erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

Marie-Theres Tinnefeld

Die selbstbestimmte Einwilligung – Bedeutung, Möglichkeiten und Grenzen

Menschenrechtliche Betrachtung

Die Einwilligungserklärung Betroffener ist nach wie vor eine der wichtigsten Rechtsgrundlagen für die Verarbeitung personenbezogener Daten durch öffentliche Stellen und durch Private (z. B. Online-Händler). Die EU-Datenschutz-Grundverordnung konkretisiert die Anforderungen an eine rechtswirksame Einwilligung. Der Beitrag von Marie-Theres Tinnefeld analysiert diese Bestimmungen im Kontext der zunehmend europäisch geprägten Menschenrechte.

Der wichtigste Schritt auf dem mühseligen Weg hin zur freien Selbstbestimmung des Menschen beginnt in Europa nach den traumatischen Unrechtserfahrungen am Ende des Zweiten Weltkrieges. Ohne dieses Ende im Jahre 1945 zur Stunde Null stilisieren zu wollen, so stellt jene Erfahrungsgeschichte doch eine Zäsur dar. Hier beginnt die Konstitution Europas – nicht nur Deutschlands – als ein eindeutiges anderes Europa, als ein Europa durch Menschenrechte (Schmale/Tinnefeld 2017: 343).

Gemeint ist eine veränderte Betrachtung des Individuums. Das europäische Recht spricht seitdem jedem Menschen wegen seiner Menschlichkeit eine unantastbare Würde zu, allein weil er lebt und unabhängig von der Frage, wie er lebt, welcher Herkunft oder welchen Geschlechts er ist, ob er alt oder jung, ob er krank oder gesund ist. Auch ein unheilbar Kranker oder „schwieriger" Mensch darf nicht entrechtet werden, wie dies unter den Nationalsozialisten der Fall war. Beispielhaft sei hier nur auf die

Geschichte des 1944 ermordeten Ernst Lossa im Dritten Reich verwiesen.[1] Die Rekonstruktion dieser Geschichte legt die Zielsetzungen der Nationalsozialisten offen, zu denen unter Mitwirkung von Ärzten, Anthropologen und Genetikern eine Politik gehörte, die auf „Rassenreinheit" setzte und zu Euthanasie und staatlich gelenkten Massenmorden führte.

Mit der Anerkennung der Gleichheit aller Menschen vor dem Gesetz im deutschen Grundgesetz (Art. 3 Abs. 1 GG) ist die Aufforderung verbunden, keinen Menschen zu entwürdigen oder verächtlich zu machen (Diskriminierungsverbot, Art. 3 Abs. 3 GG, und Gleichberechtigungsgebot, Art. 3 Abs. 2 S. 1 GG). Eine Rechtsvorstellung, die sich von der Menschenwürde her versteht, gewinnt nur einen übereinstimmenden Sinngehalt in „Gleichheit in der Freiheit" (Fries 1803: 33). Es ist daher grundlegend immer zu fragen, ob personenbezogene Unterschiede rechtlich überhaupt beeinflusst werden können und dürfen. Das Gleichheitsgebot entspricht der verfassungsrechtlichen Garantie von Menschenwürde und individueller Freiheit, die das Bundesverfassungsgericht in der digitalen Informationsgesellschaft immer wieder hervorgehoben hat.

Das Gericht hat schon frühzeitig auf grundrechtliche Schutzlücken reagiert, die durch die automatisierte Verarbeitung personenbezogener Daten in den siebziger Jahren des zwanzigsten Jahrhunderts entstanden sind, und aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m Art. 1 Abs. 1 GG) ein Grundrecht auf informationelle Selbstbestimmung bzw. ein Grundrecht auf Datenschutz geschöpft (BVerfGE 65, 1). Das „neue" Grundrecht basiert auf dem uralten Schutz von Privatheit und Intimität. Das Bundesverfassungsgericht hat den Sinn von Privatheit unter dem Aspekt der räumlichen Privatheit – hier der Wohnung – eindrücklich als Innenraum beschrieben, wo man „sich selbst besitzt" (BVerfGE 27, 1, 6). Der Schutz schließt heute vielfältige Formen des Raumes ein (Tinnefeld 2018: 44, 48 f.).Zu den notwendigen Bedingungen gleicher Freiheit ist zu sagen, dass der Einzelne auf geschützte, abgeschirmte Sphären des privaten Lebens angewiesen ist, die Hannah Arendt „die Dunkelheit des Verborgenen und Geborgenen" nennt (Arendt 1967: 50). Ohne unbeobachtete Freiräume und ohne Zeiten für ein intimes und privates Leben abseits vom „blendend unerbittlichen Licht, das aus der Öffentlichkeit strahlt", gäbe es keine Möglichkeit, eine individuelle Identität zu entwickeln und soziale Kontakte mit der Außenwelt zu knüpfen.

