Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

Prof. Ulrich Kelber

„Datenschutz in und nach der Pandemiebekämpfung“

23. Jahreskonferenz DuD 2021
Datenschutz und Datensicherheit

14.06.2021

Videorede

Es gilt das gesprochene Wort

Sehr geehrte Damen und Herren,

ich bin froh darüber, wieder **mit Ihnen** und hoffentlich nicht **nur zu Ihnen** zu sprechen. Wir alle hoffen darauf, dass im kommenden Jahr der 24. DuD-Kongress wieder in Präsenz stattfinden kann.

Ich weiß nicht, wie es Ihnen geht, aber ich freue mich wieder auf die persönliche Begegnung, das Come together in größerem Kreis und den kleinen Plausch am Rande. Den nutzen wir selbstverständlich ausschließlich nur für streng Dienstliches. Zum Schutz unserer persönlichen Daten unterlassen wir dabei selbstverständlich jedwede Lästereien über abwesende Kolleginnen oder Kollegen.

I. Einleitung

Das Ende der großen Pandemie-Krise zeichnet sich – hoffentlich – ab. Deren Spuren werden aber noch sehr lange sichtbar sein: ob in den Haushalten des Staates und der Unternehmen wie auch in allen persönlichen Bereichen.

Die vergangenen 15 Monate haben auf allen Ebenen vieles in Bewegung und manches auch ins Rutschen gebracht. Das Virus hat Schwachstellen und alte Versäumnisse schonungslos offen gelegt. Dass die Digitalisierung in Betrieben, Verwaltungen und im Bildungsbereich sträflich vernachlässigt wurde, bestreitet mittlerweile niemand mehr – jedenfalls nicht offen.

Der Wunsch, das alte Leben zurückzubekommen, ist gerade bei jungen Menschen nur zu verständlich. Aber das Verdrängen alter Fehler und die bequeme Restauration alter Verhältnisse wäre ein fauler Wechsel auf die Zukunft. Wir brauchen jetzt vielmehr eine Inventurliste der vielen gravierenden Versäumnisse. Die sind nämlich nicht erst mit Corona entstanden.

Es wäre grundfalsch, mit lautem **Hurra – das Virus ist weg** in frühere Denk- und Verhaltensmuster zurückfallen. Wir dürfen die Digitalisierung jetzt nicht wieder mal als zu aufwändig und konfliktträchtig vor uns herschieben.

Ich möchte aber noch einen Schritt weitergehen und die These aufstellen, dass der Datenschutz nach der Pandemie sogar gute Chancen auf eine Renaissance seiner öffentlichen Akzeptanz hat - sofern er den Schutz der Menschen und ihr wirtschaftliches Wohlergehen klug miteinander verknüpft. Datenschutz darf nicht als abstrakte Größe oder Nörgelveranstaltung erscheinen. Er muss vielmehr und ganz real in gute Produkte übersetzt werden.

Wie im Verhältnis zwischen Ökonomie und Ökologie.

Wer das Eine ohne das Andere angeht, wird letztlich beides gefährden.

1. Die Mär vom bösen Datenschutz

Digitalisierung und Datenschutz gehören zusammen. Wird aber aktuell ernsthaft darüber diskutiert,

- wie wir die technologischen Rückstände beispielsweise gegenüber dem totalitären China und den übermächtigen US-Internetkonzernen abbauen?
- wie es um den klugen Einsatz künstlicher Intelligenz bestellt ist?
- welchen Beitrag eine datenschutzfreundliche Digitalisierung zum Stopp der Erderwärmung leisten muss?

Ich jedenfalls nehme diese Zukunftsdiskussion - wenn überhaupt - allenfalls am Rande wahr.

Statt den verbesserten Schutz der Bürgerinnen und Bürger durch das neue europäische Recht gebührend zu würdigen, ist es Standardausrede für Denkfaule geworden, dem Datenschutz den Schwarzen Peter zuzuschieben. Natürlich soll er auch Schuld an den Pannen der Pandemie-Bekämpfung sein.

Je offenkundiger die Mängel beim Testen, Impfen, Öffnen und Schließen auf die öffentliche Stimmungslage durchschlagen, umso schriller werden die Töne. Niemand fühlt sich zuständig für die Kontrolle der Impfstellen. Die Gesundheitsämter können nicht und die Minister der Länder und des Bundes wollen nicht. **Woran liegt es angeblich? Natürlich am Datenschutz.**

Wer aber hat denn versäumt, einheitliche IT-Systeme in den Gesundheitsämtern einzuführen? Wer hat denn die Ämter so zu Tode gespart, dass sie nur zwischen Dienstag und Donnerstag brauchbare Daten liefern können? **Das war doch nicht der Datenschutz!**

Ich kann die E-Mails mittlerweile stapeln, in denen mir vorgeworfen wird, persönlich für die Corona-Tote verantwortlich zu sein und dass ich mich dafür eines Tages werde vor Gericht verantworten müssen.

