AK „Allgegenwärtige Datenverarbeitung – Herausforderungen für den Datenschutz“

Moderation: C. Goltz
Referent: P. Schaar
Protokollant: A. M. Tschirley

Allgemeine Begrüßung durch C. Goltz; Ankündigung, dass am Ende des Vortrags Zeit für Fragen sei; Vorstellung des Herrn Schaar als Bundesdatenschutzbeauftragter in der 2. Amtszeit sowie eine kurze Zusammenfassung seiner Biographie.

P. Schaar dankt für die Einladung zum EDV-GT und beginnt mit der Frage „Was ist allgegenwärtige Datenverarbeitung?“ Zunächst wendet er sich jedoch der grundlegenderen Frage zu: „Warum EDV-Gerichtstag“. Er erklärt, dass EDV früher das Gegenstück zur MDV war. Im Umfeld der EDV entstand der Datenschutz. Somit hat der Datenschutz eigentlich schon vor dem Computerzeitalter begonnen, ist zugleich aber auch als Kind des Computerzeitalters zu sehen.

Historischer Abriss/Einleitung:
1890: Wegweisender Artikel in einer juristischen Fachzeitschrift „The right to privacy“ als Antwort auf Rechtsfragen der Fotografie. Wer darf wen fotografieren? Darf man in Häuser hinein fotografieren? Die Idee des Individualrechts entsteht als Reaktion auf eine technologische Entwicklung. Übertragen ins Jahr 2010 zeigen sich Parallelen: Mit Google Street View stehen wir erneut vor einem ähnlichen Problem. Informationen werden der weltweiten Öffentlichkeit zugänglich gemacht.
Der Datenschutz begann in den 1960er/70er in den ersten Gesetzgebungen verankert zu werden. Heutzutage spricht man überall von Informationstechnologie, E-Mail und E-Justice, Smart-Diensten und sozialen Netzwerken. Beim Thema Datenschutz denken wir sofort an das Internet und die einschlägigen Dienste wie Google Street View, facebook oder StudiVZ.
Früher wurden Lochkarten gestanzt, durch Rechenzentren verarbeitet und die Ergebnisse auf Endlospapier zugestellt. Die juristische Reaktion war es, verschiedene Rollen in der Datenverarbeitung zu definieren und Regeln vorzugeben. So sind auch im aktuellen Datenschutzrecht noch immer Begriffe wie „verantwortliche Stelle“ oder „Datenverarbeiter“ präsent. Diese Zuweisung entsprach der Realität, da damals noch die Rollen der Einzelnen unterschieden werden konnten. Die verantwortliche Stelle konnte also fast immer festgestellt werden. Auch der Auftragnehmer war zu erkennen.
Heutzutage hat sich das grundlegend geändert. Man denkt bei Daten zunächst an Handys, Notebooks, etc. Aber der Realitiät entspricht vielmehr das „ubiquitous computing“, eben die unbemerkte Allgegenwärtigkeit der Datenverarbeitung und das Verschwinden der sichtbaren Datenverarbeitung aus unserer Umwelt.
Beispiel: Ein Auto der Mittel/Oberklasse ist im Grunde genommen ein Computer/Smartphone auf Rädern – es ist ein technologiegeprägtes Gerät, mit einer Vielzahl von Chips und Schnittstellen. Die Daten entstehen dabei nicht als Selbstzweck (durch einen Auftrag), sondern vielmehr nebenbei. Hierin besteht der Unterschied zur EDV die früher hauptsächlich aufgrund eines Auftrages erfolgte und somit beabsichtigt war. Mit Lochkarte wurden Daten über Lehrer gespeichert. Die Datenschutzbeauftragten hatten dabei die Erforderlichkeit der Datenerhebung zu beurteilen. Diese Problemstruktur besteht bis heute fort.
Daneben gibt es aber in der heutigen Welt ein weiteres Problem: Datenabfall.
Erstmals trat das Problem in der digitalen Vermittlungstechnik in der Kommunikation auf, wo plötzlich eine einfache Nachverfolgung der Verbindungen möglich wurde. Daten sind bereits vorhanden, bevor die Verbindung überhaupt zustande kommt. Allein deswegen ist die Vorratsdatenspeicherung ein derart wichtiges Thema.
Aber nicht nur in der Telekommunikation mittels Internet und Smartphone (mit GPS-Empfängern, die eine unbemerkte Ortung ermöglichen), sondern auch in anderen alltäglichen Lebensbereichen

