Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

Prof. Ulrich Kelber

„Bei der Digitalisierung versagt nicht der Datenschutz“

Verbandstage Berufsverband der Datenschutzbeauftragten
Deutschlands (BvD) e.V.

Berlin, 9. Mai 2023

Es gilt das gesprochene Wort

Sehr geehrter Herr Spaeing,
sehr geehrter Herr Hartz,
sehr geehrte Damen und Herren,

I. [Einleitung]

es tut mir leid, dass ich den Zeitplan des heutigen Konferenztages ein wenig durcheinandergebracht habe, aber der Gesundheitsminister hat kurzfristig zu einem High-Level-Gespräch zu den aktuellen Gesetzesplänen zur Digitalisierung im Gesundheitswesen eingeladen, und da kann ich aus vielerlei Gründen nicht absagen.

Damit bin ich eigentlich auch gleich in medias res, bei wichtigen Projekten zur Digitalisierung im Gesundheitswesen, die angeblich am Datenschutz scheitern oder durch ihn behindert werden.

II. Die elektronische Patientenakte ePA

Wie die meisten von Ihnen wissen, war ich fast 20 Jahre lang Bundestagsabgeordneter. Das heißt, ich habe im Jahr 2003 mit darüber entschieden, übrigens aus Überzeugung, dass in Deutschland eine ePA eingeführt werden soll. Heute, 20 Jahre später, haben wir diese immer noch nicht wirklich, obwohl nach 2003 noch 15 Jahre ohne DSGVO und 16 Jahre ohne BfDI Ulrich Kelber Zeit gewesen wäre.

Es liegt also nicht am Datenschutz. Sondern es liegt an den vielen Akteuren im Gesundheitswesen, die sich seit 20 Jahren behindern, beharken und gegenseitig beschuldigen. Die – oft aus wirtschaftlichen Motiven – kein Interesse an Digitalisierung, digitalen Übertragungswegen und gemeinsamen Datenformaten hatten und haben.

Jens Spahn hat als Minister versucht, wenigstens das Digitalisierungsprojekt ePA endlich umzusetzen. Herausgekommen ist eine Testphase mit einem wenig nutzerfreundlichen Produkt, dass weder auf dem aktuellen Stand der Technik ist, noch lange vereinbarte und versprochene datenschutzrechtliche Minimalstandards erfüllt. Kein Wunder, dass bisher kaum ein gesetzlich Versicherter dieses Produkt nutzt.

Minister Lauterbach versucht nun eine weitere Beschleunigung und mit einem obligatorischen Opt-Out möglichst allen gesetzlichen Versicherten eine ePA-Nutzung schmackhaft zu machen. Bis 2024 soll das umgesetzt sein, aber neben den noch nicht gelösten datenschutzrechtlichen Problemen sind ganz viele wichtige Fragen noch nicht beantwortet. Sollen z.B. auch die bisher in Praxen, Kliniken und Krankenkassen vorhanden Patientendaten in die ePA eingepflegt werden (was ja sinnvoll wäre) und wer soll dies tun? Sind diese Daten miteinander kompatibel und strukturiert und für alle Praxen, Krankenhäuser und Apotheken nutzbar und machen alle diese Institutionen mit? Können die Versicherten tatsächlich entscheiden, wer welche ihrer Daten lesen und nutzen darf und können sie selbst überhaupt diese Daten lesen? In der ePA eines Bekannten, der sie schon nutzt, erscheinen z.B. alle Daten mit der Dateibezeichnung „Dokument“ – wer soll damit etwas anfangen können?

Ich habe vor ein paar Wochen auch schon vor der Bundespressekonferenz gesagt: Ich wäre der erste, der eine ePA nutzt, alle seine Daten einstellt und allen Ärzten und Kliniken, die ich besuche, zur Verfügung stellt. Aber dafür muss dieses Ding doch erst einmal funktionieren und ich muss wissen, dass meine Daten in der ePA nutzbar und sicher sind. Genau das ist aber bis heute nicht der Fall.

Deswegen machen wir, das BSI und meine Behörde, bei ePA und eRezept nicht etwa Auflagen bei der Nutzung, sondern Vorgaben zur besseren Ausgestaltung, verlangen z.B. die Schließung von eklatanten Sicherheitslücken, die wir auffinden. Gesundheitsdaten sind die sensibelsten Daten der Menschen, deshalb darf es hier kein „da drücken wir mal die Augen zu“ oder „das können wir ja später noch nachbessern“ geben. Oder setzen Sie sich in ein Auto, wenn die Bremsen erst in einem Jahr nachgeliefert werden?

