Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

Prof. Ulrich Kelber

„Digitalisierung und Datenschutz“

Vortragsreihe Deutsche Bundesbank

„Experten zu Gast“

Dienstag, 30. November 2021
Virtuell

Es gilt das gesprochene Wort

Sehr geehrte Damen und Herren,

sehr geehrte Frau Berg,

I. [Einleitung]

ich freue mich, heute hier bei Ihnen zu sein und Ihnen zu wichtigen, aktuellen Themen die Sicht des Datenschützers zu erläutern.

Als Banker gehen Sie tagtäglich mit Daten um, die für vielen Menschen genauso sensibel sind, wie Gesundheitsdaten, denn bei den Finanzen hört bei uns Deutschen bekanntlich der Spaß auf. Ich finde es immer wieder faszinierend, aber auch höchst irritierend, dass viele Menschen auf gar keinen Fall preisgeben wollen, wieviel sie verdienen, aber in den sozialen Netzwerken munter Privates und Schützenswertes ausplaudern, frei nach dem Motto „ich habe nichts zu verbergen“.

II. Sensibilisierung für Datenschutz

Es ist heute problemlos möglich, schon nach nur einem Tag ein fast komplettes Bild eines Menschen zu erstellen: Freunde, Verwandte, Arbeitsplatz, Wege zum Ausbildungsplatz, durchschnittliche Arbeitszeit, Hobbys, politische Einstellung, Vereine, Krankheiten, Vorlieben für Filme, Bücher, Musik, Geschwindigkeitsüberschreitungen oder andere Verkehrssünden, Präferenzen für Marken, Kleidungsgröße, Gemütszustand und Verfassung - all das und noch viel mehr geben wir tagtäglich bewusst, unbewusst, direkt und indirekt von uns preis.

Mit Hilfe von Algorithmen und künstlicher Intelligenz können die großen Datensammelunternehmen, aber gegebenenfalls auch der Staat, ein sehr genaues Profil jedes einzelnen Menschen erstellen.

Und wenn sie keine Daten über Sie haben, dann werden Sie statistisch in eine Gruppe eingeordnet. Sie mögen Lakritz und Heavy Metall? Dann fahren Sie bestimmt aggressiver Auto als der Durchschnitt? Sie tippen langsamer bei WhatsApp und machen viele Fotos von Landschaften? Ihnen kann man für Produkte bestimmt mehr Geld abverlangen als anderen Kunden!

Ich erwähne dass, damit Sie nicht mehr glauben, diese Datensammelei werde nur betrieben, um Ihnen zielgerichtet Anzeigen einzublenden.

Nein, angesichts der Verschränkung von digitaler und nicht-digitaler Welt hat diese Profilbildung Auswirkungen auf Ihr gesamtes Leben, auf Ihre Chancen und Möglichkeiten.

Wie fänden Sie es, wenn Ihre Autoversicherung die Prämie erhöht, weil Ihre Fahrzeug-, Handy- oder Fitness-Tracker oder Smartwatchdaten oder die Daten sie üblich begleitender Personen aussagen, dass sie risikofreudig fahren?

Hätten Sie auch kein Problem, wenn Sie bei einer Bewerbung trotz guter Zeugnisse nicht berücksichtigt werden, weil der vermeintliche neue Arbeitgeber anhand ihrer Profildaten bei einer Plattform oder einem beim Bewerbungsgespräch mitlauschendem KI-System davon ausgeht, dass Sie mit einer gewissen Wahrscheinlichkeit unter Depressionen leiden?

Oder das die vom vermeintlichen neuen Arbeitgeber eingesetzte Software zur Bewerbervorauswahl alle Frauen aussortiert hat, weil die Stellen bisher immer nur mit Männern besetzt waren (oder auch umgekehrt) und das System aus diesen Trainingsdaten falsche Rückschlüsse zieht und völlig unerwartete Optimierungsziele entwirft?

Haben Sie auch kein Problem, wenn Ihr Zahnarzt demnächst Ihre Krankenakten vom Psychotherapeuten oder dem Urologen einsehen kann, weil der scheidende Bundesgesundheitsminister den Schutz der Daten in der ersten Version der elektronischen Akte entgegen erster Ankündigungen und entgegen der technischen Realität nicht für alle Versicherten für realisierbar hält?