Das Recht auf Privatheit bedarf angesichts der subtilen neuen Technologien, des multifunktionalen Einsatzes von „Big Data" und „Data Analytics", einer Gewährleistung durch höhere datenschutzrechtliche Barrieren. Das Bundesverfassungsgericht betonte in seinem bahnbrechenden Volkszählungsurteil bereits im Jahre 1983: „Im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt" (BVerfGE 65, 1, 41). Das heißt auch, dass die informationelle Selbstbestimmung nicht nur eine Grundbedingung für die „individuellen Entfaltungschancen des Einzelnen" ist, sondern auch für seine freien „Handlungs- und Mitwirkungsrechte in einem demokratischen Gemeinwesen" (BVerfGE 65, 1, 43).

Die Orientierung am Individuum als einem „autonomen Willens- und Handlungssubjekt" scheidet die Bereiche von Staatsmacht und Bürgerfreiheit (Denninger 1994: 9). Die eigene Person und ihre Privatheit kennzeichnen den Lebensbereich, in den der Staat nicht oder nur unter einer rechtfertigungsbedürftigen Ausnahme aufgrund eines Gesetzes oder/und der wirksamen Einwilligung einer betroffenen Person eingreifen darf. Das Vorrecht der betroffenen Person, grundsätzlich selbst über die Verwendung ihrer Daten im Wege der Einwilligung zu entscheiden, ist auch gegenüber Privaten von Bedeutung. Angesichts der Möglichkeiten der exzessiven globalen Verbreitung persönlicher Daten kann eine Einwilligung aber nur dann Wirkkraft entfalten, wenn sie an einen bestimmten Zweck gebunden wird. Nur dann kann die betroffene Person die Verarbeitungskonsequenzen überschauen. Dieses Rechtsverständnis entspricht dem supranationalen Unionsrecht.

Europäische Tonlage

Das Recht auf Privatheit (right to privacy) ist vor allem in der Europäischen Menschenrechtskonvention (Art. 8 EMRK) von 1950 verankert und umfasst heute auch das Recht auf Datenschutz. Dieses Recht findet seinen Vorläufer im Recht der Vereinten Nationen, das in der Allgemeinen Erklärung der Menschenrechte (Art. 12 AEMR) von 1948 festhält, dass das Private als „universelles Menschenrecht" zu schützen ist (Guradze 1956: 201 ff.). Das right to privacy wurde später im UN-Zivilpakt[2] von 1966 eigens verbrieft (Art. 17 IPbpR) und von allen Mitgliedern des Europarates unterzeichnet.

Das Recht auf Privatheit und Datenschutz hat Eingang in die EU-Grundrechtecharta gefunden. Die Charta ist zusammen mit dem Vertrag von Lissabon am 1. Dezember 2009 in Kraft getreten und besitzt den gleichen Rang wie diese, sie gehört also zum Primärrecht der Union. Die Charta hat das Menschenrecht auf Privatheit (Art. 7 GRCh) verankert und es explizit um ein Datenschutzgrundrecht (Art. 8 GRCh) ergänzt. Damit wird auf der Unionsebene das historische Menschenrechtsverständnis an den Lebensverhältnissen und -bedingungen im digitalen Zeitalter ausgerichtet: Art. 8 Abs. 2 S. 1 GRCh hält fest, dass personenbezogene Daten „nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlichen legitimen Grundlage verarbeitet werden [dürfen]." Das Grundrecht schreibt zudem ein Auskunfts- und Berichtigungsrecht der betroffenen Person über die sie betreffenden Daten fest (Art. 8 Abs. 2 S. 2 GRCh) und statuiert die Überwachung dieser Vorschriften durch eine unabhängige Stelle (Art. 8 Abs. 3 GRCh).

