Datenschutz – das unbekannte Wesen

von *Wolfgang Däubler, Professor an der Universität Bremen*

„Daten“ sind Angaben über bestimmte Menschen. Name und Vorname, Adresse, Beruf, aber auch Vorlieben für bestimmte Bücher, Käufe bei E-Bay oder das Buchen einer Ferienreise – das alles sind Daten, die sich auf eine einzelne Person beziehen. Daneben gibt es „Sachdaten“ wie das Geräusch eines Motors oder die Höhe eines Gebäudes, die als solche nicht auf eine Person bezogen sind.

Das Prinzip und seine Ausnahmen

Wenn man von „Datenschutz“ spricht, meint man nur die erste Gruppe von Informationen. Solche Daten sind keine Sachen, die allen gehören. Wissen über andere zu sammeln, es zu speichern und bei Gelegenheit auszuwerten, ist grundsätzlich verboten. Wenn Juristen „grundsätzlich“ sagen, gibt es allerdings immer Ausnahmen. Diese sind hier von beträchtlicher Bedeutung.

Der Datenschutz gilt nicht im rein persönlichen und familiären Bereich. Man muss deshalb kein schlechtes Gewissen haben, wenn man eine Liste mit Geburtstagsgästen auf dem Computer speichert. Auch das Adressbuch im privaten PC ist unbedenklich.

Die zweite Ausnahme ist noch sehr viel wichtiger. Das Datenschutzrecht ermächtigt ausdrücklich zu bestimmten Datenverarbeitungen. Man spricht deshalb von einem „Verbot mit Erlaubnisvorbehalt“. Wie weit gehen diese Erlaubnisse? Offen gesagt: Ziemlich weit. Erlaubt ist alles, was für den Abschluss und die Erfüllung von Verträgen notwendig ist. Natürlich steht das Datenschutzrecht nicht im Wege, wenn persönliche Daten in einen Wohnungsmietvertrag aufgenommen werden. Wird ein Leiharbeitnehmer zu einem Einsatz bei der Firma X geschickt, so können natürlich vorher einige Daten über ihn an X übermittelt werden: Diese muss ja wissen, wer da in der Frühe am Werkstor Einlass begehrt.

Unbedenklich ist weiter jede Datenverarbeitung, in die der Betroffene vorher eingewilligt hat. Das ist man bei Angeboten im Internet gewohnt: Man erklärt sein Einverständnis damit, dass

man in Zukunft Angebote der Firma X über antiquarische Bücher oder Angebote der Firma Y über preiswerte Kredite ohne Schufa erhält. Besonders wichtig sind die Einwilligungen bei sozialen Netzwerken. Wer sich bei Facebook registrierte, musste lange Zeit einwilligen, dass seine Daten auch in die USA übermittelt wurden. Andernfalls konnte man nicht dabei sein und zur großen Facebook-Gemeinde gehören (was manche Menschen als Nachteil empfinden).

Neben Vertrag und Einwilligung gibt es weitere Gründe. Das Gesetz kann ausdrücklich oder sinngemäß vorschreiben, dass bestimmte Informationen zu übermitteln sind: Der Arbeitgeber kann die Lohnsteuer nicht an Finanzamt abführen, ohne den Arbeitnehmer konkret zu bezeichnen, und dasselbe gilt für die Abführung von Sozialbeiträgen an die AOK.

Außerdem gibt es noch eine ganz allgemeine Ermächtigung: Hat derjenige, der über die Daten verfügen kann („Verantwortlicher“ genannt), ein berechtigtes Interesse, sie z. B. Dritten zugänglich zu machen, so kann er dies tun, wenn nicht das Interesse der betroffenen Person überwiegt. Unterstellt, ein Unternehmen soll verkauft werden: Der am Erwerb Interessierte will wissen, wer die Führungskräfte sind und wer von den Ingenieuren bereits eine Erfindung gemacht hat. Dies dem potentiellen Käufer mitzuteilen, entspricht einem berechtigten Interesse des Arbeitgebers. Für die betroffenen Arbeitnehmer stellt es keine ernsthafte Beeinträchtigung ihrer Privatsphäre dar, wenn ihre Rolle als Führungskraft bzw. ihre Eigenschaft als Erfinder einem möglichen Käufer mitgeteilt wird.