Und finden Sie es nicht besorgniserregend, wenn Unternehmen, Politiker und Staaten Sie mit gezielten Hinweisen, Nachrichten und Filtern manipulieren, weil sie wissen, auf was Sie wie reagieren? Wenn man Ihnen nach dem Mund redet und gleichzeitig verheimlicht, dass man Menschen mit entgegengesetzten Interessen gerade hofiert?

Wenn Sie beim Ausleben Ihrer Grundrechte wie Versammlungsfreiheit und Meinungsfreiheit und Freizeitverhalten präventiv erfasst und identifiziert werden?

Das alles sind keine gruseligen Zukunftsvisionen, damit beschäftigen wir Datenschützer uns tagtäglich. Diese Dinge passieren. Und wir wollen das stoppen. Das ist der Kern meiner Arbeit. Digitalisierung muss ohne Ausspioniert werden, ohne manipuliert werden, ohne übervorteilt werden, funktionieren. Und es gibt auch kein akzeptables Argument, dass das nicht möglich ist.

Wirklich entziehen können wir uns dieser digitalen Welt kaum. Auch völlige Abstinenz dürfte kein probates Mittel sein.

Denn: Auch wer keine Daten hinterlasst, erzeugt dadurch Daten über sich. Und vieles lernen die Systeme auch von anderen über Sie.

Außerdem gilt: Wer nicht digital mitspielt, wird bald gar nicht mehr mitspielen, verliert bisherige Teilhabemöglichkeiten, verbaut sich neue Potenziale und lässt andere entscheiden. Eine digitale Total-verweigerung wäre daher aus meiner Sicht der falsche Weg. Denn ein Rückzug aus digitalen Angeboten geht schlicht auch mit einer massiven Einschränkung der persönlichen Entfaltung einher.

III. Fortschreitende Digitalisierung

Die Digitalisierung schreitet massiv voran und sie ist nicht mehr zu stoppen – zum Glück, sagt auch der Informatiker in mir. Das war schon vor Corona so, aber durch die Pandemie sind viele schon geplante oder angedachte Schritte deutlich beschleunigt worden.

Was sich während all dieser Zeit gezeigt hat ist, dass die vielfältigen Folgen der Pandemie konsequent auch Fragen des Datenschutzes tangieren. Standen zunächst noch die Warn-Apps im Mittelpunkt der Aufmerksamkeit, rückten mehr und mehr arbeitsrechtliche Fragen und die Probleme in öffentlichen Einrichtungen wie in unseren Schulen und Kitas in den Mittelpunkt. An der rechtlichen Brisanz hat sich nichts geändert.

Die Pandemie-Krise hat unseren Alltag nachhaltig verändert. Klagen über die vielen Beschwernisse helfen uns aber nicht weiter. Wir sollten jetzt aus der Krise die richtigen und vor allem nachhaltigen Lehren ziehen.

Dabei müssen wir insbesondere die vielen gravierenden Versäumnisse ansprechen und beheben – und die sind nicht erst mit Corona entstanden. Dass die Digitalisierung in Betrieben, Verwaltungen sowie im Bildungs-und Gesundheitsbereich sträflich vernachlässigt wurde, hat sich mittlerweile herumgesprochen. Digitalisierung wurde viel zu lange als lästig und konfliktträchtig beiseitegeschoben und vernachlässigt. Dies alles rächt sich nun, in viel zu vielen Felder hinkt Deutschland hinter anderen Ländern und Regionen her und nutzt seine Möglichkeiten nicht.

Ich möchte an dieser Stelle aber nicht nur über frühere Versäumnisse sprechen. Noch wichtiger ist es mir, Mut und Zuversicht zu vermitteln. Ich bin fest davon überzeugt: Datenschutz wird Digitalisierung dazu bringen, den Schutz der Menschen und wirtschaftlichen Erfolg miteinander zu verbinden. Das wird dann gelingen, wenn Datenschutz von Anfang an mitgedacht wird, wenn er in gute Produkte übersetzt wird. Das ist wie mit dem Verhältnis von Ökonomie und Ökologie. Dann ist er kein Kostentreiber, kein Hemmschuh, sondern ein Innovationstreiber.

IV. Grundrechtsschutz in Krisenzeiten

Für Regierungen ist gerade in Krisenzeiten die Versuchung groß - natürlich stets zum Wohl der Menschen und der Lösung ihrer Probleme - mal eben deren Grundrechte zu kürzen, um wirkliche oder vermeintliche Lösungen auf eine ganz bestimmte Art zu entwickeln. Das entspringt alles dem alten Irrglauben, mit autoritären Mitteln Krisen schneller zu überwinden.