Die Auslegung des Menschen- und Grundrechts auf Privatheit und Datenschutz hat sich von nationalen Verfassungsgerichten auf die höchsten europäischen Gerichte verlagert: den Europäischen Gerichtshof für Menschenrechte (EGMR) in Straßburg und den Europäischen Gerichtshof (EuGH) in Luxemburg. Das Straßburger Gericht stärkt europarechtlich seit langem die Abwehr von unzulässigen oder unverhältnismäßigen staatlichen Informationszugriffen. In den letzten Jahren ist auch der EuGH zunehmend zu einer herausragenden Instanz in Fragen des Grundrechtsschutzes mit dem Schwerpunkt Datenschutz geworden, der gegenüber staatlichem und privatem Eingreifen Wirkkraft entfaltet.[3]

Voraussetzung einer freiwilligen Einwilligung ist eine umfassende Information (Jarass 2016: Art. 8 Rn. 9). Die betroffene Person ist über die jeweiligen Verwendungsabsichten und deren mögliche Konsequenzen zu informieren. Sie muss vor einer Zustimmung, etwa für die Datenverarbeitung bei einer Kreditvergabe durch die Bank, einer Behandlung durch den Arzt oder einer Videoüberwachung durch den Arbeitgeber so aufgeklärt werden, dass sie in der Lage ist, sich von der Bedeutung ihrer Erklärung ein Bild zu machen, um eine Einwilligung ggf. auch verweigern zu können.

Die Forderung nach Autonomie des Einzelnen macht es verständlich, dass im Datenschutzrecht die Einwilligung und ihre für die Datenverarbeitung konstitutive Funktion betont wird. Vor dem Hintergrund praktischer Erfahrungen mit der Einwilligung ist es allerdings fraglich, ob die vorausgesetzte autonome Entscheidung etwa im Bereich des Datenschutzes für Arbeitnehmer oder für Patienten nicht in erster Linie dazu dient, einseitige Regelungen im Interesse des Verantwortlichen für die Datenverarbeitung zu sanktionieren. Ist daher eine Reduktion der Legitimationswirkung der Einverständniserklärung in abhängigen Verhältnissen zugunsten von zwingenden gesetzlichen Vorgaben notwendig? Diese Frage stellt sich auch bei der Einwilligung von Kindern, Jugendlichen oder Schwerkranken. Sind sie einsichtsfähig? Es gibt nicht immer ein klares Ja oder Nein. Hier ist eine Rückbesinnung auf die primäre Funktion der Einwilligung im Datenschutzrecht notwendig. Eine letztlich die betroffene Person völlig übergehende Verarbeitung ihrer persönlichen Daten ist jedenfalls ohne eine Legitimationsgrundlage schrankenlos, so wie dies in der Zeit des Nazi-Regimes der Fall war.

Die Charta bindet die Legitimation der Datenverarbeitung an den „Grundsatz von Treu und Glauben mit Rücksicht auf die vereinbarte Zweckbindung". Anders ausgedrückt: Zweckentfremdungen sind nur zulässig, wenn sie gesetzlich vorgesehen sind oder mit Kenntnis der betroffenen Person und deren Einwilligung erfolgen. Mit der informationellen Selbstbestimmung wäre es unvereinbar, wenn der Zweckbindungsgrundsatz vom Verantwortlichen für die Datenverarbeitung ignoriert oder heruntergespielt würde.

Seit dem Volkszählungsurteil des BVerfG folgt aus der informationellen Selbstbestimmung, dass eine Verarbeitung personenbezogener Daten für die betroffene Person durch die Möglichkeiten von Kontrolle und Korrektur durchsichtig sein muss. Zu den flankierenden prozeduralen Schutzvorschriften gehört daher der Grundsatz der Transparenz sowie auch das Gebot unabhängiger Aufsichtsbehörden. Ziel ist es, die Autonomie des Einzelnen und somit seine Kommunikations- und Partizipationsfähigkeit zu sichern. Eben diese Fähigkeit ist auch erforderlich, um eine demokratische Gesellschaft zu erhalten.

Im Vertrag von Lissabon findet sich eine grundsätzlich umfassende Rechtsetzungskompetenz für das sekundäre Datenschutzrecht (Art. 16 AEUV). Der Unionsgesetzgeber hat auf dieser Grundlage die allgemeine Datenschutz-Grundverordnung (DSGVO) 2016 (VO (EU) 2016/679) verabschiedet. Sie gilt ab 25. Mai 2018 in allen EU-Mitgliedstaaten und löst die bis dahin geltende Datenschutz-Richtlinie (RL 95/46/EG) ab.