Rechtsgrundlagen

Wo steht das alles geschrieben? Bisher konnte man auf das Bundesdatenschutzgesetz verweisen, das alle grundsätzlichen Aussagen zum Datenschutz enthielt und das durch Sondervorschriften etwa für die Sozialversicherung oder das Meldewesen ergänzt wurde. Allerdings lohnt es sich nicht mehr, dort intensiv hineinzuschauen, denn es hat den 25. Mai 2018 als Verfallsdatum. An diesem Tag tritt die Datenschutz-Grundverordnung der EU in Kraft, die grundsätzlich dem gesamten deutschen Recht vorgeht. Sie gilt in allen Mitgliedstaaten der EU und hat unmittelbare Wirkung auch zwischen einzelnen Bürgern wie Vermieter und Mieter, Arbeitgeber und Arbeitnehmer. Sie enthält eine umfassende Regelung des Datenschutzes, um so einheitliche Standards von Sizilien bis nach Helsinki und von Warschau bis Lissabon zu schaffen. Gleichzeitig findet man dort aber eine Reihe sog.

Öffnungsklauseln. Der Beschäftigtendatenschutz kann beispielsweise in beträchtlichem Umfang national geregelt werden. Auch können die Mitgliedstaaten die recht weit gehenden Rechte des Individuums auf Information, Auskunft, Berichtigung und Löschung beschränken. Davon hat der deutsche Gesetzgeber Gebrauch gemacht. Am 25. Mai 2018 tritt daher das neue Bundesdatenschutzgesetz (BDSG) in Kraft, das u. a. eine vergleichsweise eingehende Regelung des Beschäftigtendatenschutzes enthält.

Interpretationsfragen

Dieses rechtliche „Gerüst" wirft natürlich eine Reihe von Rechtsfragen auf. Ist es z. B. notwendig, dem Einsatzbetrieb auch das Geburtsdatum des Leiharbeiters mitzuteilen? Darf der Vermieter bei den Vertragsverhandlungen danach fragen, ob sich das junge Paar Kinder anschaffen will? Was sind die Voraussetzungen einer Einwilligung? Reicht es, wenn sie automatisch als erklärt gilt, sofern man nicht ein bestimmtes Kästchen („Keine Werbung") ankreuzt? Kann der potentielle Unternehmenskäufer Angaben über alle Belegschaftsmitglieder einschließlich Fehlzeiten in den letzten fünf Jahren verlangen? Dies ist nur ein ganz kleiner Ausschnitt aus den vielen Auslegungsfragen, die sich hier stellen.

Um zu sehen, was andere Juristen von einem Problem denken, schauen Richter und Rechtsanwälte in Kommentaren nach. Die Datenschutz-Grundverordnung (abgekürzt: DSGVO) ist innerhalb kurzer Zeit Gegenstand von acht Kommentaren mit bis zu 1000 Seiten geworden; ein neunter, besonders umfangreicher, ist fast fertig. In die Einzelfragen des Datenschutzrechts einzusteigen, ist an dieser Stelle nicht möglich. Deshalb nur zwei Punkte: Wer sind die Instanzen, die für die Umsetzung und praktische Beachtung des Datenschutzrechts sorgen sollen? Zum zweiten wäre es vielleicht interessant zu wissen, in welchen Punkten die DSGVO vom bisherigen deutschen Recht abweicht.

Durchsetzungsinstanzen

Wir sind es gewohnt, die Durchsetzung des geltenden Rechts ausschließlich als Aufgabe der staatlichen Gerichte zu sehen. Im Strafrecht trifft dies auch in vollem Umfang zu, denn private Strafgerichte gab es nur im Feudalismus, wo die Gutsherrn mit ihrer Hilfe schalten und walten konnten wie sie wollten. Heute gibt es ein staatliches Strafmonopol. Auch im Zivilrecht geht man meist zu Gericht; wenn der Schuldner nicht bezahlt oder der Verkäufer

den Mangel der Sache nicht einräumt, bleibt oft kein anderer Ausweg als die Gerichte zu bemühen. Dies gilt allerdings nicht für große Firmen und den internationalen Handelsverkehr: Dort werden im Streitfalle private Schiedsgerichte eingeschaltet, die schnell und meist auch kostengünstig den Konflikt erledigen.