Die Pandemie ist zwar noch nicht vorbei. Aber nach mehr als 20 Monaten lässt sich doch eine erste Bilanz ziehen. Für mich steht dabei fest: **Auch in einer solchen Zeit macht es keinerlei Sinn und gibt es keine Berechtigung, am Grundgesetz vorbei Krisenmanagement zu betreiben.**

Alle Maßnahmen müssen stets auf ihre **Eignung** überprüft werden, etwa um Infektionen zu erfassen, infizierte Personen zu behandeln oder Neuinfektionen zu verhindern.

Die geplanten Maßnahmen müssen zudem auch **erforderlich** sein. Das heißt, besonders stark freiheitseinschränkende Maßnahmen müssen an besondere Voraussetzungen geknüpft werden. Und nach Ende der Krise müssen sie auch wieder zurückgenommen werden.

Das gilt ganz besonders für die hoch sensiblen **Gesundheitsdaten**. Ihre Verwendung birgt für die betroffenen Personen besondere Risiken. Arbeitgeber wollen natürlich gerne wissen, wie gesund – und das heißt wie belastbar – ihre Beschäftigten sind. Wenn der alte Spruch „Wissen ist Macht“ Gültigkeit hat, dann in der Hierarchie von Betriebsleitung und ihren Mitarbeiterinnen und Mitarbeitern. Die Datenschutz-Grundverordnung schützt daher aus gutem Grund diese sensiblen Daten in Art. 9 Abs. 1 DSGVO. Ich komme darauf noch einmal zurück.

Ich kenne natürlich auch all die immer wieder vorgebrachten Vorwürfe, der Datenschutz sei als einziges Grundrecht nicht beschränkt worden (Falsch!) oder habe zukunftsweisende Projekte zur Pandemiebekämpfung verhindert (Falsch!)

Ich kann es nur immer wieder wiederholen: **Aus datenschutzrechtlicher Sicht gab es bei der Prüfung der verschiedenen Maßnahmen zur Pandemiebekämpfung keine wirklich unlösbaren Probleme. Keine einzige geeignete und effektive Maßnahme zur Pandemiebekämpfung ist am Veto der Datenschutzaufsicht gescheitert!**

Im Gegenteil: Mehrfach haben wir rechtliche Regelungen für eine weitergehende Datennutzung sogar empfohlen (Cell Broadcasting, automatische Warnung CWA, 3G-Regelung am Arbeitsplatz, Check-In und Broadcasting CWA).

Dass trotzdem wider besseres Wissen der Datenschutz zum Sündenbock gemacht wird, ist leider nichts Neues. Gestern war Datenschutz Wirtschaftshemmnis, heute hindert er die Pandemie-bekämpfung, morgen wieder begünstigt er angeblich Kriminelle.

Manchmal ist es Unkenntnis, manchmal will man eine lästige Vorschrift beiseite schieben, um Dinge zu machen, die die europäischen Werte eben nicht erlauben. Und immer öfter sind es die Digitalisierungs-versager, die sich hinter der Ausrede Datenschutz zu verstecken versuchen. Bestes Beispiel zuletzt: der geschäftsführende Verkehrs-minister machte den Datenschutz dafür verantwortlich, dass es keine rechtzeitige Warnung für die Flutopfer gab, weil wir gegen den Versand von Warn-SMS, sog. Cell Broadcast, gewesen seien. Die Wahrheit: wir fordern genau dies schon seit über fünf Jahren aber die Bundes-regierung fand NINA-Warn-App sinnvoller und wollte Cell-Broadcast sogar europaweit abschaffen. Zum Glück wird es Cell-Broadcast jetzt doch bald wieder in Deutschland geben.

V. Arbeitsstruktur im Umbruch

Bei allen Behörden und private Unternehmen wandeln sich die internen Arbeits- und Kommunikationsformen rasant, das ist bei Ihnen sicher auch so wie in meinem Haus. Und wir sind froh, dass wir, anders als andere, die jetzt besonders laut schreien, die Voraussetzungen dafür schon vor der Pandemie geschaffen hatten.

