichtsbehörden obliegen, gibt es für sie einen Einschätzungsspielraum oder entscheiden letztlich die Gerichte?

II. Reformmöglichkeiten

1. Anknüpfungspunkte

- Ist es sinnvoll und geboten, spezielle Regelungen für besondere Gefährdungen des allgemeinen Persönlichkeitsrechts (im Sinne eines Risikomodells) vorzusehen?
- An welchem Schutzgut müssten Regelungen für besondere Gefährdungen anknüpfen: der Privatsphäre[1], dem allgemeinen Persönlichkeitsrecht[2] oder dem personenbezogenen Datum an sich[3]? Sollte auch das vom Bundesverfassungsgericht beschriebene Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als Schutzgut in das Datenschutzrecht aufgenommen und näher ausgestaltet werden?
- Welche besonderen Gefährdungen sind regelungsbedürftig und wie ließen sich diese rechtlich kategorisieren?
- Bietet der Katalog in Art. 33 Abs. 2 Datenschutz-Grundverordnungs-Entwurf bereits die richtigen und ausreichenden Anknüpfungspunkte für die Regelung risikoreicher Datenverarbeitungen?

---

[1] Vgl. Art. 1 Abs. 1 EG-Datenschutz-Richtlinie 95/56 (deutsche Sprachfassung), Art. 7 EU-Grundrechte-Charta; in Art. 1 der Datenschutzkonvention 108 des Europarates heißt es in der dt. Sprachfassung „Recht auf einen Persönlichkeitsbereich"; in den englischen Sprachfassungen jeweils „Privacy".

[2] Vgl. § 1 Abs. 1 BDSG sowie die Herleitung des Rechts auf informationelle Selbstbestimmung durch das Bundesverfassungsgericht (BVerfGE 65, 1).

[3] Vgl. Art. 8 EU-Grundrechte-Charta und Art. 16 Abs. 1 AEUV

- Sind folgende (weitere) Kategorisierungen denkbar und wie könnten sie – im Hinblick auf die Annahme einer besonderen Gefährdung – ggf. präzisiert werden:
  - Sensibilität der Daten aufgrund ihres Inhalts (Regelbeispiele)
  - Besonderer Vertrauensschutz aufgrund des Kontextes bei der Erhebung bzw. Verarbeitung (z.B.: Nutzer hat begründete Erwartung einer besonders geschützten Privatsphäre, etwa bei „Veröffentlichungen" von personenbezogenen Daten in geschlossenen Nutzerkreisen sozialer Netzwerke, oder bei der Nutzung von Suchmaschinen)
  - Unterscheidung offline-Welt vom Internet
  - Heimliche Erhebung und Verarbeitung
  - Besonders intensive Datenverarbeitung, z.B. aufgrund des Verwendungszwecks (Profilbildung), einer erhöhten Gefahr unzulässiger Verarbeitung (Vielzahl Zugriffsberechtigter/Empfänger, Verknüpfungsmöglichkeiten) oder besonders schwerwiegender Nachteile (irreversibel, potentiell diskriminierend, schwerwiegende Verletzungen der Intimsphäre oder der persönlichen Ehre)?

2. Beschränkungen bzw. besondere Pflichten/Regelungen

- Sind Fälle denkbar, in denen die konkrete Datenverarbeitung im Interesse des Persönlichkeitsschutzes absolut verboten sein sollte? Wenn ja, welche?
- In welchen Fällen sollte die Datenverarbeitung von einer vorherigen behördlichen Genehmigung[4] abhängig gemacht werden sollten? Wenn ja, durch wen?
- Sind Fälle denkbar, in denen Einwilligungen des Betroffenen als Legitimation einer Datenverarbeitung ausgeschlossen werden sollten? Wenn ja, welche?
- Ansonsten: Wie sollte das Schutzkonzept bei besonderen Gefährdungen gestaltet sein? Wie sollten Regelungen für bestimmte Daten, Branchen, Personen (Kinder) etc. aussehen; gehören sie in einen Besonderen Teil des Datenschutzrechts?
- Wären folgende Rechtsfolgen denkbar und sinnvoll:
  - Strenge Zweckbindung oder Kontextbindung,
  - Eingeschränkte Übermittlung,
  - Koppelungsbeschränkungen von Diensten,
  - Spezifische Informationspflichten,
  - Folgenabschätzung,
  - Anonymisierungen und Pseudonymisierungen,
  - Besondere technische oder organisatorische Maßnahmen, insbesondere auch in Bezug auf die Integrität und Vertraulichkeit von IT-Systemen,
  - Vorgaben für Entwickler und Hersteller von IT-Systemen zur Gewährleistung von Systemdatenschutz,
  - Befugnisse zum Erlass dienstespezifischer oder individualisierter Maßnahmen (Auflagen, allgemeine Bedingungen),

[4] Vgl. für den öffentlichen Bereich das Zustimmungserfordernis der obersten Landesbehörden in § 10 Abs. 3 Satz 2 BDSG.

- Vermutete Haftung des Verantwortlichen,
- Schadenersatz,
- vereinfachte Unterlassungsansprüche,
- erweiterte Kontrolle, z.B. durch ergänzende allgemeine Vollzugsbehörden der Mitgliedstaaten
- Bußgelder, Strafrecht?

3. Verantwortlichkeiten

- Wer sollte Adressat welcher Maßnahmen sein?
- Sollte bei der Verantwortlichkeit nicht nur im Telemediengesetz (TMG), sondern im allgemeinen Datenschutzrecht, wie z.B. einer neuen Verordnung, in einem besonderen Teil zwischen Anbietern bzw. den (kommerziellen) Betreibern von IT-Systemen und deren Nutzern unterschieden werden? Bedarf es Regelungen zur gemeinsamen Verantwortlichkeit?
- An wessen Verantwortlichkeit sollte bei der Veröffentlichung von Daten im Internet angeknüpft werden? Sollten die Regelungen des TMG zur Verantwortlichkeit der Anbieter auf das Datenschutzrecht übertragen werden?
- Sollte die Verantwortung auch davon abhängen, in welchem Maß der Datenverarbeiter oder Betreiber eines IT-Systems (bewusst) Vertrauenstatbestände schafft?
- Wie kann die internationale Durchsetzung der Verpflichtungen sichergestellt werden; wer ist zuständig?

Teilnehmer des Workshops 1 am 28. August 2012

Stärkere Regelungen für besondere Gefährdungen des allgemeinen Persönlichkeitsrechts

Universität Mannheim

1&1

Landesminister a.D., Universität Hamburg

Landesbeauftragter für Datenschutz und Informationsfreiheit Berlin

Humboldt Universität zu Berlin

BVDW - Bundesverband Digitale Wirtschaft e.V.

Humboldt Universität zu Berlin

Bayerisches Landesamt für Datenschutzaufsicht

Humboldt Universität zu Berlin

Stockholm University

Rechtsanwalt

Universität Bonn

Humboldt Universität zu Berlin

europe versus facebook

Fachhochschule Köln

Siemens

GDV - Gesamtverband der Deutschen Versicherungswirtschaft e.V.

Council of Europe

Bayerisches Staatsministerium des Innern