Unionsweite Verordnung

Im digitalen Zeitalter sind staatliche Aktivitäten für die betroffene Person ebenso gefährlich wie diejenigen von Privaten, etwa der Konzernriesen Google und Facebook. Die neuen Technologien werden im öffentlichen wie im nicht-öffentlichen Sektor mit dem stets gleichen Ziel angewendet, über die betroffene Person nicht nur alles zu erfahren, sondern auch alltägliche Prozesse durch Big Data und datenauswertende Algorithmen zu steuern. Die Verarbeitungsanlässe mögen im öffentlichen und privaten Bereich verschieden sein. Der Informationswert ist aber auch dann in beiden Bereichen von großem Interesse, wenn die Reaktionen verschieden ausfallen. Für beide gilt „Ordne so lange, bis du Dein Ziel erreicht hast" (Schirrmacher 2011: 191). Erst recht kommt es darauf an, dass die betroffene Person von jedem öffentlichen und nicht-öffentlichen Verantwortlichen für die Datenverarbeitung in verständlicher Form über ihre jeweils verarbeiteten Daten informiert wird und ggf. auch ein Beschwerderecht bei einer zuständigen Aufsichtsbehörde hat. Im Zeichen der digitalen vernetzten Datenverarbeitung ist allerdings eine getrennte Kompetenz der Aufsichtsbehörden nach den Kategorien öffentlicher bzw. nicht-öffentlicher Bereich unhaltbar.

Die DSGVO hat unmittelbare Geltung: Sie will in den Mitgliedstaaten ein gleichmäßig hohes Datenschutzniveau unionsweit gewährleisten und bezieht in ihrem Anwendungsbereich grundsätzlich öffentliche und nicht-öffentlich Verantwortliche ein. Grundvoraussetzungen einer wirksamen Einwilligung sind in der DSGVO in Übereinstimmung mit der Grundrechte-Charta geregelt.

Maßstäbe für die Einwilligung

Es stellt sich die Frage, ob ein selbstbestimmtes Entscheiden angesichts von Vorselektionen durch die digitale Auswertung enormer Datenmengen in der Praxis noch möglich ist. Der ehemalige Bundesverfassungsrichter und ausgewiesene Kenner riskanter Datenverarbeitung, Wolfgang Hoffmann-Riem, der federführend ein IT-Grundrecht[4] initiiert hat, beantwortet diese Frage positiv mit Blick auf die Reformen in der DSGVO (Hoffmann-Riem 2016: 646). Es gilt, die Maßstäbe der Einwilligung zu betrachten, die im Spiegel der Grundrechte-Charta und technischer Gefährdungslagen entstanden sind.

Unter der Verordnung kommt der Einwilligung als Erlaubnistatbestand für eine rechtmäßige Datenverarbeitung weiterhin eine zentrale Rolle zu.[5] Die Verordnung enthält eine Definition der freiwilligen Einwilligung (Art. 4 Nr. 11 DSGVO), die in Art. 7 Abs. 4 DSGVO sowie in den Erwägungsgründen (EG) ausdifferenziert wird. EG 43 macht die Freiheit in der Gleichheit zur Antriebsfeder bei der Beurteilung der Freiwilligkeit. Anders ausgedrückt: Es darf kein Ungleichgewicht zwischen der betroffenen Person und den Verantwortlichen in staatlichen oder privaten Lebensbereichen geben. Damit sich Machtungleichheiten etwa zwischen Arbeitgeber und Arbeitnehmer durch eine „fiktive" Einwilligung nicht verfestigen, kann diese durch eine geschärfte, ggf. auch nationale gesetzliche Regelung in angemessene Bahnen gelenkt werden. Bei einer informationellen Unterlegenheit kann keine freiwillige Entscheidung der betroffenen Person angenommen werden (Spindler 2012: F 99 f.). Sie steht auch nicht im Einklang mit dem Grundsatz von Treu und Glauben (Art. 5 Abs. 1 lit. a DSGVO).

Welche Person kann eine wirksame Einwilligung abgeben?

Voraussetzung ist, dass eine betroffene Person einwilligungsfähig ist. In diesem Kontext muss auch die Handlungskompetenz und Selbstverantwortlichkeit von solchen Personengruppen, die im Dritten Reich rechtlos gestellt waren (Erbkranke, Juden, „Asoziale" u. a.), nach dem Gleichheitsgrundsatz gesehen werden. Es gilt auch einen verantwortungsvollen Umgang mit den Möglichkeiten und Konsequenzen etwa genetischer Diagnostik zu suchen. In seinem 1970 erschienenen Buch „The Patient as Person" fordert Paul Ramsey eine nicht-paternalistische, nicht-direktive Arzt-Patient-Beziehung ein, in der die Entscheidungsfreiheit des Patienten geachtet wird.

Die Verordnung behandelt vor allem die Einwilligungsfähigkeit von Kindern (EG 65). Kinder bedürfen eines besonderen Schutzes, weil sie sich der langfristigen und weitreichenden Folgen ihres Handelns hinsichtlich der Verarbeitung ihrer Daten in der Regel (noch) weniger bewusst sind als Erwachsene (EG 38, 58, 65). Diese Einschätzung findet sich in mehreren Artikeln (Art. 6, 8, 12, 14 und 57) der DSGVO wieder. Die der Einwilligung vorausgehenden Hinweise sollen in einer verständlichen Sprache erfolgen (EG 58), die allerdings häufig in Online-Klauselwerken fehlt, die vielfach schon volljährige Personen nicht verstehen.