Meine Referatsleiterinnen und Referatsleiter kommunizieren mit ihren Mitarbeiterinnen und Mitarbeiter via Telefon, Intranet und Video-konferenzen. Ich selbst verbringe einen guten Teil meiner Arbeit im Büro oder Homeoffice am Bildschirm. Das klappt alles recht gut. Meine Leute sind motiviert und auch kreativ, mit der Situation umzugehen. Die Technik funktioniert zunehmend reibungslos, vor allem die 2019 lücken-los eingeführte elektronische Akte, die verschlüsselte Kommunikation mit allen Partner:innen von Bürger:innen bis hin zu den Nachrichtendiensten und die 2021 eingeführten erweiterten digitalen Beschwerde- und Meldungsmöglichkeiten.

Die Krise hat somit fast überall Veränderungen des bisher bekannten Arbeitsalltags erzwungen. Ich bin mir sicher, dass diese Umwälzungen nachhaltig sein werden – und zwar überall. Meine ganz persönlichen Erfahrungen als Leiter einer unabhängigen Obersten Bundesbehörde decken sich an dieser Stelle mit denen in vielen andere Behörden und privaten Unternehmen.

Homeoffice beispielsweise ist kein Notnagel, der sich nach Corona wieder aus der Wand ziehen lässt. Ich bin mir sehr sicher, dass wir nach Ende der Pandemie nicht wieder zu den alten starren Arbeitsweisen zurückkehren werden. Nicht jede Besprechung von einer oder zwei Stunden muss mit tausenden Bahn- oder Flugkilometern und dem entsprechenden Zeitaufwand verbunden sein – einmal ganz abgesehen von den ökologischen Folgen des innerdeutschen Flugverkehrs. In unserem Haus haben wir schon jetzt die dauerhaften Möglichkeiten für Homeoffice dramatisch ausgeweitet.

An anderen Stelle wünsche ich mir aber doch ein Stück alter Normalität zurück. Ich möchte mit meinen Mitarbeiterinnen und Mitarbeitern endlich wieder mehr von Angesicht zu Angesicht sprechen. Der direkte persönliche Kontakt ist nicht ersetzbar. Das gilt gerade in schwierigen Gesprächssituationen, aber auch dann, wenn sich viele Teilnehmerinnen und Teilnehmer zu Wort melden.

Auch innerhalb meiner Teams steigt der Wunsch, wieder direkt miteinander zu reden, auch mal wieder gemeinsam einen Kaffee zu trinken und beim Mittagessen das eine oder andere abzuklären.

Das geht angesichts der stetig weiter steigenden Inzidenzwerte gerade wieder gar nicht, dafür kommen mit der 3G-Regelung für Arbeitsplätze und deren Überprüfung jetzt die Fragen zum **Beschäftigtendaten-schutz** auf.

Ich begrüße es ausdrücklich, dass die Arbeitgeber jetzt verpflichtet werden, die Einhaltung der 3G-Regel auch am Arbeitsplatz zu überprüfen, aber das hätte der Gesetzgeber früher, einfacher und datenschutzfreundlicher gestalten können. Nach meiner Auffassung wäre es in der Regel ausreichend, 3G-Daten der Beschäftigten für eine Zutrittskontrolle zu prüfen und diese dann nach Zutritt oder am Ende des jeweiligen Tages zu löschen. Auch ist für dieses Gesetz grundsätzlich keine längerfristige Speicherung der personenbezogenen 3G-Daten bei Arbeitgeberinnen und Arbeitgebern erforderlich ist. Für die Zutritts-kontrolle genügt ein ‚Abhaken' oder sogar eine Strichliste. Für die „regelmäßige Dokumentation", ob die Zutrittsvoraussetzungen ein-gehalten werden, reicht es aus, wenn Arbeitgeberinnen und Arbeitgeber nachprüfbare Prozesse etabliert haben, auf welche Weise täglich der 3G-Status der Beschäftigten geprüft wird. Die personengenaue Speicherung sensibler Gesundheitsdaten ist dafür nicht erforderlich.

- **Homeoffice: Datenschutz auch am heimischen Schreibtisch**

Lassen Sie mich zum Thema Homeoffice ein paar Anmerkungen machen, weil uns, wie schon angesprochen, das Arbeiten von zu Hause aus auch nach Ende der Pandemie erhalten bleibt.

Anders als beispielsweise die Warn-App oder Impfstatusabfragen ist Homeoffice für den Datenschutz kein neues Feld. Aber die plötzliche Ausweitung dieser Arbeitsform ist doch eine quantitative Veränderung mit ganz neuen Problemlagen auch für die Datenschutzaufsicht.