Auf meine Frage, welche Maßnahmen denn konkret durch den Datenschutz behindert wurden, bekomme ich allerdings nie eine Antwort. Besonders ärgerlich ist, dass sich an der Verstärkung des Narrativs vom bösen Datenschutz angesehene Persönlichkeiten, Ministerpräsidenten und sogar versammelte Zeitungsredaktionen beteiligen. Sie wähnen sich im Mainstream, bedienen den mit Wonne und halten es deshalb auch nicht mehr für nötig, Fakten zu liefern. So wird die vermeintliche Gefühlslage der Nation bedient und mit unreflektiertem Halb- und Nichtwissen angereichert. Auf diese Weise verfestigen sich Vorurteile und Fehleinschätzungen.

Diese Art der Pseudo-Debatte beobachte ich immer häufiger und losgelöst von einem konkreten Diskussionsgegenstand. Sie ist anti-aufklärerisch und für die politische Kultur äußerst gefährlich - wie eine schleichende Vergiftung mit Schwermetallen.

Ganz im Sinne dieser Diskussionskultur wurde, durch eine leider nicht kleine Gruppe von Politikern, Wirtschaftsvertretern und sogar Wissenschaftlern, in die Welt hinausposaunt, dass der Datenschutz als einziges Grundrecht unangetastet fortbestehe, während wir sonst überall tiefgreifende Eingriffe in unsere Freiheitsrechte tolerieren müssten.

Das ist natürlich vollständiger Unsinn, denn wie andere Grundrechte auch, wurde auch der Datenschutz – und zwar zu Recht – zur Pandemiebekämpfung eingeschränkt. Denken wir nur an die Kontakterfassungen bei Reiserückkehrern oder in der Gastronomie und im Einzelhandel. Oder die Nachweise eines Gesundheitsstatus. Dennoch hält sich die Mär vom unantastbaren Datenschutz konstant in der Rhetorik Vieler, ungeachtet, wie oft ihnen das Gegenteil evident bewiesen wird.

2. Die Kampagne im Faktencheck

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!

Lassen Sie mich meine Position am Beispiel des sog. **elektronischen Impfausweises** erläutern: Es hat ja ein wenig gedauert, aber die Einführung läuft gerade auf Hochtouren.

Ob im Urlaub auf Lummerland, dem Liederabend mit Hape Kerkeling oder beim Italiener um die Ecke: Weiterhin gilt der alte analoge gelbe Impfpass. Schließlich haben nicht alle Smartphones und es soll auch kein Druck ausgeübt werden, sich eines anzuschaffen. Sinnvoll und richtig ist es selbstverständlich, dass Geimpfte künftig ihre Corona-Schutzimpfung auch digital nachweisen können. Kein Zweifel: Gerade Reisen in andere EU-Länder werden so einfacher. Das macht den Sommerurlaub unkomplizierter und entspannter.

Aber auch Veranstalter und Gastronomen sollen mit dem neuen Ausweis schnell und ohne großen Aufwand nachprüfen können, ob eine vollständige Impfung vorliegt und damit der Einlass möglich ist.

Der digitale Impfpass bleibt aber in jedem Fall ein freiwilliges und ergänzendes Angebot. Wer kein Smartphone besitzt oder den Nachweis nicht digital vorlegen möchte, kann auch weiterhin den gelben Papier-Impfpass nutzen.

Geplant ist, dass Arztpraxen, Impfzentren und Apotheken den digitalen Impfnachweis ausstellen. Sie erstellen nach Eingabe oder Übernahme der Impfdaten einen QR-Code, den die Geimpften direkt abscannen können oder auf einem Papierausdruck mitbekommen und später bei Bedarf einlesen können. Eine kostenlose App mit dem schönen altdeutschen Namen „CovPass“ und alternativ die aktualisierte Version der Corona-Warn-App speichert den digitalen Impfnachweis lokal auf dem Smartphone.

Bei Bedarf zeigen Verbraucher den QR-Code in der App, sodass Gastronomen, Fluggesellschaften und andere Dienstleister, die den Impfstatus überprüfen möchten, mit einer Prüf-App das Impfzertifikat auslesen können - ähnlich etwa wie bei einer digitalen Bahnfahrkarte.

Ich achte selbstverständlich während der Testphase und ihrer Auswertung sowie der anschließenden praktischen Umsetzung dieser Ergebnisse streng auf das Gebot der Datensparsamkeit. Je weniger Daten in den Umlauf kommen, umso reibungsloser klappt das Verfahren.

Das Gesundheitsministerium hat mir zugesagt, dass künftig alle digitalen Impfnachweise nur vorübergehend im Impfprotokollierungs-System erstellt und anschließend gelöscht werden. Dauerhaft sollen die eigenen Daten nur auf dem eigenen Smartphone gespeichert und mit einer Signatur fälschungssicher geschützt werden.

Sicher, das alles hätte schon früher vorbereitet sein sollen – spätestens mit dem Impfbeginn bei den Hausärztinnen und Hausärztinnen. Ich bin mir auch nicht sicher, ob neben den Vermerken „geimpft“ oder „genesen“ auch das höchst dynamische Testen auf dem gleichen Ausweis vermerkt sein muss. Je mehr Funktionen, umso komplizierter, störanfälliger und datenschutzrechtlich komplexer ist das dann. Der Drang zur bundesweiten zentralen Datenbank nimmt allzu schnell überhand.