Die im deutschen Recht zu findende Unterscheidung von Kindern und Jugendlichen trifft die Verordnung zwar nicht. Sie sieht aber in Bezug auf „Dienste der Informationsgesellschaft" eine Regelgrenze von 16 Jahren vor. Bei Präventions- und Beratungsdiensten, die unmittelbar einem Kind angeboten werden, ist davon auszugehen (EG 38), dass eine Einwilligung des Trägers der elterlichen Verantwortung entbehrlich sein kann bzw. sein muss (Ernst 2017: 111). Die Verordnung legt allerdings eine absolute Untergrenze von 13 Jahren fest, die der Gesetzgeber in den Mitgliedstaaten auf keinen Fall unterschreiten darf.

Wann ist eine selbstbestimmte Einwilligung „freely given" und konkret?

In der Verordnung lautet durchgängig die Vorgabe: Es darf keinen Zwang bei der Abgabe einer Einwilligung geben, jede/r muss so handeln können, wie es ihr/ihm bis zur Todesstunde richtig erscheint (Borasio 2014:116 ff., Will 2018: 18).

Die Freiwilligkeit lässt sich an vielen Kriterien festmachen. Sie knüpft u. a. auch an das aus dem deutschen Recht bekannte Koppelungsverbot an. Danach darf die Erfüllung eines Vertrages nicht von der Verarbeitung personenbezogener Daten abhängig gemacht werden, „die für die Erfüllung eines Vertrages nicht erforderlich sind" (Art. 7 Abs. 4 DSGVO und EG 43). Beispielsweise kann die Koppelung einer Leistung, etwa die des Zugangs zu einem Telemediendienst, nicht mit einer Einwilligung in eine Datennutzung, die dafür nicht zwingend erforderlich ist, verbunden werden. Dies dürfte für die Mehrzahl der Online-Dienstleistungen gelten, die ihre Geschäftsmodelle auf dem Prinzip „Dienstleistungen gegen Daten" aufbauen.

Die Verordnung hält fest, dass die betroffene Person ihre Einwilligung nur „für einen oder mehrere bestimmte Zwecke" geben darf (Art. 6 Abs. 1 lit. a EG 32). Die autonome Zwecksetzung darf keinen pauschalen Charakter haben, darf nicht zur Bedeutungslosigkeit herabsinken. Auch mit Hilfe der Technik darf der Zweck eines Verwendungszusammenhangs nicht determiniert werden, etwa im präventiv-medizinischen Bereich. Je tiefer der Eingriff in das informationelle Selbstbestimmungsrecht ist, desto exakter muss der Zweck der Datennutzung oder -weitergabe angegeben werden, in die eingewilligt werden soll. Demnach ist auch eine Zweckänderung zu nicht kompatiblen Zwecken bei einer Weiterverarbeitung nur unter ganz bestimmten Voraussetzungen möglich (Art. 6 Abs. 4 DSGVO).

Was sind die Voraussetzungen für eine informierte und transparente Einwilligung?

Die betroffene Person muss ihre Einwilligung in „informierter Weise" (Art. 4 Nr. 11 DSGVO) abgeben. Ein „informed consent" liegt nur dann vor, wenn sie zumindest weiß, „wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen" (EG 42 S. 4).

Im Nachlass von Franz Kafka findet sich eine kurze Erzählung mit dem Titel „Zur Frage der Gesetze" (Kafka 2004), in dem der Autor davon spricht, wie quälend es sei, von Gesetzen beherrscht zu werden, die man nicht kennt. Deshalb sollte ein Gesetz jedem zugänglich sein und einfach, klar und verständlich formuliert und publiziert werden. Ähnliches gilt für eine selbstbestimmte Einwilligungserklärung, die Legitimationswirkung erzeugen kann. Die betroffene Person muss daher nicht nur wissen, wer nach der von ihr zu gebenden Einwilligung welche seiner Daten zu welchem Zweck verwenden darf, sondern auch, dass sie ihre Einwilligung für die Zukunft jederzeit widerrufen kann (Art. 7 Abs. 3 S. 1 DSGVO). Die Forderung betrifft insbesondere auch vorformulierte Einwilligungen in Allgemeinen Geschäftsbedingungen (AGB), die nicht nur hervorgehoben, sondern von anderen Sachverhalten klar unterschieden werden müssen (Art. 7 Abs. 2 S. 1 DSGVO). Von einer informierten Einwilligung kann nur gesprochen werden, wenn die Hinweise, die die erforderlichen Fragen erklären sollen, in einer verständlichen Sprache verfasst sind. Anders gesagt: Normen, die juristische Regeln für die Einwilligung und damit für das Zusammenleben der Menschen enthalten, sollten nicht in einer unverständlichen Rechtssprache vorgelegt werden. Wenn ein internationaler Konzern von deutschen Verbrauchern eine wirksame Einwilligung in die Nutzung ihrer Daten erwartet, dann sollte er die Datenschutzhinweise in deren Muttersprache formulieren. Er ist zudem verpflichtet, eine Widerrufsbelehrung anzufügen. Sie ist notwendig, um eine „faire und transparente" Verarbeitung zu gewährleisten (vgl. Art. 13 Abs. 2 lit. c).

