Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Prof. Ulrich Kelber

„Digitalisierung und gute Datenpolitik“

bei Summer Talk der FDP-Bundestagsfraktion

Berlin, 18. August 2020

Es gilt das gesprochene Wort

Sehr geehrte Damen und Herren,

I. [Einleitung]

Herzlichen Dank für die Einladung. Ich freue mich, heute mit dabei sein zu dürfen.

Die Digitalisierung unserer Welt schreitet voran. Seit Beginn der Corona-Pandemie ist der Druck auf noch durchgreifendere und noch schnellere Digitalisierung massiv gestiegen. Alle haben bemerkt, an wie vielen Stellen wir mehr und bessere digitale Produkte und Dienstleistungen brauchen, als viele bisher dachten.

Der Deutsche Bundestag, in dessen Räumen wir hier sind, ist da ein wunderbares Beispiel. Wie Sie vielleicht wissen, war ich selbst fast 20 Jahre Mitglied des Parlaments. In allen Ausschusssälen hängen seit dem Umzug von Bonn nach Berlin Fernseher und Kameras, um Videokonferenzen zu ermöglichen. Wie oft sind die in den letzten 20 Jahren genutzt worden? Ich brauche nur eine Hand, um die Male zu zählen, an denen ich an so etwas teilgenommen habe. Seit dem Frühjahr diesen Jahres ist das völlig anders. Jetzt wird die Technik endlich eingesetzt, wenn sie denn funktioniert, jetzt werden unzählige Besprechungen und Ausschusssitzungen und Anhörungen online abgewickelt. Und: Es funktioniert.

Ähnliches erlebe ich im Umgang mit home office. Da gab es auch in meinem Haus einige Vorbehalte. Trotzdem haben wir bereits 2019 alle Mitarbeitern mit für unsere vertraulichen Vorgängen geeigneten Laptops ausgestattet und vollständig auf die elektronische Akte umgestellt. Das hat uns gut durch den Lockdown gebracht. Mein Haus hat weitgehend ganz normal weiterarbeiten können, obwohl teilweise bis zu 90 Prozent der Mitarbeiterinnen und Mitarbeiter im home office gearbeitet haben.

Was ich sagen will: die weiterschreitende Digitalisierung braucht vor Mut sich auf Neues einzulassen und das begründete Vertrauen, dass die neuen Möglichkeiten keine Rückschritte in Sachen Arbeitsschutz, Datenschutz, Freiheit und Schutz der Kommunikation mit sich bringen.

Deshalb ist es aus meiner Sicht so wichtig, diese Ziele bei Neuentwicklungen stets von Anfang an mitzudenken, mit zu Bedenken, wenn ich diese kleine Anspielung hier machen darf.

Wie die Entwicklung der Corona-Tracing-App gezeigt hat, schafft Transparenz im Entwicklungsprozess und Berücksichtigung des Datenschutzes von Anfang an erst das notwendige Vertrauen, damit die Menschen diese App auch nutzen. Sie ist nicht von ungefähr die erfolgreichste Corona-App in Europa. Diese Ziele müssen deshalb auch das Fundament der Datenstrategie der Bundesregierung sein. Denn auch in anderen Bereichen wird die Digitalisierung nur gelingen, wenn die Bürgerinnen und Bürger Vertrauen darin haben.

Nicht Daten, sondern Vertrauen ist die Währung des 21. Jahrhunderts.

II. Datenstrategie

Eine Datenstrategie innerhalb einer Digitalisierungsstrategie muss daher zwingend eine klare Linie beim Datenschutz beinhalten.

Datenschutz ist in Europa von den Grundrechten abgeleitet und nicht optional. Eine Kopie der Datenstrategien der USA oder China ist daher zum Glück in Europa nicht möglich. Wenn wir den Datenschutz also ohnehin als Faktor berücksichtigen müssen, warum machen wir ihn dann nicht gleich zum Erfolgsfaktor? Mein Vorschlag: Lassen Sie uns Datenschutz als Innovationsmotor einer Digitalisierung „made in Germany“ bzw. „made in Europe“ nutzen.

Bereits heute sind Daten nicht mehr auf ein paar Informationen über unsere Person beschränkt. Sie ermöglichen ein vollständiges Abbild des Menschen, seiner Familie und Freunde, seiner Ausbildung und Arbeit, seiner Hobbys, Krankheiten, Vorlieben und Schwächen, seines täglichen Bewegungsradius, seine Einkäufe, seine politischen und religiösen Einstellungen, seines Gemütszustands usw. Das ist angesichts der Verschränkung des digitalen und des nicht-digitalen Lebens von herausragender Bedeutung.