Im Datenschutzrecht liegen die Dinge anders. Für den Einzelnen ist es oft nicht erkennbar, dass mit seinen Daten Schindluder getrieben wird. Zwar kann er Auskunft über alle Daten verlangen, die ein anderer über ihn gespeichert hat, aber dafür muss er wissen, wer „der andere" ist, und er muss die Zeit aufbringen, die ein schriftliches „Auskunftsersuchen" voraussetzt. Deshalb bringen solche Individualrechte relativ wenig – sie existieren in Deutschland seit 1977, also seit über 40 Jahren, und dennoch gibt es sehr wenige Gerichtsentscheidungen zu diesem Bereich. Der Gesetzgeber muss also dafür sorgen, dass sich andere Instanzen um die Einhaltung des Datenschutzrechts kümmern; man kann dies nicht in alt-liberaler Weise nach dem Motto „Die werden sich schon wehren" allein den Betroffenen überlassen.

In jedem Unternehmen, wo regelmäßig mindestens zehn Personen mit der Verarbeitung personenbezogener Daten befasst sind, muss ein sog. betrieblicher Datenschutzbeauftragter bestellt werden. Er wacht als unabhängige Instanz darüber, dass dem Gesetz entsprechend mit den Daten von Arbeitnehmern, Lieferanten und Kunden umgegangen wird. Handelt es sich – wie häufig – um einen im Unternehmen tätigen Arbeitnehmer, so muss ihm die nötige Zeit für diese Kontroll-Tätigkeit eingeräumt werden. Außerdem hat er Anspruch auf die erforderlichen Ressourcen, was von einem Büro für vertrauliche Gespräche bis zum Besuch von Weiterbeildungsveranstaltungen reicht. Auch besitzt er einen ähnlich weit reichenden Kündigungsschutz wie ein Betriebsratsmitglied. Nur: Anders als dieses ist er nicht von der Belegschaft gewählt, sondern wird vom Arbeitgeber benannt. Der Betriebsrat kann zwar manchmal mitreden, aber letztlich kaum etwas verhindern. Der Arbeitgeber wird also oft Personen aussuchen, die ihm aller Erfahrung nach nicht „weh tun" werden. Wichtiger ist deshalb in der Praxis oft der Betriebsrat, der effektiv unabhängig ist und sich auch um die Einhaltung des Arbeitnehmerdatenschutzes kümmern muss.

Erhebliche Bedeutung hat die Aufsichtsbehörde. Sie existiert in jedem Bundesland und wird vom Parlament eingesetzt; sie ist von den Ministerien und der Regierung unabhängig. Jeder, der einen Verdacht hat, dass mit Daten Missbrauch getrieben wird, kann sich an sie wenden;

dies ist auch anonym möglich. Sie ist jedoch nicht auf solche Initiativen angewiesen, sondern kann – ähnlich wie die Gewerbeaufsicht – ohne vorherigen Ankündigung in bestimmten Betrieben auftauchen und sich zeigen lassen, wie man dort mit Daten verfährt. Bestimmte Praktiken kann sie untersagen und im Einzelfall auch Bußgelder verhängen.

Datenschutzbeauftragter, Betriebsrat und Aufsichtsbehörde sind eher als der Einzelne in der Lage, im Detail nachzuvollziehen, was mit den Daten der betroffenen Personen passiert. Oft sorgt schon ihre Existenz dafür, dass einigermaßen nach Gesetz und Recht verfahren wird. Auch wenn dies nicht der Fall ist: Nehmen sie ihre Aufgabe ernst, können sie vieles entdecken, was den betroffenen Personen immer verborgen geblieben wäre. Die jährlichen Berichte der Aufsichtsbehörden sind eine Fundgrube für jeden Datenschützer (und auch für Menschen, die sich für die tatsächliche Lage des Datenschutzes interessieren).