In welcher Form ist die Abgabe einer Einwilligung zulässig?

Eine unmissverständliche Einwilligungserklärung (Art. 4 Nr. 11 DSGVO) ist grundsätzlich in jeder Form möglich, auch als elektronisch in Textform abgegebene Erklärung (EG 32). Ebenso ist die mündliche Einwilligung möglich, wegen der Beweislastverteilung aber weniger praktikabel (Art. 7 Abs. 1 DSGVO). Eine Einwilligung kann auch dann vorliegen, wenn die betroffene

Person per Mausklick „ich bin einverstanden“ erklärt (EG 32). Möglich ist auch eine aktive Auswahl technischer Einstellungen bei Diensten der Informationsgesellschaft (EG 31). Schweigen und Untätigkeit sind anders als etwa im römischen Recht keine Erklärung (EG 31). Dasselbe gilt für sogenannte Widerspruchslösungen. Bei einer vorformulierten „fingierten“ Einwilligung, die die betroffene Person etwa per Mail erreicht, muss sie bei Einwänden nicht widersprechen. Verzicht auf den Widerspruch ist keine eindeutige bestätigende Handlung. Gleiches gilt für Opt-out-Kästchen. Ihre Nichtbeachtung erzeugt keine Einwilligung.

Die Frage nach der Formwirksamkeit einer Einwilligung stellt sich auch im Medizinbereich (Buchner 2013: 340). Die Einwilligung des betroffenen Patienten in die ärztliche Verarbeitung seiner Daten muss zwar grundsätzlich nicht in Schriftform erfolgen. Stimmt der Patient damit aber auch wirksam der Weitergabe seiner Daten etwa an eine externe Abrechnungsstelle zu? Die freie Selbstbestimmung des Einzelnen würde bedeutungslos, wenn er sich bestimmten Angeboten und Entscheidungen nicht aktiv entziehen kann bzw. sich nicht dem Maß einer Anwendung zu entziehen weiß.

Ist eine wirksame Einwilligung in die Verarbeitung besonderer (sensitiver) Daten möglich?

Für die Verarbeitung besonderer Kategorien personenbezogener Daten enthält die Verordnung bereichsspezifische Verbote (Art. 9 Abs. 1 DSGVO). Es handelt sich jeweils um gebotene und nunmehr auch im Unionsrecht anerkannte informationelle Diskriminierungsverbote. Eine Einwilligung in die Verarbeitung von Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse und weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist nur dann wirksam, wenn die betroffene Person für einen oder für mehrere festgelegte Zwecke ausdrücklich eingewilligt hat (Art. 9 Abs. 2 lit. a DSGVO).

Diese Regelung kommt nicht zur Anwendung, wenn nach dem Unionsrecht oder dem Recht der Mitgliedstaaten das Verarbeitungsverbot durch die Einwilligung der betroffenen Person nicht aufgehoben werden kann (Art. 9 Abs. 2 lit. a DSGVO). Anders ausgedrückt: Die nationalen Gesetzgeber haben bei der Umsetzung der Einwilligungsbestimmung einen Gestaltungsspielraum. Sie können die Einwilligung in die Verarbeitung besonderer Datenkategorien ausschließen oder mit zusätzlichen Bedingungen versehen, etwa für genetische und biometrische sowie für Gesundheitsdaten (s. Art. 9 Abs. 4 DSGVO). Denn biometrische und genetische Daten (Art. 4 Nr. 13 und 14 DSGVO) zeichnen sich dadurch aus, dass sie eine eindeutige Identifikation der betroffenen Person ermöglichen.[6] Wenn Fingerabdrücke oder biometrische Daten zur Gesichtserkennung (EG 53 S. 3) verwendet werden oder Gesundheitsdaten (Art. 4 Nr. 15 DSGVO) Rückschlüsse auf den Gesundheitszustand oder die sexuelle Orientierung einer Person zulassen, dann fallen sie unter die Kategorie und den Schutz sensitiver Daten (Art. 9 Abs. 1 DSGVO). Ausnahmen von dem allgemeinen Verbot der Verarbeitung etwa von Gesundheitsdaten für Forschungszwecke (Art. 9 Abs. 2 lit. j und i DSGVO) sollten speziell im mitgliedstaatlichen Recht oder bei ausdrücklicher Einwilligung der betroffenen Person und bei bestimmten Notwendigkeiten (EG 51) konkretisiert werden.