Die technische Fortentwicklung macht es möglich, dass diese Daten bis ins letzte Detail gespeichert und dauerhaft vorgehalten werden können. Speicherplatz ist schon lange keine Frage des Geldes mehr und die heutigen Rechnerleistungen ermöglichen immer neue Auswertungen in Echtzeit.

Diese Eigenschaften und technischen Möglichkeiten sind es auch, die personenbezogene Daten so viel wertvoller machen. Profilbildung und Scoring machen Bürgerinnen und Bürger transparent für Privatunternehmen und natürlich auch für den Staat. Solche Daten können dazu verwendet werden, Krankheiten besser zu verstehen und vielleicht sogar zu heilen. Sie können sinnvoll für Bildung und Planung genutzt werden. Sie können maßgeschneiderte Angebote im Interesse der Menschen ermöglichen.

Gleichzeitig aber sind sie geeignet, um Menschen zu übervorteilen, auszugrenzen oder sogar zu manipulieren . Profilbildung und Scoring hat längst die Nische der individualisierten Werbung verlassen. Das müssen alle verstehen, die über die Regeln der Datenverwendung entscheiden. Es geht nicht mehr um die Werbeerlöse deutscher Verlagshäuser, es geht um die Grundlagen einer offenen, demokratischen Gesellschaft. Btw: Erste Erkenntnisse zeigen, dass die verhaltensbasierte Werbung die Einnahmen der Verlagshäuser gar nicht signifikant erhöht. Es wird Zeit, dass mehr Studien zeigen, dass der Kaiser verhaltensbasierte Werbung nackt ist.

Deshalb benötigen wir klare Leitplanken, die dort Grenzen ziehen, wo Daten von Bürgerinnen und Bürger nicht mit ihrem informierten, konkreten und freiwilligen Einverständnis und zu ihrem Wohl, sondern zu deren Nachteil genutzt werden oder genutzt werden können.

Diese Leitplanken können nur durch einen funktionierenden Datenschutz mit klaren Regelungen und wirksamen Sanktionen gewährleistet werden. Ohne diesen kann der Grundrechtsschutz in unserer digitalisierten Welt nicht sichergestellt werden. Die Idee, nur Missbrauch zu sanktionieren und ansonsten die Regeln fallen zu lassen, ist entweder hoch naiv oder interessensgetrieben. Das wäre unkontrollierbar.

Diese essentielle Aufgabe des Grundrechtsschutzes kann Datenschutz übrigens gewährleisten, ohne die digitale Entwicklung zu blockieren. Digitalisierung und Tracking sind nicht gleichbedeutend, Profilbildung nicht die einzige Art von Wertschöpfung digitaler Angebote. Datenschutz als Ausdruck von Grundrechten und „Digitaler Souveränität“ gibt digitaler Innovation eine Richtung. Er verbindet unsere europäischen Werte mit einem digitalen Geschäftsmodell.

Eine Datenstrategie der Bundesregierung muss den Bürgerinnen und Bürgern ermöglichen, die Hoheit über ihre digitalen Datenspuren zurückzugewinnen. Wer kann heute behaupten zu wissen, welche Informationen über ihn an welchen Stellen vorliegen und – noch wichtiger – welche Schlüsse dort aus diesen Informationen gezogen werden?

Gerade das ist aber doch eine elementare Voraussetzung um entscheiden zu können, wie man mit seinen Daten umgeht und wem man sie zur Verfügung stellen will.

Wenn Deutschland und Europa anderen Wirtschaftsräumen bei der Digitalisierung hinterherhinken, dann nicht, weil es Probleme mit Datenschutzvorschriften gibt. Weder bei der Registermodernisierung, wo der Föderalismus und das Ressortdenken zu beachten sind, und schon gar nicht bei der elektronischen Patientenakte, wo die Datenschutzanforderungen seit Jahren klar sind. Unbegreiflich, dass sie dann zum Start der ePatientenakte nicht fertiggestellt sind.

Glaubwürdiger Datenschutz by design, also schon bei der Planung berücksichtigt, schützt nicht nur unsere Werte, sondern kann noch zum Alleinstellungsmerkmal für Produkte und Dienstleistungen auf den Weltmärkten werden. Überall gibt es Nachfrage für solche Angebote. In Ländern ohne Datenschutzregelungen und mehr noch dort, wo die EU-DSGVO Pate für eigene Regelungen steht.