Im Gesetz zur ePA ist außerdem vorgesehen, das die Daten aus der elektronischen Patientenakte für die Forschungsnutzung freigegeben werden können, was für die Forschung von großer Bedeutung wäre. Die freigegebenen Daten sollen an das Forschungsdatenzentrum beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) übermittelt werden. Hier befinden sich übrigens schon die Abrechnungsdaten (sog. „Routinedaten“) der gesetzlichen Krankenkassen. Aber das Forschungsdatenzentrum hat seinen Betrieb noch nicht aufgenommen, eine Nutzung der Daten für Forschungszwecke ist deshalb noch nicht möglich. Die Einrichtung dieses Forschungsdatenzentrums ist deshalb besonders dringlich. Und nein, die Verzögerung dort liegt ebenfalls nicht am Datenschutz.

III. Gesundheitsdatenforschung mit Datenschutz

Ganz ähnlich ist es im Bereich der allgemeinen Forschung mit Gesundheitsdaten. Die Wissenschaftsfreiheit als Freiheit von Forschung und Lehre ist wie der Datenschutz ebenfalls durch das Grundgesetz als Grundrecht geschützt. Ebenso ist die Datenschutzgrundverordnung forschungsfreundlich und privilegiert die Nutzung personenbezogener Daten zu Forschungszwecken gegenüber anderen Verarbeitungszwecken.

Ich bin daher auch der festen Überzeugung, dass das geltende Datenschutzrecht – anders als immer wieder behauptet – der verantwortungsbewussten Gesundheitsforschung überhaupt nicht entgegensteht. Wir Datenschützer haben sogar ein großes Interesse daran, eine im Interesse der Allgemeinheit stehende bestmögliche Nutzung von Gesundheitsdaten in der Forschung zu ermöglichen.

In diesem Sinne hat die Datenschutzkonferenz im letzten Herbst auch die Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung verabschiedet, in der Ansätze für hierfür erforderliche Voraussetzungen vorgestellt werden.

Und, meine Damen und Herren, hierbei sprechen wir nicht von unrealistischen oder praxisfremden Forderungen, sondern praxisorientierten Ansätzen, wie der Schaffung einheitlicher Formate und Standards, Lösungen zur Verschlüsselung, Anonymisierung und Pseudonymisierung (jedenfalls soweit dadurch das Forschungsziel nicht

gefährdet wird), der Einführung von Treuhändermodellen oder der Forderung nach klaren und bundesweit einheitlichen rechtlichen Rahmenbedingungen.

Ein Forschungs- und Gesundheitsdatenzugangsgesetz, in dem man entsprechende Regelungen treffen könnte, fordern wir Datenschützer übrigens schon seit 2004. In dieser Zeit ist es den Ländern nicht gelungen, die nach ihren Krankenhausgesetzen erfassten Daten so zu erfassen, dass sie bundeseinheitlich genutzt werden können. Wieviel weiter könnten wir bei den Forschungsdaten sein, wenn der politische Wille und die Prioritätensetzung da gewesen wären?

Eine der wichtigsten Forderungen aus datenschutzrechtlicher Sicht ist aber vor allem eine echte Transparenz für die Betroffenen, mit deren Daten geforscht wird. Nur wer weiß, was von wem mit seinen Daten gemacht wird, kann Vertrauen in den Prozess entwickeln. Und Vertrauen ist eine Schlüsselvoraussetzung, wenn wir wollen, dass Menschen dazu bereit sind, Informationen aus ihrer Intimsphäre mit gutem Gewissen für das Wohl der Allgemeinheit zur Verfügung zu stellen. Ein guter Datenschutz ist ein wesentliches Element zur Schaffung dieses Vertrauens.

Das waren jetzt nur zwei Beispiele aus dem Gesundheitsbereich, die mich im Laufe des Tages beim Gespräch mit dem Minister weiter beschäftigen werden. Es sind aber auch zwei traurige, leider passende Beispiele dafür, wie lange Digitalisierungsprojekte in unserem Land brauchen können, wenn nur genügend Verbändevertretungen,

Länderegoismen und mangelnder politischer Durchsetzungswille zusammenwirken. Ich hätte bei der Abstimmung vor 20 Jahren jedenfalls nicht gedacht, dass eine gut funktionierende und sichere elektronische Patientenakte auch 2023 noch nicht im Einsatz ist.

IV. Digitalisierung von Verwaltungsakten

Aber nicht nur im Gesundheitswesen läuft in Sachen Digitalisierung einiges schief. Ich hatte erst kürzlich wieder so ein Erlebnis, wo mir als Informatiker wirklich jedes Verständnis fehlt. In meiner Heimatstadt Bonn kann ich die Anmeldung eines neuen PKWs inzwischen online abwickeln, ohne lästigen Termin beim Bürgeramt. Soweit zumindest die Theorie. Gescheitert ist diese Online-Anmeldung dann aber daran, dass das „E“ für Elektroauto auf dem Kennzeichen nicht verarbeitet werden konnte. Ich musste am Ende mich dann eben doch frühmorgens am Bürgeramt anstellen und hoffen, dass ein Termin ausfällt, weil reservieren konnte man erst wieder Wochen später. Was ist das für eine Digitalisierung von Verwaltungsleistungen, die neue Entwicklungen auch nach acht Jahren noch nicht aufgenommen hat?