Perspektiven

Die allgemeine Datenschutz-Grundverordnung hat notwendige Bedingungen gleicher informationeller Selbstbestimmung in der Union geschaffen. Varianten des mitgliedstaatlichen Datenschutzrechts – so auch das am 25. Mai 2018 in Kraft tretende neue Bundesdatenschutzgesetz – dürfen nur in vorgesehenen Fällen von den Vorgaben des Unionsrechts abweichen.

Bei der Berlin-Brandenburgischen Akademie der Wissenschaften findet sich zu einem Projekt der Verständlichkeitsforschung des Rechts folgender Text: „Ein juristischer Text soll verständlich, aber zugleich unmissverständlich sein, zwei Eigenschaften, die leicht im Widerstreit stehen“.[7] Übertragen auf die Anforderungen an eine selbstbestimmte Einwilligung kann demnach betont werden: Das Gemeinte muss nicht nur im Gesetz stehen, sondern sich auch aus einer unmissverständlichen wirksamen Einwilligungserklärung ergeben – und zwar einfach und nicht verklausuliert. Das Recht muss für diejenigen verständlich sein, die nach ihm handeln und leben sollen. Diese Forderung gewinnt im Europäischen Kulturerbejahr 2018 für das Menschenrecht auf Privatheit und Datenschutz als Teil unseres Kulturerbes große Bedeutung: Im Jahre 2018 darf nach der Datenschutzgrund-

Marie-Theres Tinnefeld

Prof. Dr. **Marie-Theres Tinnefeld** ist Juristin und Publizistin, mit zahlreichen Konferenzen und Veröffentlichungen im In- und Ausland zum Thema *Informationsrecht und europäische Rechtskultur*. Sie ist Mitglied im Beirat des FIfF e. V.

Zuletzt ist von ihr erschienen: *Überleben in Freiräumen. 12 Denkstücke* 2018, Verlag Böhlau, Wien/Köln/ Weimar; und Tinnefeld, Marie-Theres/ Buchner, Benedikt/Petri, Thomas/ Hof, Hans-Joachim, *Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht*, 6. Auflage 2017, Verlag de Gruyter, Berlin/ Boston.

verordnung die selbstbestimmte Einwilligung einer betroffenen Person in den einzelnen EU-Mitgliedstaaten nicht mehr unterschiedlich stark oder gering gewährleistet werden.

Der Beitrag erschien in vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftpolitik #211/212 (1/2018). Wir danken Redaktion und Autorin für die freundliche Genehmigung zum Nachdruck.

Referenzen

Arendt, Hannah 1967: Vita activa oder vom Tätigen Leben, München

Buchner, Benedikt 2013: Outsourcing in der Arztpraxis – zwischen Datenschutz und Schweigepflicht, MedR (Zeitschrift für Medizinrecht) S. 337–342

Borasio, Gian Domenico 2014: selbst bestimmt sterben, München

Ernst, Stefan 2017: Die Einwilligung nach der Datenschutzgrundverordnung, ZD (Zeitschrift für Datenschutz), S. 110–114

Fries, Jakob Friedrich 1803: Philosophische Rechtslehre und Kritik aller positiven Gesetzgebung, Jena

Guradze, Heinz 1956: Der Stand der Menschenrechte im Völkerrecht, Göttingen

Hoffmann-Riem, Wolfgang 2016: Innovation und Recht – Recht und Innovation, Frankfurt a. Main

Jarass, Hans D. 2016: GRCh, Charta der Europäischen Grundrechte, Kommentar (3. Auflage), München

Kühling, Jürgen/Buchner, Benedikt 2017: Datenschutz-Grundverordnung, Kommentar, München

Kafka, Franz 2004: Zur Frage der Gesetze und andere Schriften aus dem Nachlass (Taschenbuchausgabe), Frankfurt a. Main

Ramsey, Robert 1970: The Patient as Person, Yale University Press, New Haven

Schirrmacher, Frank 2011: Payback. Warum wir im Informationsalter gezwungen sind zu tun, was wir nicht tun wollen, und wie wir die Kontrolle über unser Denken zurückgewinnen, München

Schmale, Wolfgang/Tinnefeld, Marie-Theres 2017: Europa durch Menschenrechte, in: Datenschutz und Datensicherheit (DuD) Heft 6, S. 343–47

Spindler, Gerold 2012: Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung, Gutachten F zum 69. Deutschen Juristentag, F 1 ff.