Was ist neu an der Datenschutz-Grundverordnung?

Von ihrer Form her ist die DSGVO nicht eben attraktiv: Die Häufung von Substantiven würde jeden Deutschlehrer zum Rotstift greifen lassen, die Sätze sind lang wie die vieler Professoren, und die Begriffe werden mal so, mal anders versstanden. Manche verwenden dafür den Ausdruck „Brüsseler Bürokratensprech“. Will man einen Abiturienten davon abhalten, jemals Jura zu studieren, sollte man ihm die DSGVO als „Einführungslektüre“ geben. Wenn er dann immer noch auf seinem Studienwunsch beharrt, handelt es sich um einen wirklichen Überzeugungstäter, dem man keine Steine mehr in den Weg legen sollte.

Inhaltlich ist die DSGVO besser als das bisher geltende Recht. Einige wichtige Punkte seien genannt.

- Wer (etwa im Rahmen eines Vertrages) Daten anderer Menschen verarbeitet, muss dokumentieren, für welchen konkreten Zweck er dies tut. Damit ist eine Festlegung auf diesen Zweck verbunden. Werden die Daten später in anderem Zusammenhang verwendet, ist dies grundsätzlich rechtswidrig. In einem Unternehmen wird beispielsweise eine Zugangskontrolle praktiziert; nur wer am Eingang einen Betriebsausweis in einen bestimmten Schlitz steckt, darf rein. Später fällt der X wegen arbeitgeberkritischer Äußerungen in Ungnade. Man wertet deshalb die „Zugangsdaten“ aus und stellt fest, dass er des Öfteren zu spät kam und will ihm deshalb eine Abmahnung verpassen. Das geht nicht: „Pünktlichkeitskontrolle“ ist ein anderer

Zweck als „Zugangskontrolle“ und den kann der Arbeitgeber nicht einfach nach Gutdünken neu einführen.
- Der Abschluss eines Vertrages (z. B. mit einem Telekommunikationsanbieter) darf nicht davon abhängig gemacht werden, dass der Einzelne damit einverstanden ist, seine Daten auch für andere Zwecke als die Durchführung des Vertrages zur Verfügung zu stellen. Eine solche „Koppelung“ ist ausdrücklich verboten. Die Einwilligung, Werbesendungen zu erhalten, ist deshalb unwirksam, wenn sie zur Voraussetzung für den Abschluss eines Handy-Vertrages gemacht wurde.
- Die Datenerhebung muss mit Treu und Glauben vereinbar sein. Damit ist eine heimliche Beobachtung über eine verdeckte Videoanlage oder einen Privatdetektiv ausgeschlossen, es sei denn, dies wäre das einzige Mittel, um den Verdacht einer Straftat zu klären – wobei der Verdacht nicht auf Mutmaßungen, sondern auf konkreten Tatsachen beruhen muss.
- Verstößt der Verantwortliche gegen eine Vorschrift der DSGVO oder des neuen BDSG, so ist er zum Schadensersatz verpflichtet. Dabei ist anders als bisher auch der immaterielle Schaden zu ersetzen, also eine Art Schmerzensgeld zu bezahlen. Dieses muss so hoch sein, dass es „abschreckend“ wirkt. Illegale Videoaufnahmen werden in Zukunft vielleicht 50.000 Euro kosten.
- Werden wesentliche, im Einzelnen aufgezählte Bestimmungen der DSGVO verletzt, so kann die Aufsichtsbehörde nicht nur ein entsprechendes Verhalten in der Zukunft verbieten. Vielmehr darf sie ein Bußgeld verhängen, das amerikanische Ausmaße hat: Bei bestimmten Verstößen kann es bis zu 10 Mio. Euro, bei anderen bis zu 20 Mio. Euro betragen. Bei Unternehmen gibt es als Obergrenze 2 % bzw. 4 % des weltweiten Jahresumsatzes (nicht etwa des Gewinns!), sofern dadurch die 10 bzw. 20 Mio. überschritten sind. Auch wenn die Aufsichtsbehörden mit Sicherheit nicht bis an diese Obergrenzen gehen – schon die Möglichkeit dazu verbreitet in manchen Direktionsetagen Furcht und Schrecken.