entstehen Datenspuren. So ist beim Auslesen von PKW-Chips in der Werkstatt eine Erstellung von Profilen über die Verteilung der Motorsteuerung, dessen Belastung, etc. herauszufinden.
In der Welt der Informationsverarbeitung wird unter Einsatz von Technologien wie RFID-Chips immer mehr miteinander vernetzt. Sie liefern eine Schnittstelle zwischen der Sache und der weltweiten virtuellen Welt.
Durch die Verwendung von Gegenständen, bei denen der Benutzer nicht einmal annimmt, dass es sich um datenproduzierende Geräte handelt, besteht kein Bewusstsein mehr über die Fülle der alltäglich anfallenden Daten.
Das BVerfG hat darauf hingewiesen, dass es keine unsensiblen oder harmlosen Daten gibt. Daten, die an sich nicht aussagekräftig sind, werden aber schnell in Summe und Auswertung sehr interessant. Daher stellt sich die Frage: Greifen Schutzkonzepte des Datenschutzes also überhaupt noch? Selbst Daten, die isoliert betrachtet nicht direkt als personenbezogen erkannt werden, können Personenbezug durch Hinzuziehung weiterer Daten erfolgen.

Ein Konzept des Datenschutzes von heute besteht im Schutz von Daten, die einer konkreten, bestimmbaren oder direkt bestimmten natürlichen Person zurechenbar sind. (NB: In der Europäischen Union erfolgt der Schutz auch in Bezug auf natürliche Personen).
Man muss sich also zwecks Anwendung des BDSG zunächst fragen, ob es sich bei den vorliegenden Daten um ein personenbezogenes Datum handelt. Oftmals stellt dies Probleme bei Unternehmen dar. Beispiel: Gilt die IP-Adresse als personenbezogenes Datum? Viele Unternehmen verneinen dies, weil sie nicht wissen, wer sich hinter einer Adresse verbirgt. Sie könnten es aber herausfinden! Besonders einfach wäre eine Verknüpfung bei statischen IPs. Aber auch bei dynamischen IPs lässt sich unter Hinzuziehung des Wissens des Access-Providers ebenfalls eine Verknüpfung der IP-Adresse und der dahinter stehenden Person durchführen. Daher ist das Datenschutzrecht hier ebenso anwendbar.
Zu beachten ist auch der zeitliche Aspekt. Daten die zunächst nicht personenbezogen sind, können es mit der Zeit werden. Beispiel 1: Cookies eines Betreibers und anschließende Nutzung eines persönlichen Dienstes des Betreibers, z.B. bei Bestellungen. Dadurch wird die Person dem Unternehmen bekannt. Beispiel 2: Automobile – Beschleunigungswerte werden nicht als personenbezogen sondern alltägliche Daten angesehen. Aber Nutzer und Fahrer sind spätestens bei Auslesung in einer Werkstatt identifizierbar. Versuche im Zuge der E-Privacy-Richtlinie die IP-Adresse als personenbezogenes Datum auszuschließen sind durch den Einsatz der Datenschutzbeauftragten gescheitert. Sie haben damit eine drastische Einschränkung des Datenschutzes verhindert.

