ZVR-Zahl 091008066 IBAN: AT64 14000 10010672 746 BIC: BAWAATWW

Digital vernetzte Gesellschaft: Datenschutz und Datensammlung – Überwachung und Kontrolle im Netz

Vortrag am 19. 2. 2014 von **Mag. Dr. Eva Souhrada-Kirchmayer**: Juristin und Absolventin der Europaakademie, langjährige Erfahrung als Expertin für Datenschutz, u. a. im Bundeskanzleramt, von 2010 bis Ende 2013 Leiterin der Geschäftsstelle der Datenschutzkommission und deren geschäftsführendes Mitglied, Datenschutzbeauftragte des Europarates; seit 1. 1. 2014 Richterin am Bundesverwaltungsgericht.

Zusammenfassung:

Datenschutz zählt nach europäischem Verständnis zu den Grund- und Freiheitsrechten. Die Europäische Datenschutzkonvention des Europarates ist Grundlage der EU-Datenschutz-Richtlinie und entsprechender nationaler Datenschutzgesetze. Im Österreichischen Datenschutzgesetz ist ein Grundrecht auf Datenschutz in Verfassungsrang verankert. Das Datenschutzgesetz 2000 regelt unter anderem, welche Daten als sensible Daten gelten, die Rechte der Betroffenen und die Pflichten der datenschutzrechtlichen Auftraggeber sowie den Rechtsschutz. Weil Datenschutz im Internet durch unterschiedliche nationalstaatliche Regelungen nicht einfach durchzusetzen ist, kommt einer internationalen Harmonisierung – zumindest auf EU-Ebene – besondere Bedeutung zu. Derzeit werden in der EU neue Rechtsinstrumente für den Datenschutz vorbereitet: Im Mittelpunkt stehen dabei die Stärkung der Betroffenenrechte, Aufwertung und Harmonisierung der nationalen Datenschutzbehörden und eine inhaltliche Modernisierung entsprechend der technischen Entwicklung.

Mehr zum Thema:

Das derzeit in Österreich gültige **Datenschutzgesetz (DSG 2000)** basiert auf der EU-Richtlinie zum Datenschutz aus 1995. Österreich war aber in gewisser Weise ein Vorreiter in Bezug auf Datenschutz, da bereits 1978 ein erstes Datenschutzgesetz erlassen worden war. Historisch geht Datenschutz auf die Grund- und Freiheitsrechte zurück: Bereits die Europäische Menschenrechtskonvention sieht eine Regelungen zum Schutz der Privatsphäre vor (*„jedermann […] Anspruch auf Achtung des Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs“*). 1981 wurde die **Europäische Datenschutzkonvention** des Europarates vereinbart, in welcher Grundsätze des Datenschutzes festgelegt sind (z. B. rechtliche Voraussetzungen für Datenverwendungen, Befristung der Speicherung).

Das DSG 2000 enthält ein **Grundrecht auf Datenschutz, das in Verfassungsrang steht**. In § 1 DSG 2000 wird jedermann ein Recht auf Geheimhaltung persönlicher Daten zugesichert. Behörden dürfen persönliche Daten ausschließlich auf Basis gesetzlicher Grundlagen verwenden. Privaten (z. B. Unternehmen) ist es nur bei einem überwiegenden rechtlichen Interesse und bei Einhaltung bestimmter Verpflichtungen erlaubt, personenbezogene Daten zu speichern. Organisationen, die personenbezogene Daten speichern, müssen dies beim **Datenverarbeitungsregister** melden; es gibt allerdings klar geregelte Ausnahmen, so müssen z. B. Vereine die Speicherung ihre Mitgliederdaten nicht melden, sofern sie bestimmte, in der Standard- und Musterverordnung geregelte Vorgaben einhalten.