Herausforderungen in der Zukunft

Je weiter die Digitalisierung voranschreitet, umso mehr Daten fallen über den Einzelnen an. Wo alles nur noch IT-gesteuert funktioniert, wird insbesondere am Arbeitsplatz jedes Schrittchen des Einzelnen erfasst. Hier wird die Kontrolle der Datenverarbeitung noch viel notwendiger als heute – was voraussetzt, dass z. B. die Aufsichtsbehörden mit genügend „manpower“ bzw. „womanpower“ ausgestattet sind. Die hohen Sanktionen könnten dazu

führen, dass dieser Zustand wirklich eintritt – jeder zusätzliche Aufsichtsbeamte bringt dem Fiskus sehr viel mehr ein als die Gehaltskosten ausmachen.

Datenverarbeitung wird immer internationaler. In den USA gilt aber kein oder jedenfalls kein vergleichbares Datenschutzrecht wie in Europa. Außerdem haben die Sicherheitsbehörden Zugriff auf alle Dateien, zu denen irgendein US-Bürger von den USA aus Zugriff hat. Dies dient der Terrorabwehr, doch gibt es kein objektives Verfahren, um im Einzelfall zu überprüfen, ob die abgefragten Informationen wirklich „terrorrelevant" sind oder ob sie nur dazu dienen, die Aktivitäten europäischer Konkurrenten auszukundschaften. Der Europäische Gerichtshof in Luxemburg hat deshalb die Übermittlung der Facebook-Daten in die USA für illegal erklärt. Dies ist als solches natürlich richtig (und war angesichts der sonstigen „Linie" des Gerichtshofs nicht unbedingt zu erwarten). Dennoch bleibt das Problem, dass es auch Zugriffe von US-Geheimdiensten in Europa geben kann. Wenn schon das Handy der Kanzlerin abgehört wird – warum sollten die Entwicklungsabteilungen von Siemens oder BASF besser geschützt sein? Hier muss das Recht vor der Macht kapitulieren.

Ungelöst ist auch ein anderes Problem. Sind Angaben über eine Person einmal im Internet, so kann man sie natürlich an ihrer Quelle wieder entfernen. Wie will man aber alle diejenigen zu einer Löschung veranlassen, die sich in der Zwischenzeit die Daten heruntergeladen haben? Das funktioniert ersichtlich nicht. Einzige Möglichkeit scheint mir ein „eingebautes Verfallsdatum" zu sein, gewissermaßen ein digitaler Radiergummi, der sich auch auf Kopien überträgt: Nach der vorgegebenen Zeit würden die Daten automatisch verschwinden. Bisher sind marktgängige technische Entwicklungen in dieser Richtung aber nicht erkennbar.

Letztes Problem: Big Data. Eine unübersehbare Zahl von Daten wird ausgewertet und zu „Erfahrungssätzen" verdichtet. Um es am Beispiel zu verdeutlichen: Eine US-Firma hat durch Big-Data-Analysen herausgefunden, dass Beschäftigte, die fünf Jahre lang nicht befördert wurden, als Person kein Entwicklungspotential mehr besitzen. Sie empfiehlt daher ihren Arbeitgeber-Kunden, sich von solchen Mitarbeitern zu trennen. In manchen Ländern ist dies einfach, in anderen muss man eine Abfindung bezahlen, deren Höhe Verhandlungssache ist. Die eigentliche Schwierigkeit liegt darin, dass durch Big Data künftiges Verhalten prognostiziert wird und daraus gravierende Konsequenzen abgeleitet werden. Niemand ist aber in der Lage zu beurteilen, nach welchen Kriterien die Daten ausgewählt waren und wie viel Aussagekraft sie deshalb hatten. Das viel beschworene Transparenzprinzip steht hier auf

dem Papier. Doch davon ganz abgesehen: Wollen wir, dass in Zukunft die Erkenntnisse unbekannter Systemherrn über unser Schicksal entscheiden? Nicht nur auf die Datenschützer werden große Aufgaben zukommen.