Datenverarbeitung in der Rechtsentwicklung:
Ein weiteres Problem besteht darin, dass Instrumente des Datenschutzes aus einem Bereich meistens nicht ohne Problem auf einen anderen übertragen werden können und anwendbar sind. So kann ein Löschungsanspruch mitunter schwer durchsetzbar sein. Auch die Identifizierung einer verantwortlichen Stelle ist zunehmend schwieriger.
Als Folge des Volkszählungs-Urteils wurde das Grundrecht auf informationelle Selbstbestimmung geschaffen: Der Einzelne muss wissen, was mit seinen Daten geschieht und muss über sie bestimmen können. Heutzutage gestaltet es sich aber schwieriger denn je die Geltung des Grundrechts durchzusetzen. Als Abwehrrecht ist der Datenschutz eine machtbegrenzende Materie, der einem Einzelnen gewährleisten soll, dass auch öffentliche Stellen nicht unbefugt in die Daten eingreifen und auf sie zugreifen dürfen. Heutzutage werden allerdings mehr als 90% aller Daten nicht von öffentlichen Stellen gespeichert. Daher MUSS die Perspektive des Datenschutzes heute auch eine andere sein. Ein Datenschutz, der sich primär auf öffentliche Stellen richtet, ist also veraltet.
Ungeachtet dessen hat der Staat trotz Datenschutzes noch immer Möglichkeiten auf Daten Privater zuzugreifen: Beispielsweise bei der Vernehmung eines Zeugen, Beschlagnahme, Auskunftspflichten oder auch die Online-Durchsuchung.

Das Verhältnis Staat-Bürger darf deshalb zwar nicht aus dem Blick geraten; Hauptadressat aber sollte nicht mehr nur der Staat sein, sondern vielmehr die Unternehmen. Dies ist ein grundlegender Unterschied zu den Vereinigten Staaten wo man in den 1970ern absichtlich auf den Schutz gegen nicht-staatliche Stellen verzichtet hat. Eine erhoffte und prognostizierte Regelung durch den Markt ist dabei allerdings nicht eingetreten. Vielmehr profitieren Unternehmen von den schlechten Datenschutzbestimmungen. (vgl. VZ-Betreiber und facebook) Die Botschaft lautet: Schlechter Datenschutz zahlt sich aus?! Die Regulierung durch den Markt funktioniert als Gegenmodell allenfalls dort, wo es um besonders sensible Daten geht und Unternehmen Fehler machen oder bewusst gegen Datenschutzvorschriften verstoßen. So etwas wirkt sich gegen die jeweiligen Unternehmen aus.
Folglich braucht es Regelungsmechanismen - auch in Europa - die einen Anreiz für guten Datenschutz setzen und die heutigen Umsetzungsdefizite beseitigen. Es bedarf starker Datenschutzaufsichtsbehörden und gleichzeitig Instrumente, die Datenschutz attraktiv machen, so z.B. ein Datenschutz-Audit (nur gibt es leider bislang noch kein Datenschutz-Audit-Gesetz sondern nur eine Diskussion über die Stiftung Datenschutz). Das Datenschutz-Audit wäre ein Instrument, dass sich im Wettbewerb einsetzen ließe.

Es gibt eine Vielzahl von Herausforderungen für den Datenschutz:
* Intransparenz von Datenverarbeitungsvorgängen: Wie kann man Transparenz wieder herstellen? Zwar gibt es klassische Informationspflichten, aber es ist nicht hinnehmbar beispielsweise erst lange Gebrauchsanweisungen zu studieren, um an die elementaren Informationen zu gelangen. Ein aktueller Vorschlag besteht darin Datenbriefe einmal im Jahr an alle Betroffenen zu versenden. Dieser Vorstoß scheint aber wegen der zu erwartenden Datenflut eher inpraktikabel. Besser wäre es, wenn dadurch Transparenz geschaffen wird, dass es ein elektronisches Auskunftsrecht gibt, dass sich auf die Quellen und Empfänger bezieht. Es sollte also ein Überblick möglich sein, an wen Daten aus Melderegister fließen.