In Kalifornien wurde kürzlich ein neues Datenschutzrecht eingeführt, dass in Teilen sogar noch schärfer ist als die DSGVO. Nach der Logik der Datenschutzkritiker müssten in Konsequenz die digitalen Innovationen aus dem Silicon Valley fortan stagnieren. Ich bezweifle, dass das der Fall sein wird. Vielmehr sehe ich, wie die großen amerikanischen IT-Firmen das Thema Datenschutz als Wettbewerbsmerkmal für sich besetzen.

Diese Herangehensweise würde ich mir auch für die hiesige Wirtschaft wünschen. NY, Japan, Korea, Indien, Brasilien und Mexiko orientieren sich an der DSGVO. Diese Chance sollten unsere Unternehmen nutzen, sie hätten auf diesen Märkten einen Know-How- und Vertrauensvorsprung, wenn sie nur endlich vom Jammermodus in den Wettbewerbsmodus umschalten würden.

Die Datenethikkommission hat der Bundesregierung wichtige Empfehlungen gegeben, wie datenschutzfreundliche Innovationen gezielt gefördert werden könnten. Gerade im Bereich Dataspaces, persönliche Datenmanagementsysteme und Datentreuhänder sowie dezentrale KI könnte Deutschland leicht in Führung gehen. Auch im Bereich der Interoperabilität können Regierung und Gesetzgeber Voraussetzungen schaffen, damit die bestehenden Oligopole abgebaut werden und Raum für europäische Wettbewerber entsteht.

III. Datentreuhänder

Der in der öffentlichen Diskussion vielfach verwendete Begriff des Datentreuhänders wird in verschiedenen Kontexten sehr unterschiedlich gebraucht. Es gibt hier beispielsweise Projekte des BMJV (Einwilligungsmanagement) und des BMWi (Cookie-Nutzung). Während das Projekt des BMJV zum Einwilligungsmanagement das Ziel verfolgt, den Nutzern die Vornahme von Datenschutzeinstellungen zu erleichtern, verfolgt das BMWi hingegen im Wesentlichen das wirtschaftspolitische Ziel, es der deutschen Wirtschaft zu ermöglichen, Cookies zu setzen, ohne durch die Anbieter wie Google daran gehindert zu werden.

Zudem werden im Bereich der Wirtschaft Datentreuhandmodelle diskutiert[1] und ganz neu, das BMG führt im Rahmen der elektronischen Patientenakte eine Vertreterregelung ein. Wenn über Datentreuhänder gesprochen wird, muss also zunächst klar sein, welches Begriffsverständnis gemeint ist.

[1] (vgl. S. 5f. des Positionspapier der CDU/CSU-Fraktion im Deutschen Bundestag zur Datenstrategie der Bundesregierung, Anlage)

Der BfDI hat sich bisher mit dem Konzept der Datentreuhänder in Zusammenhang mit Personal Information Management Systems (PIMS) beschäftigt. Bei PIMS handelt es sich um digitale Dienstleistungen, die zum Ziel haben, den Betroffenen Kontrolle über ihre personenbezogenen Daten zu ermöglichen und sie von Entscheidungen zu entlasten, die sie überfordern, sei es technisch (Einstellungen) oder fachlich (Forschung).

Datentreuhand-Modelle im Rahmen der PIMS würden eine beauftragte und vordefinierte Fremdverwaltung der Daten der Nutzenden ermöglichen. Im Interesse der Rechtssicherheit wäre es wünschenswert, wenn die Aktivitäten im Rahmen von PIMS rechtlich zumindest „umhegt“ wären. Aus datenschutzrechtlicher Sicht muss dabei stets die Frage im Auge behalten werden, inwiefern der nationale Gesetzgeber angesichts der Vorgaben des Europäischen Datenschutzrechts diesbezüglich über Regelungsspielräume verfügt. Dies hängt davon ab, wie das jeweilige PIMS genau ausgestaltet ist.

Der rechtliche Rahmen für Datentreuhänder muss aus datenschutzrechtlicher Sicht so ausgestaltet werden, dass Interessenkonflikte der Datentreuhänder ausgeschlossen werden. PIMS müssen eindeutig den Interessen der betroffenen Personen dienen und dürfen nicht an der Nutzung der Daten verdienen. Diese Forderung wurde durch uns auch in das Gutachten der Datenethikkommission (DEK) eingebracht.

Eine Realisierung von PIMS ist nur dann möglich, wenn Kommunikationsprotokolle etc. standardisiert werden und offene Schnittstellen geschaffen werden. Auch hier braucht es Vorgaben. Wer keine Cookie-Banner oder ähnliches will, sollte datenschutzfreundlichere Angebote machen oder eben verbindliche Instrumente wie PIMS vorantreiben.