Klar ist, dass Unternehmen und Behörden weiterhin an die Vorgaben der Datenschutz-Grundverordnung gebunden sind. Homeoffice ist kein Ablass für Nachlässigkeiten beim Umgang mit personenbezogenen Daten.

Vielmehr gilt der Grundsatz: Auch zu Hause muss ich grundsätzlich in der Lage sein, das gleiche Level an Datenschutz und IT-Sicherheit zu gewährleisten wie im Büro.

Es gilt unter allen Umständen, dem Datenmissbrauch durch Dritte vorzubeugen. Diese Vorsicht liegt letztlich auch im Interesse der Betriebe selbst. Schließlich besteht auch immer die Gefahr von Betriebsspionage durch Nachrichtendienste und Konkurrenten. Da war auch schon vor Corona manche Firmen-IT offen wie ein Scheunentor beim Einbringen der Ernte.

Zum Schutz der personenbezogenen Taten der Beschäftigten und der betrieblichen Datensicherheit sind eine Reihe technischer und organisatorischer Maßnahmen in jedem Fall unverzichtbar.

Es gilt hier der bewährte Grundsatz, dass je sensibler die schutz-würdigen personenbezogenen Daten sind, desto wirkungsvoller müssen die erforderlichen technischen und organisatorischen Maßnahmen sein.

Nach der DSGVO sind besonders schutzwürdig:

- die Beschäftigtendaten,
- Sozialdaten nach § 67 Sozialgesetzbuch X (SGB X),
- Angaben nach Art. 9 DS-GVO (Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit oder Daten zum oder der sexuellen Orientierung einer natürlichen Person),
- genetische Daten und Gesundheitsdaten sowie biometrische Daten und zur eindeutigen Identifizierung einer natürlichen Person.

Ich rate den Geschäftsführungen und Behördenleitungen dringend, für die Arbeit im Home-Office eindeutige und transparente Regeln aufzustellen.

Die Vereinbarungen müssen die Rechte und Pflichten beider Seiten beschreiben. Ich kann auch nur dringend empfehlen, hier den Sachverstand der betrieblichen und behördlichen Datenschutzbeauftragten sowie der Betriebs- und Personalräte einzubinden.

VI. Datenschutz und die internationale Machtfrage

Die DSGVO hat national, in Europa und weltweit viel bewegt. Die Begrenzung der Macht der dominierenden US-Technologie-Konzerne ist und bleibt wohl noch lange die unbewältigte Herausforderung. Sogar die viel besprochene und beispielgebende Corona-Warn-App ist technisch von den Smartphone-Systemen von Apple und Google abhängig.

In der Pandemie-Krise ist die Macht dieser US-Riesen immer weiter gestiegen. Die DSGVO sollte hier eigentlich einen Werkzeugkasten für die Aufsichtsbehörden liefern, um das datenschutzrechtliche Selbstbestimmungsrecht der Menschen vor dieser Macht zu schützen.

Alle europäischen Aufsichtsbehörden müssen daher endlich das in der DSGVO geregelte Verfahren der Zusammenarbeit im Europäischen Datenschutzausschuss besser nutzen. Das bestehende Verfahren muss auch bei den großen, grundsätzlichen und grenzüberschreitenden Verfahren mit Leben gefüllt werden. Es wird ganz entscheidend darauf ankommen, dass die Datenschutzbehörden der EU-Mitgliedsstaaten die Möglichkeiten der DSGVO tatsächlich nutzen.

Es ist von daher mehr als ärgerlich, dass in Europa erst über **eine(!)** der datenschutzrechtlich problematischen Verhaltensweisen der großen internationalen Datenkonzerne entschieden werden konnte. Das liegt daran, dass die federführenden Aufsichtsbehörden aus Irland und auch Luxemburg schlichtweg zu langsam agieren können/sollen/wollen.

Gelingt es nicht bald, die bereits seit fast mehr als drei Jahren anhängigen Verfahren gegen Facebook, Amazon und Co auf dortiger nationaler Ebene und sodann im Rahmen der EDSA-Beratungen abzuschließen, können wir Reputation und Akzeptanz des gesamten Regelwerks weitgehend abschreiben. Die DSGVO schafft den Rechtsrahmen.

Der muss aber auch durch konkretes Handeln durchgesetzt werden. Wir deutsche Aufsichtsbehörden werden den Druck in den europäischen Gremien dafür hochhalten.