* Wie kann man Datenschutz aber durchsetzen, so dass Daten schnell gelöscht werden, anonymisiert werden und geschützt bleiben (privacy by design)?

*Was geschieht mit den Daten, wenn sie einmal erhoben wurden? Zweckbindung vs. Data-Mining. Die Erhebung einzelner Daten ist an sich nicht so schlimm, aber das Zusammenspiel, das die Erstellung von Interessen-, Bewegungs- und Persönlichkeitsprofile erlaubt, ist das kritische. Daher braucht es Grenzen, die eine Erhebung und Verarbeitung hinter dem Rücken des Betroffenen und ohne dessen Einwilligung verbietet.

*Recht auf „Vergessen-werden“ im Internet in Form eines „digitalen Radiergummis“. Leider existieren dafür heute noch keine wirklich geeigneten Instrumente. Man kann allerdings Daten eine Art Verfallsdatum anhängen welches dann mit den Daten mitgegeben wird. Das würde zwar den Verfall nicht endgültig sichern, aber man könnte z.b. ein Verwendungsverbot daran knüpfen.

Datenschutzrecht heute:
Als nur ein Beispiel lässt sich die Zutrittskontrolle bei Datenverarbeitungsanlagen als ein schwer realisierbares Ziel nennen, welches bei Smartphones fast unmöglich ist.

Fazit:
Schutzziele müssen neu bestimmt werden und zwar so, dass sie Bestand haben. Auch die Kontrolle des Betroffenen über seine Daten könnte als technologisches Schutzziel definiert werden. Bei der Datenverarbeitung ist ein Identitätsmanagement möglich, das eine Verknüpfung von Daten erschwert (Vergleich: Österreich).

Umgang von uns allen mit persönlichen Daten:
Diejenigen, die persönliche Daten in Sozialen Netzwerken veröffentlichen machen dies selbst und freiwillig. Auch ist es nur ein Teil der Bevölkerung, der sich so verhält. Es will nicht jeder Nutzer jedem anderen auf der Welt Zugriff auf seine Daten gewähren, sondern vielleicht nur seinen Freunden.
Deshalb bedarf es auch hier eines gesetzlichen Rahmens an der Schnittstelle zwischen Privatsphäre und Öffentlichkeit. Ein Problem besteht in der Verknüpfbarkeit der Daten, z.B. bei Geo-Diensten, Geo-Tracking, Social Networks. Wichtig ist, dass wer sich selbst in Sozialen Netzwerken darstellt, nicht den Anspruch auf die Verwertung seiner Daten verliert.
Zudem geht es um eine Gestaltungsfrage: Wie können die Entwicklungen beeinflusst werden? Aktuelles Beispiel: Eric Schmidt, CEO von Google, hat einen Namensänderungsanspruch von Jugendlichen mit Eintritt ins Erwachsenenalter als möglich prophezeit. Problematisch stellt sich dabei aber unter anderem die Sicherstellung der Nicht-Verknüpfung der Daten des alten und des neues Ichs dar.
Zudem stellt sich überhaupt die Frage: Wer steuert hier was? - Die Gesellschaft muss die Kontrolle behalten. Es liegt an den Juristen belastbare Konzepte und Rahmen zu schaffen, die robust genug sind, durchgesetzt zu werden. Dieser Rahmen muss – auch europäisch und weltweit – weiterentwickelt werden.

Dank durch Herrn Goltz und Eröffnung der Fragerunde.

Frage: Wie ist der Datenschutz beim Datenschützer selbst ausgestaltet?
Antwort: Behördlicher Datenschutzbeauftragter ist ein Mitarbeiter, aber unabhängig. Es ist zugegebenermaßen ein nur schwach geregelter Bereich.