Das DSG 2000 unterscheidet zwischen **sensiblen Daten** und nicht sensiblen Daten. Sensible Daten sind taxativ aufgezählt, dazu gehören u. a. Gesundheitsdaten, Angaben über Weltanschauung und Religion, Zugehörigkeit zu politischen Parteien und Gewerkschaften, sexuelle Orientierung und sogenannte rassische Merkmale. Jeder Auftraggeber einer Datenanwendung muss in allen Fällen für angemessene **Sicherheitsbestimmungen** sorgen: Es ist zu klären, wer Zugang zu welchen Daten hat und es sind ausreichende technische Sicherheitsmaßnahmen vorzusehen, z. B. Schutz vor Hacking, Verschlüsselung.

Die **Rechte der Betroffenen** sind ebenfalls im DSG 2000 geregelt, dazu zählen das Recht auf auf Geheimhaltung, auf Auskunft, auf Richtigstellung und Löschung. Auskunftspflicht besteht binnen acht Wochen, wird diese Frist überschritten, ist eine Beschwerde bei der Datenschutzbehörde möglich. Nur dieses Auskunftsrecht kann die Datenschutzbehörde für Betroffene sowohl bei öffentlichen als auch bei privatrechtlichen Organisationen durchsetzen, alle anderen Rechte kann sie nur bei öffentlichen Einrichtungen einfordern; gegen private Auftraggeber, z. B. Unternehmen, müssen Betroffene zivilrechtlich vorgehen, die Datenschutzbehörde hat in diesen Fällen nur Ombudsfunktion. Verletzungen des Datenschutzes können mit Verwaltungsstrafen geahndet werden oder – im Falle eines wissentlichen Bruchs, z. B. durch Hacker – auch auf Basis eigener strafrechtliche Bestimmungen. Seit 2010 ist die Frage der Videoüberwachung in einem eigenen Abschnitt des DSG 2000 geregelt. Abgesehen davon ist das DSG 2000 technologieneutral, d. h. es ist unabhängig vom Medium der Datenspeicherung einzuhalten.

Datenschutz im Internet ist nicht einfach durchzusetzen: Die Rechtslage ist durch unterschiedliche nationalstaatliche Regelungen schwierig, umso wichtiger ist eine Harmonisierung zumindest auf EU-Ebene. Alljährlich wird am europäischen Datenschutztag, am 28. Jänner, an die Auflage der Europakonvention zur Unterzeichnung erinnert. Der Europarat lädt auch Drittstaaten ein, sich diesem Abkommen anzuschließen. Derzeit gibt es zwar einige Interessenten, z. B. lateinamerikanische Staaten, aber für das Internet ganz wesentliche Länder wie die USA und China sind nicht beteiligt. Seit 2010 sind europäische datenschutzrechtliche Auftraggeber verpflichtet, Betroffene über Datendiebstahl zu informieren, sofern ihnen ein Schaden droht (**Data Breach Notification**). Diese Bestimmung muss leider auch immer wieder zum Einsatz kommen.

Der Begriff **Whistleblowing** kommt aus den USA und bezeichnet die Aufdeckung illegaler Machenschaften durch Insider. Whistleblower genießen in den USA gesetzlichen Schutz. Für Europa beschäftigte sich die Artikel-29-Datenschutzgruppe der Europäischen Union mit diesem Thema; die Arbeitsgruppe setzt sich aus VertreterInnen der nationalen Datenschutzstellen sowie der Kommission zusammen und bemüht sich generell um eine zunehmende Harmonisierung der Datenschutzregelungen und ihrer Interpretation. Die Artikel-29-Gruppe schlug vor, dass Whistleblowing unter bestimmten Voraussetzungen auch in Europa zulässig sein soll, was mittlerweile in die Rechtsprechung der Datenschutzbehörde eingeflossen ist. In Österreich gibt es bei der Wirtschafts- und Korruptionsstaatsanwaltschaft eine Meldestelle für Hinweisgeber.