Gerade bei der Umsetzung des europäischen Datenschutzrechts muss sich vieles verändern. Um hier überhaupt Grenzen setzen zu können, wird übrigens auch die Zusammenarbeit von Wettbewerbsschutz und Datenschutz immer wichtiger werden.

Wir sehen in den USA, dass auch dort das Geschäftsgebaren der Technologiekonzerne auf immer mehr Widerstand stößt, nicht zuletzt im Kongress. Auch hier spielen wettbewerbsrechtliche Argumente eine entscheidende Rolle.

Erfreulicherweise arbeiten meine Behörde und das Bundeskartellamt daher auch immer öfter eng zusammen. Eins sollte jedem klar sein: Bekommt Europa die Datenriesen und ihre Geschäftsmodelle nicht in den Griff, wird nicht nur die DSGVO scheitern, sondern Deutschland und Europa werden wirtschaftlich weiter zurückfallen.

Hier sind Regierungen, Parlamente und Aufsichtsbehörden gefordert, den Schutz der Bürgerinnen und Bürger vor der Übermacht der Datenkraken wirksam zu schützen. Zusätzlich entsteht dann auch mehr Raum für europäische IT-Lösungen. Eine Win-Win-Situation. Die Rechtsetzungsakte der Europäischen Kommission zu Digitalen Diensten und KI, aber auch viele Vorhaben aus dem neuen Koalitionsvertrag bieten dafür viele Chancen.

Die Arbeit von Staat und Aufsichtsbehörden allein wird aber nicht ausreichen. Auch die Wirtschaft ist gefordert, die internationale Herausforderung anzunehmen. Ich sehe gerade jetzt in der Krise die große Chance für die Wirtschaft, endlich mit datenschutzfreundlichen Lösungen zu punkten. Wir werden einen Markt haben, an dem Anbieter ein echtes Gewicht in die Waagschale werfen können.

Diskussionen und Verbraucherumfragen zur Corona-Warn-App, zu vernetzten Fahrzeugen oder ganz aktuell dem Digitalen Euro zeigen: Datenschutz ist für Bürgerinnen und Bürger ein äußerst wichtiges Entscheidungskriterium, wenn man ihnen echte Wahlfreiheit gibt oder verschafft. Datensparsame Konzepte tragen übrigens zur besseren Effektivität und Effizienz des jeweiligen Datenverarbeitungssystems bei.

Der Markt hat aber noch immer zu wenig im Angebot, um die riesige Nachfrage zu befriedigen. Dabei kann die Wirtschaft mit daten-schutzfreundlichen Lösungen auf den nationalen-, europäischen und weltweiten Märkten punkten. Die Menschen werden nur digitalen Systemen vertrauen, die sie nicht ausspähen und in deren Folge keinerlei Nachteile oder Repressalien zu erwarten sind. Transparenz und ein wahrnehmbarer datenschutzrechtlicher Einfluss sind zwingend notwendige Voraussetzungen für die Unterstützung der Bevölkerung.

VII. Internationaler Datentransfer

Datenübermittlungen machen nicht an Grenzen halt. Auch nicht an den EU-Außengrenzen. Das erfahren wir jeden Tag im Privaten oder auch im Arbeitsleben. Denn der Datentransfer in andere Länder oder zumindest in den Geltungsbereich ausländischen Rechts gehört mittlerweile zu unserem Alltag. Auch wenn wir es nicht auf den ersten Blick sehen, so findet dieser dennoch täglich statt.

Sei es das Nutzen von Social Media Profilen oder Seiten, das Speichern von Fotos in der Cloud oder die Nutzung von Emaildiensten und Office-Anwendungen. Auch die Bestellung in einem großen Webshop ist oft mit einem Datentransfer über die Grenzen hinaus verbunden. Unsere Daten werden heute nicht mehr lokal erhoben, gespeichert, verarbeitet und genutzt, sondern global.

Deshalb **kann und darf aber auch der Datenschutz nicht an den Grenzen enden**. Mit der DSGVO wurde ein Regelwerk geschaffen, das diesen Schutz innerhalb der Europäischen Union und dem Europäischen Wirtschaftsraum gewährleistet, aber auch – durch Aufnahme des sog. Marktortprinzips - darüber hinaus wirkt.