Frage: Wieso wurde in Deutschland nicht verhindert, dass Google Häuser abfotografiert? Und wie steht es um das digitale Radiergummi, dass laut Ankündigung des Innenministers bereits im Oktober einsetzbar sein könnte?
Antwort: Die Beurteilung von Google Street View ist primär eine Frage des Wegerechts und nicht des Datenschutzes. Das Datenschutzrecht sieht hier keine Möglichkeit vor, die Datenerhebung direkt zu verhindern; höchstens eine anschließende Ahndung durch Verhängung von Bußgeldern. Die Anfertigung von Bildern im öffentlichen Raum kann nicht verhindert werden.
Beim Widerspruchsrecht kommt es auf § 28 BDSG an. Google hat aber von sich aus schon ein Widerspruchsrecht eingeräumt. Erschreckend ist allerdings, die Art und Weise der Ausgestaltung. Es sollte besser ein generelles Widerspruchsrecht geben, das in ein Widerspruchsregister bei einer vertrauenswürdigen Stelle eingetragen werden könnte. Geodaten-verarbeitende Stellen sollten dann nur Informationen über einen Widerspruch aber nicht die dazugehörigen personenbezogen Daten erhalten. Dieser Vorschlag wird am 20. September bei einem Spitzentreffen besprochen.
Zum digitalen Radiergummi liegt bislang kein Gesetzesentwurf vor.

Frage: Ist Ihnen das „Saarbrücker Radiergummi“ bekannt, dass die Informatik kürzlich der Öffentlichkeit vorgestellt hat?
Antwort: Nein, nicht bekannt. Ansätze auf dem Gebiet sind allerdings bekannt. So scheint das Verteilen von Daten Erfolg versprechend. Im Grunde handelt es sich um das gleiche Problem wie im Urheberrecht. Wenn man etwas wahrnehmbar machen will, muss es irgendwie präsentiert werden. Dann kann man aber nicht verhindern, dass es aufgenommen und kopiert wird. Einen absoluten Schutz wird es wohl kaum geben.

Frage: Personaler die in sozialen Netzwerken nach Informationen suchen sind nicht die eigentliche Zielgruppe. Die Daten werden nicht für die Personaler, sondern für Freunde eingestellt. Wie soll und kann eine zweckwidrige Verwendung unterbunden werden? Nur symbolisch? Oder sollten

drastische Sanktionen eingeführt werden, die eine abschreckende Wirkung entfalten?
Antwort: Der von der Bundesregierung beschlossene Entwurf zum Arbeitnehmerdatenschutz sieht diesbezüglich Regelung vor. So sollen solche Daten, wie eben jene aus sozialen Netzwerken, nicht ohne Einwilligung des Betroffenen in Bewerbungsverfahren genutzt werden dürfen. Ausnahme bilden dabei natürlich die Netzwerke, die allein diesem Zweck dienen – der sogenannte XING-Paragraph. Die vorgesehenen Bußgelder scheinen wirklich zu niedrig zu sein. Eine Durchsetzung wird daher wohl wirklich schwierig. Aber es ist auch eine begrüßenswerte Entwicklung zu beobachten. Es hat ein Lernprozess in der Gesellschaft eingesetzt. Personaler sehen ein, dass wir nicht alle Engel sind; sie sind somit also auch toleranter werden. Die gesamte Gesellschaft muss toleranter werden und damit leben, dass immer mehr Informationen über den Einzelnen preisgegeben werden.
Gegenfrage: Wäre nicht eine Meldepflicht für einen betrieblichen Datenschutzbeauftragten erforderlich?
Antwort: Das würde seine Stellung innerhalb des Betriebes nicht wirklich besser machen.