Was ist das für eine Digitalisierung von Verwaltungsleistungen, wenn die Papierformulare einfach eins zu eins in ein digitales Formular überträgt ohne die Möglichkeiten des digitalen „wenn ja, dann x, sonst y“ zu nutzen? Wenn ich dreimal gefragt werde, ob ich eine weitere Staatsbürgerschaft angeben will, weil dafür früher drei Zeilen im analogen Formular vorhanden waren.

Wenn ich solchen digitalen Verwaltungslösungen begegne und Sie alle kennen sicher auch welche, dann macht mich das erst einmal sprachlos. Das sind die klassischen Fälle für „gut gemeint ist nicht gleich gut gemacht“ und all diese Beispiele haben nichts, absolut nichts mit Datenschutzvorgaben zu tun. Sie sind ein Teil des Problems, dem ich immer wieder mit unserem Credo begegne: wer Datenschutz nicht von Anfang an mitdenkt, mitentwickelt und einbaut, der hat am Ende schlechte Lösungen, die teuer nachgesteuert werden müssen. Agile Entwicklung beginnt damit, ein sicheres rechtliches und technisches Fundament zu wählen.

V. Datenschutz als Differenzierungsmerkmal

Datenschutz ist gelebter Grundrechtsschutz und wichtiger Vertrauensanker für die Digitalisierung unserer freiheitlichen Gesellschaft. Damit hat Digitalisierung auch eine enorme wirtschaftspolitische Dimension. Hier geht es darum, Prozesse durch die Digitalisierung effizienter zu gestalten. Aber es geht auch darum, z.B. im produzierenden Gewerbe völlig neue Wege zu beschreiten. Um perspektivisch viel kundenspezifischer, termingerechter und ressourcenschonender zu produzieren.

All diese Systeme müssen „Daten“-sicher sein. Denn es stellen sich neue Herausforderungen, etwa mit Blick auf das Thema Industriespionage und Sabotageschutz. Ohne starken Datenschutz und ein hohes Maß an Datensicherheit steigen die Risiken hierfür massiv an.

Gerade in Deutschland als dem ,,Land der Entwickler“ und der vielen kleinen und mittelständischen Unternehmen, die mit ihren Ideen „hidden Champions“ sind, wäre ein Know-how- und Wissensabfluss existenzbedrohend. Wenn Produktionsabläufe und Arbeitsverfahren digitalisiert werden, ist man gut beraten, die genutzten IT-Systeme bestmöglich zu schützen. Datenschutz und Datensicherheit sind kostengünstiger, sicherer und ressourcenschonender. Und sie schützen eben nicht nur Menschen, sondern auch Ideen, Patente, Wissen, Verfügbarkeit, Glaubwürdigkeit und Kooperationsfähigkeit.

VI. Datenschutz als Wettbewerbsvorteil nutzen

Es wird hier hoffentlich niemanden überraschen, wenn ich sage, was ich immer betone und auch bei Ihnen schon erwähnt hatte: Datenschutz ist kein Hemmschuh und wir Datenschützer sind keine Bremser, sondern Datenschutz ist innovationsfördernd und wir Datenschützer können mit den meisten digitalen Lösungen sehr viel besser leben als mit ihren analogen Vorgängern, zumindest wenn sie gut gemacht sind.

Datenschutz ist keine heilige Kuh, die über allem anderen steht, sondern wird immer zusammen mit anderen Anforderungen gedacht. Und Datenschutz ist kein Wirtschaftshemmnis und damit auch nicht der Sargnagel der deutschen Unternehmen. Datenschutz könnte noch viel stärker Innovationsträger und Wettbewerbsvorteil sein, wenn wir uns darauf einlassen! Unser Ziel sollte es sein, weltweit Marktführer bei sicheren und datenschutzkonformen Produkten und Dienstleistungen zu werden.

Datenschutzkonforme Produkte „Made in Europe“ könnten sich als positives Differenzierungsmerkmal am Markt etablieren. Weil wir durch unsere Historie beim Thema, unserem Rechtsrahmen und den Datenschutzbeauftragten in Unternehmen und Behörden einen Glaubwürdigkeitsvorsprung haben. Gerade jetzt, wo die Datenschutzgrundverordnung weltweit als Referenz und Blaupause für eigene Rechtsvorgaben herangezogen wird, in Korea, Japan, Mexiko, Indien, Brasilien und in US-Bundesstaaten sowie auf der nationalen Ebene der USA. Zuletzt sogar in China, wenn auch aus ganz anderen Gründen.