Datenschutz kann sich aber eben nicht nur auf einzelne Länder oder eine Staatengemeinschaft beschränken, sondern muss **ein globales Anliegen** sein. Gerade deshalb ist es wichtig, dass wir über den Tellerrand schauen und uns regelmäßig national und international mit Kolleginnen und Kolleginnen austauschen.

Wie ich schon sagte, es ist wichtig, dass wir innerhalb Europas und auch darüber hinaus daran arbeiten, dass es **ein einheitliches Verständnis des Grundrechtsschutzes und damit auch des Datenschutzes** geben muss.

Dass die DSGVO wirkt und ein gutes und wirksames Regelwerk ist, zeigen uns die internationalen Entwicklungen wie in Japan, Südkorea und Brasilien, wo neue Datenschutzgesetze verabschiedet wurden, deren Vorbild die DSGVO ist.

Nicht zuletzt das **Schrems II Urteil** des EuGH von vor gut einem Jahr hat im Hinblick auf den internationalen Datentransfer einen wahren Paukenschlag gelandet.

Das Urteil sendet an uns alle, und damit meine ich nicht nur die Aufsichtsbehörden, sondern in erster Linie auch die Unternehmen, eine klare Botschaft:

Es kann kein angemessenes Datenschutzniveau in einem Drittland existieren, wenn umfangreiche Zugriffsrechte der Sicherheitsbehörden nicht durch angemessene Schutzmaßnahmen zum Schutz der Rechte von Betroffenen gesichert werden.

Das Urteil sagt aber auch, dass nicht per se alle Übermittlungen an Drittländer unzulässig oder unmöglich sind.

Vielmehr gibt es einen Rahmen vor, ob und inwieweit eine Datenübermittlung an Drittländer durch die geeigneten Garantien i. S. d. DSGVO und ggf. zusätzlicher geeigneter Maßnahmen (den sogenannten **Supplementary measures**) stattfinden kann. Das Urteil sagt auch, welche Umstände bei der Prüfung und Bewertung zu berücksichtigen sind.

Hier sei noch einmal daran erinnert, dass der EuGH selbst sehr deutlich gemacht hat, dass die Beurteilung einer datenschutzkonformen Übermittlung an Drittländer von den konkreten Umständen des Einzelfalls abhängig ist. Eine Lösung von der Stange im Umgang mit dem Urteil kann und wird der Europäische Datenschutzausschuss daher auch in Zukunft nicht liefern können.

Auf europäischer Ebene hat es sich der **Europäischen Datenschutzausschuss** – nicht nur nach dem Schrems II Urteil – zur Aufgabe gemacht, Möglichkeiten aufzuzeigen, wie eine datenschutzkonforme Datenübermittlung an Drittländer oder an internationale Organisationen im Sinne der DSGVO erfolgen kann. Daran arbeiten wir dort weiter intensiv.

Ich bin fest überzeugt, dass wir auch alle Kräfte bündeln sollten, mit den USA und anderen liberalen Demokratien einen gemeinsamen Datenraum zu schaffen, in dem Grundregeln für staatliche Zugriffe auf personenbezogene Daten gelten, die jeweiligen Datenschutzgesetze durchsetzbar sind und somit zum Nutzen aller ein freier Datenverkehr möglich wäre.

Das wäre übrigens auch eine Säule für den jetzt so oft beschworenen Systemwettbewerb mit China und anderen autoritären Systemen.

VIII. Zum Schluss

Dies war jetzt ein längerer Ritt durch verschiedene aktuelle Themen, die mich und mein Haus, ich denke aber auch Sie und die Bundesbank, derzeit beschäftigen. Ich hoffe, dass ich damit ausreichend Stoff für Nachfragen und Diskussion geliefert habe.

Ich möchte zum Schluss nur noch einmal meine drei wichtigsten Punkte hervorheben:

1. Wenn Datenschutz bei der Entwicklung und Umsetzung neuer Produkte von Anfang an mitgedacht wird, ist er nicht Bremser sondern Förderer.

2. Datenschutz ist der Schutz von Grundrechten der Bürgerinnen und Bürger, Ihrer Grundrechte. Dies hat das Bundesverfassungsgericht bereits 1972 festgestellt und es seitdem immer wieder bestätigt.

3. Wir Datenschützer schützen nicht Daten, sondern Menschen und Ideen. Auch der Schutz von Betriebsgeheimnissen und Patentschutz ist mit Datenschutzregeln leichter.

Ich danke Ihnen für Ihre Aufmerksamkeit.