Im Bereich der Wirtschaft werden Datentreuhandmodelle sowohl im B2B als auch im B2C-Bereich diskutiert. Im B2B-Bereich sollen durch Datentreuhänder gegenseitige oder auch einseitige Datennutzungsrechte zwischen Unternehmen eingeräumt werden. Mögliche Anwendungsgebiete sind der Zugriff auf Gerätedaten durch Hersteller und Nutzer in der Produktion, aber auch die Bereitstellung von Kundendaten an einen Dritten. Im B2B-Bereich ist immer zu prüfen, ob personenbezogene Daten betroffen sind. Dies kann bspw. auch bei Gerätedaten der Fall sein, wenn diese Rückschlüsse auf den bedienenden Mitarbeiter ermöglichen.

Sobald personenbezogene Daten betroffen sind, sind bei der Ausgestaltung eines Datentreuhandmodells die datenschutzrechtlichen Vorschriften einzuhalten. Sollen beispielsweise Kundendaten nur anonymisiert zur Verfügung gestellt werden, so ist u. a. genauestens zu prüfen, ob das Anonymisierungsverfahren wirklich zu anonymen oder nur zu pseudonymen Daten führt.

Im B2C-Bereich werden ebenfalls viele Datentreuhandmodelle diskutiert. Hierdurch sollen die Nutzer die Möglichkeit haben, „an der Wertschöpfung“ aus ihren Daten zu profitieren. Dieses Konzept hat Parallelen zur Diskussion um das „Dateneigentum“. Das Konzept des Dateneigentums wird vom BfDI und der DEK abgelehnt. Solche Datentreuhandmodelle im B2C-Bereich sind aus datenschutzrechtlicher Sicht sehr kritisch zu hinterfragen.

Eine Vermischung von Datentreuhändern i. S. d. PIMS mit dem Wertschöpfungsansatz im B2C-Bereich sollte aus Datenschutzsicht nicht erfolgen. Hier sind Interessenkonflikte, die es auszuschließen gilt, vorprogrammiert.

IV. Datentransfer

Ein weiterer wichtiger und ganz aktueller Punkt ist die Frage des Datentransfers in Drittländer. Der EuGH hat vor drei Wochen das Privacy Shield, welches große Teile des Datentransfers zwischen der EU und den USA regelte, für unwirksam erklärt und damit die Rechte der Betroffenen im internationalen Datenverkehr gestärkt.

Der EuGH macht deutlich, dass internationaler Datenverkehr weiter möglich ist. Dabei müssen aber die Grundrechte der europäischen Bürgerinnen und Bürger beachtet werden. Er stellt hohe Anforderungen an die Nutzung etwa von Standardvertragsklauseln und besonderer Schutzmaßnahmen, die Unternehmen und Behörden ergreifen und Aufsichtsbehörden kontrollieren müssen.

Dies wird für alle Beteiligten noch ein hartes Stück Arbeit.

Aber auch wenn wir bei den Fragen des internationalen Datentransfers zuerst immer auf die USA und die amerikanischen Internetfirmen schielen, so ist dieser Focus deutlich zu eng. Man kann die Tiraden von US-Präsident Trump gegen TikTok und WeChat für Wahlkampfgetöse halten und als Muskelspiele abtun, dahinter verbergen sich aber eine Unmenge von Fragen die wir baldmöglichst klären müssen. Was passiert mit transferierten Daten in Russland, Indien, Indonesien oder China? Welche Zugriffsmöglichkeiten haben die jeweiligen Regierungen und Sicherheitsdienste dort auf Kommunikations- und Wirtschaftsdaten? Welche Rechte haben die europäischen Bürgerinnen und Bürger in Fällen des Datentransfers dorthin? Wir haben es in zahlreichen Fällen ja nicht nur mit Drittländern ohne adäquate Datenschutzgesetzgebung zu tun, sondern mit einem regelrechten Clash der Rechtskulturen. Wie gehen wir damit auf Dauer um und welchen Rechtsrahmen müssen wir für den Datentransfer in solche Länder setzen?

Der Datentransfer in Drittländer wird uns in den nächsten Monaten und Jahren verstärkt beschäftigen und ich gestehe offen, dass auch ich da noch viele offene Fragen , aber wir in Europa dürfen uns nicht vor dem Thema wegducken.

Ich hoffe, dass ich damit ein paar Punkte ansprechen konnte, über die wir heute Abend intensiv diskutieren können und die Ihnen als Anregung dienen, Ihre Leitlinien für eine liberale Datenpolitik zu entwickeln.

Ich danke Ihnen für Ihre Aufmerksamkeit.