Frage: Daten gelten immer mehr als „Währung“ im Internet. Das Schlagwort lautet „Dienste gegen Daten“, Steuersünder-CDs etc.
Antwort: Prognosen hierzu sind schwierig. Eine Vision ist aber wohl vorhanden. Es ist eine Frage globaler Standards und Vereinbarungen. Ein Datenschutz-Konvention auf internationaler Ebene wäre denkbar. Zum Thema technologischer Datenschutz: Der Einzelne soll technische Mittel in die Hand bekommen, um den Bereich abzudecken, den Datenschutzbehörden keineswegs abdecken könnten.
So müsste es zum Beispiel selbst-exekutierende Instrumente geben. Man müsste auch zivilrechtliche Ansätze, wie Mechanismen der Wirtschaftsprüfung verfolgen. Der Umgang der Einzelnen mit ihren Daten ist aber positiv zu bewerten. Die Jugend lernt hier sehr schnell. Sie sollen es auch wagen, ihre Rechte einzufordern. Die scheint ein geeignetes Konzept, da es kaum möglich sein wird diese „Goldgrube“ zuzuschütten.

Frage: Stichwort: Recht am eigenen Bild. Wieso gilt das bei Google Street View nicht? Warum gibt es die Unterstellung, dass eine Einwilligung vorhanden ist?
Antwort: Nein, zivilrechtlicher Schutz wird gewährleistet, wenn Personen abgebildet sind! Die Personen werden auch verpixelt. Auf Häuser bezieht sich das Recht am eigenen Bild bislang aber nicht!
Gegenfrage: Es müsste aber doch jeder angeschrieben werden!
Es handelt sich aber um in der Öffentlichkeit angefertigte Bilder. Zudem handelt es sich hierbei eher um eine politische Frage. Es muss wirksame Datenschutzmechanismen geben. Street View an sich ist aber beispielsweise weniger problematisch als die Speicherung der Suchanfragen über Google. Diese Datenerhebung ist zudem auch nicht sichtbar. Auch das Google Dashboard gibt da keine all umfängliche Auskunft.

Frage: Google Street View wird wohl überbewertet. Wie kann Google das steuern? Google ist ja immerhin größter Hersteller von Gesichtserkennungssoftware. Wie wäre es zudem mit der Regelung eines immateriellen Schadensersatzanspruchs?
Antwort: Zum Gesichtsbild: Das Problem ist, dass keine gezielte Erhebung der Gesichter erfolgt, sondern dies eher nebenbei stattfindet. Hauptsächlich geht es um Fassaden. Die beiläufige Sammlung dieser Daten verhindert eine Anwendung des BDSG.
Zum immateriellen Schadensersatz: Datenschutzrechtlich gibt bei öffentlichen Stellen bereits einen Anspruch, nicht aber gegenüber nicht-öffentlichen Stellen. Es stellt sich die Frage, ob man über das BGB gehen kann, weil ja bereits im BDSG eine Regelung existiert. Zu befürworten wäre aber wohl ein pauschalierter und gesetzlich zu normierender Schadensersatz. Problematisch ist hierbei aber, dass auf den Weg des zivilrechtlichen Rechtsschutzes verwiesen wird, was nicht gerade der Königsweg ist.

Ergänzung aus dem Publikum: Die entsprechende EU-Richtlinie kennt bereits den immateriellen Schadensersatz. Dieser wurde auch gerichtlich bei der Einstellung von Daten in Terrordatenbanken bestätigt. Problem ist also die Auslegung des § 7 BDSG – entweder EU-konform oder nicht-konform auslegen?

Frage: Die Innovation ist dank der Verknüpfung von Daten in der Vergangenheit vorangeprescht. Soll der Datenschutz jetzt als Innovationsbremse fungieren? Somit wäre z.B. auch dem amerikanischer Markt nie eine solche Entwicklung von Google möglich gewesen.
Antwort: Kann nicht zustimmen, dass Datenschutz eine Innovationsbremse ist. Zudem kein gangbarer Weg, wenn nur über Nichtachtung der Persönlichkeitsrechte Innovation zu erreichen wäre. Vielmehr muss gemeinsam mit den USA nach einem Rahmen gesucht werden, der dieses regelt.

Dank seitens C. Goltz an P. Schaar für den interessanten Vortrag. Bemerkung, dass es sich um ein Feld mit Zukunft handelt, das auch weiterhin eine Vielzahl von Diskussionen hervorrufen wird.