Tinnefeld, Marie-Theres 2018: Überleben in Freiräumen. 12 Denk-Stücke, Wien/Köln/ Weimar

Tinnefeld et al. 2017: Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht (6. Auflage), Berlin, Boston

Will, Rosemarie 2018: Kein Ende des jahrzehntelangen Rechtsstreites zum Erwerb eines Medikaments zur Selbsttötung in: Grundrechte-Report 2018

Anmerkungen

1 *Mit der Perversion des „Euthanasie"-Systems am Beispiel der Ermordung von „geisteskranken" oder „schwierigen" Kindern durch Aushungern oder tödliche Spritzen von Nazi-Psychiatern befasst sich der Film „Nebel im August" (2016, Regie: Kai Wessel) nach dem gleichnamigen, 2008 erschienenen Buch, in dem Robert Domes das Leben und die Ermordung von Ernst Lossa darstellt, der zum fahrenden Volk der Jenischen gehörte, einer heterogenen Gruppe, die von den Nationalsozialisten als „Zigeuner" bezeichnet wurde.*

2 *Internationaler Pakt über bürgerliche und politische Rechte (IPbpR).*

3 *Tinnefeld, in Tinnefeld et al. 2017: Prolog S. XIX.*

4 *IT-Grundrecht = Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme; s. BVerfG, Urteil des Ersten Senats v. 27. Februar 2008 – 1 BvR 370/07 (=BVerfGE 120, 274 ff.).*

5 *Buchner/Kühling, in Kühling/Buchner 2017: Art. 7 Rn. 5 ff.*

6 *Tinnefeld, in Tinnefeld et al. 2017: 208 ff.*

7 *„Sprache des Rechts. Vermitteln, Verstehen, Verwechseln." Interdisziplinäre Arbeitsgruppe an der BBAW, http://www.bbaw.de/iag/ag_sprache/ueber.html.*

Rainer Rehak

(Meta-) Daten im Zeichen der Sicherheit?

Zum staatlichen Umgang mit vernetzten Datenbeständen

Mit der zunehmenden Digitalisierung hinterlassen die Handlungen von Menschen Metadaten in den jeweiligen Systemen. Sie werden für die kommerzielle Profilerstellung, aber auch für folgenschwere polizeiliche und geheimdienstliche Zwecke ausgewertet. Über diese technikgläubige Herangehensweise muss dringend diskutiert werden.

Seit ihrer Existenz sammeln und speichern staatliche Stellen Informationen über ihre BürgerInnen. Auch die damit eng verbundene Grenze zwischen als notwendig erachteter Verwaltung und weit darüber hinausgehenden Kontrollabsichten ist seit jeher Gegenstand gesellschaftlicher Diskussionen. Seit Jahrzehnten befinden wir uns nun im Prozess einer zunehmenden automatisierten Datenverarbeitung persönlicher, geschäftlicher sowie gesellschaftlicher Interaktionen – inzwischen lapidar *Digitalisierung* genannt. Informationen werden nicht mehr in dunklen Kellern in Form von papierenen Aktenmetern angelegt, aufbewahrt und mühsam manuell durchsucht, sondern können in vernetzen informationstechnischen Systemen erzeugt und verarbeitet werden. Volltextsuche, Mehrfachindexierung, Sortieren, Filtern und effizientes Speichern sind dabei nur noch Fingerübungen der Informatik, die in jedem Informatikbuch über Algorithmen nachzulesen sind.[1] Neuere Methoden drehen sich eher um das Finden von Korrelationen durch statistische Analysen oder das Entdecken ähnlicher Strukturen durch Muster(wieder)erkennung, beispielsweise mit *lernenden* künstlichen neuronalen Netzen (KNN) oder anderen heuristischen – und damit nicht-exakten – Ansätzen. Ist die Datengrundlage vergleichsweise groß und vielfältig, so fällt häufig der unscharfe, aber politisch und wirtschaftlich wirkmächtige Begriff *Big Data*. Wenn es darum geht, die Ergebnisse solcher Herangehensweisen zu interpretieren, stellen sich jedoch weitreichende Fragen: Was sagen beispielsweise Korrelationen über kausale Zusammenhänge aus?