Datenschutz und Datensicherheit müssen als wichtige Erfolgsfaktoren wahrgenommen werden. Beides sind großartige Qualitätsmerkmale im globalen Markt. Datenschutz muss daher – ich wiederhole es - von Anfang an als Teil der „DNA" eines jeden Produkts und einer jeden Dienstleistung mitgedacht werden.

Die Grundsätze des Datenschutzes durch Technikgestaltung („Data Protection by Design“) und der datenschutzfreundlichen Voreinstellungen („Date Protection by Default“) sind ein wichtiger Bestandteil der Datenschutzgrundverordnung (Art. 25 DSGVO). Ich will daher auch die Hersteller von IT-Verfahren und IT-Produkten stärker in die Pflicht nehmen. Es kann und darf nicht sein, dass es dem Softwarehersteller egal sein kann, ob sein Produkt datenschutzkonform und er nur dann verantwortlich ist, wenn er es selbst einsetzt und damit personenbezogene Daten verarbeitet. Der Grundgedanke der Herstellerhaftung muss auch ins Datenschutzrecht übertragen werden.

Das würde dann auch kleine und mittelständische Unternehmen von Pflichten und Bürokratie befreien können.

VII. Aktuell: KI und KI-Verordnung

Ich will noch kurz auf die aktuelle Entwicklung in Sachen Künstlicher Intelligenz (KI) eingehen, auch wenn dies kein reines Datenschutzthema ist, sondern sehr viele wirtschaftliche und gesellschaftliche Bereiche betrifft und auch dort Regelungen bedarf.

Die Vorstellung des Programms ChatGPT Anfang des Jahres durch die Firma OpenAI hat jede Menge höchst unterschiedliche Reaktionen hervorgerufen. Am Anfang haben es viele eher als nettes Spielzeug genutzt oder sich tatsächlich die Hausaufgaben schreiben lassen. Die wichtigste Wirkung war aus meiner Sicht aber, dass die Suchscheinwerfer der Medien im großen Stil auf KI, ihre Nutzen, Wirkungen, Möglichkeiten aber auch Fehlentwicklungen geworfen haben. Die Tatsache, dass ChatGPT einfach Dinge erfindet, wenn es nicht genügend Trainingsdaten/Wissen hat oder auch die mittels KI erzeugten Bilder von einer vermeintlichen gewalttätigen Verhaftung Donald Trumps in New York verdeutlichen die Risiken, die mittels KI erzeugt werden können.

Ich konnte mir auf einer Konferenz vor zwei Wochen in Italien weitere KI-Anwendungen als kommende Erweiterungen weit verbreiteter Softwarelösungen anschauen, die absolut nützlich und arbeitserleichternd sind.

Es ist wie immer nicht alles nur weiß oder schwarz, sondern es gibt verdammt viel dazwischen.

Aber auch bei diesen nützlichen Erweiterungen stellen sich natürlich auch neue datenschutzrechtliche Fragen.

Die EU-Kommission arbeitet derzeit intensiv an einer KI-Verordnung, die ich – Stand heute – für im Grunde sinnvoll und zielführend halte. Das liegt sicher auch daran, dass die Vorschläge vielen Handlungsempfehlungen der Datenethikkommission entsprechen, die wir vor vier Jahren vorgelegt haben. Ziel einer KI-Regulierung muss sein, die Möglichkeiten der KI intensiv zu nutzen, wo sie nicht schaden können und dort einzugreifen, wo Menschen, Unternehmen oder auch die Gesellschaft insgesamt Schaden nehmen könnten.

Es wird sicher nicht einfach sein, hier die Grenzen immer genau zu ziehen, aber es ist notwendig. Der Datenschutz ist hier insofern gefragt, als dass er mit dafür Sorge tragen muss, dass die Trainingsdaten nicht schon diskriminierend sind, weil sich dies im „Lernprozess“ immer weiter potenziert oder geklärt ist, welche Daten zum Schutz dieser Daten nicht verwendet werden dürfen etc.

Meine Behörde hat sich bereits früh mit den Einsatzmöglichkeiten von KI gerade auch im Sicherheitsbereich auseinandergesetzt und wird dies auch weiter tun. Wir bauen die Kompetenz im Bereich KI strategisch auf und aus.

VIII. Schluss

Kurz und gut: es bleibt spannend und ich hoffe, Sie alle werden dabei weiter die Fahne des Datenschutzes hochhalten. Und dafür, dass Sie alle das schon so lange tun, möchte ich mich herzlich bedanken.

Wir können uns Datenschutz nämlich nicht nur leisten, wir müssen es sogar – für die Menschen genauso wie für die Wirtschaft.

Ich danke Ihnen für Ihre Aufmerksamkeit.