Aus Sicht der USA fallen allerdings die Enthüllungen von Edward Snowden nicht unter “Whistleblowing“, da die von ihm aufgedeckten Vorgänge als legal angesehen werden. In Folge der NSA-Aufdeckungen wurde eine gemeinsame Arbeitsgruppe von DatenschutzexpertInnen aus der EU und den USA eingerichtet, in der grundsätzliche **Auffassungsunterschiede** zur Sprache kamen: Während in Europa bereits beim Sammeln und

Speichern von Daten die Verhältnismäßigkeit geprüft werden muss, werden in den USA Vorratsdaten großzügig gespeichert und Fragen der Verhältnismäßigkeit erst bei der Auswertung berücksichtigt. Zudem sind US-BürgerInnen im Datenschutzrecht der USA besser gestellt als Angehörige anderer Nationalitäten, während europäisches Datenschutzrecht – als Menschenrecht – für alle gleichermaßen gilt. Auch erlaubt die Rechtsordnung der USA den Geheimdiensten wesentlich umfassenderen Zugriff auf personenbezogene Daten als dies in vielen europäischen Ländern zulässig ist. In Österreich sind das Heeresnachrichtenamt, das Heeresabwehramt sowie das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung an klare Rechtsgrundlagen gebunden und im Verteidigungs- und Innenministerium gibt es auch Rechtsschutzbeauftragte.

Es gibt eine Fülle **internationaler Datenaustausch-Abkommen**, bekannt sind z. B. die Vereinbarungen über den Austausch von Fluggast-Daten und das SWIFT-Abkommen über den Austausch von Zahlungsverkehrsdaten.

Derzeit werden in der EU **neue Rechtsinstrumente** für den Datenschutz vorbereitet: Im Mittelpunkt stehen dabei die Stärkung der Betroffenenrechte, die Aufwertung und Harmonisierung der nationalen Datenschutzbehörden und eine inhaltliche Modernisierung entsprechend der technischen Entwicklung. Die Europäische Datenschutzkonvention des Europarates wird demgemäß überarbeitet, in Abstimmung mit den Entwürfen der Europäischen Union für eine neue Datenschutz-Grundverordnung und eine neue Richtlinie für Polizei und Justiz. Der zuständige Ausschuss des Europäischen Parlaments (LIBE, für bürgerliche Freiheiten, Justiz und Inneres) hat sich bereits im Oktober 2013 einstimmig für den vorliegenden Entwurf ausgesprochen, auf Ratsebene ist allerdings noch keine Einigung in Sicht.

Aus der Diskussion:

*Die elektronische Gesundheitsakte **ELGA** baut auf dem bestehenden dezentralen System der Verwaltung von Gesundheitsdaten auf: Bisher wurden die Daten in jedem Krankenhaus getrennt gespeichert, allerdings in nicht standardisierter Form. ELGA wird den Austausch standardisierter Daten ermöglichen, der aber nur im Behandlungsfall erfolgen darf. Alle PatientInnen haben die Möglichkeit, der elektronischen Gesundheitsakte ihre „Zustimmung" zu entziehen (Opt-Out). Der Widerstand der Ärzteschaft gegen ELGA hat viele Gründe, darunter auch Haftungsfragen. Die Information der Öffentlichkeit über ELGA ist bisher leider nicht besonders gut geglückt.*

*Der **Handel mit Adressdaten** ist Adressverlagen bei Einhaltung bestimmter Voraussetzungen gestattet und wird in der Gewerbeordnung geregelt. Adressdaten sind grundsätzlich keine sensiblen Daten. Als Quelle werden häufig auch Daten aus Kundenbindungsprogrammen herangezogen.*

*Das große Unbehagen vieler Menschen in Bezug auf Datenschutzverletzungen ist auch darin begründet, dass diese **Eingriffe in die Privatsphäre** zunächst oft unbemerkt geschehen und erst im Nachhinein bekannt werden.*

*Die neuen europäischen Rechtsinstrumente zum Datenschutz werden stärker als bisher auf die Themen **Bewusstseinsbildung** und Öffentlichkeitsarbeit eingehen. Die Österreichische Datenschutzkommission hat eine Broschüre für Jugendliche veröffentlicht, die bei der Datenschutzbehörde in gedruckter Form bestellt werden kann und auf ihrer Webseite auch zum Download angeboten wird: Du bestimmst! Datenschutz – Fakten und Gefahren*

Protokoll: Barbara Smrzka