Ich bin jedenfalls zuversichtlich, dass der Impfpass datenschutzrechtlich in Ordnung ist. Hier aber der Hinweis zur verspäteten Datenminimierung!

II. Grundrechtsschutz in der Bewährungsprobe

„Not kennt kein Gebot“, mit diesen Worten rechtfertigte Reichskanzler von Bethmann-Hollweg den verhängnisvollen Einmarsch der kaiserlichen Armee ins neutrale Belgien am Beginn des Ersten Weltkriegs. Bis heute nutzen Exekutiven Krisensituationen gerne als Lizenz zum Durchregieren, wenn auch weniger drastisch als 1914. Sie gefallen sich in der Flucht vor den Grundrechten der Bürgerinnen und Bürger als dem vermeintlichen Schlüssel für die Lösung der Probleme. Widerspruch, Einwände und Klagen werden dann schnell zum Sündenbock.

Eine derartige Beliebigkeit der öffentlichen Debatte beim Umgang mit den Gesundheitsdaten – ja mit dem Datenschutz insgesamt – dürfen wir nicht hinnehmen.

Die Pandemie ist noch nicht vorbei. Der Versuch einer allzu frühen Abschlussbilanz könnte sogar zu Fehlschlüssen verführen. Dennoch kann ich keinen sachlich plausiblen Grund finden, an Sinn und Bestand der Grundrechtsordnung unserer Verfassung auch in Krisenzeiten zu zweifeln. Das müssen wir auch öffentlich so kommunizieren.

Aus welchem Grund sollte beispielsweise der besondere Schutz unserer hoch sensiblen Gesundheitsdaten gelockert werden? Wenn wir jetzt anfangen, bei den Daten im Zusammenhang mit Corona zu schludern, sind morgen die Daten der Krankenkasse und übermorgen die genetischen Daten an der Reihe. Die unkontrollierte Verwendung all dieser vielen Informationen birgt für die betroffenen Personen besondere Risiken.

Nehmen wir ein Beispiel: Arbeitgeber wollen doch gerne wissen, wie gesund – und das heißt wie belastbar – ihre Beschäftigten sind.

Soll die Auszubildende übernommen werden? Lohnt es sich, in die Weiterbildung eines vielleicht schon älteren Beschäftigten zu investieren?

Die Datenschutz-Grundverordnung schützt in Artikel 9 aus gutem Grund diese sensiblen Daten. Ich habe keine Veranlassung, über eine Korrektur dieser europäischen Richtungsentscheidung nachzudenken.

1. Die DSGVO als wirkungsvoller Schutz – auch in der Pandemie

Ich bin froh darüber, dass wir mit der DSGVO bei all ihrer Unzulänglichkeiten ein wirkungsvolles Instrument haben, den Rechtsschutz europaweit zu vereinheitlichen und wirksamer zu kontrollieren.

Die DSGVO hat am 25. Mai dieses Jahres im Windschatten der öffentlichen Wahrnehmung ihren 5. Geburtstag gefeiert. Sie trat - anders als landläufig gedacht - nicht erst vor 3 Jahren, am 25. Mai 2018, in Kraft, sondern bereits 2 Jahre vorher.

In dem Zusammenhang eine Anmerkung: Ich kann nur hoffen, dass der Umgang einiger Unternehmen mit der Kundschaft nicht genau so zäh abläuft wie deren Umsetzung datenschutzrechtlicher Vorgaben.

Sonst müssen wir uns ernsthafte Sorgen um deren Konkurrenzfähigkeit machen. Die mühselige und schleppende Umsetzung datenschutz-rechtlicher Vorgaben wirft in meinen Augen auch ein Schlaglicht auf die verbreitete Rückständigkeit bei der Digitalisierung selbst.

2. Die Plage mit den Cookies

Ein weiterer Bereich: Seit dem Start der Datenschutz-Grundverordnung vor drei Jahren sind die sog. Cookie-Banner überall im Netz anzutreffen. Die datenschutzrechtliche Brisanz der Cookies wird öffentlich erheblich unterschätzt. Mit ihrer Hilfe können Nutzerprofile erstellt und so weitreichende Rückschlüsse über Surfverhalten, Vorlieben und Lebensgewohnheiten gezogen werden. Dieses Wissen wird etwa für personalisierte Werbung herangezogen. Es gibt eben keine per se harmlosen Daten. Die Cookies sind dafür ein gutes Beispiel. Die Menschen werden dadurch ausspioniert, über jedes erträgliche Maß hinaus und in einer Form, die analog nie akzeptiert würde.

Das europäische Zentrum für digitale Rechte - Noyb - von Max Schrems will dagegen vorgehen. Er hält diese Anfragen für manipulativ - und will mit einer Beschwerdewelle gegen rechtswidrige Cookie-Zustimmungsabfragen im Web vorgehen. Ich begrüße diese Initiative.

Der Verein verschickte rund 560 Beschwerdeschreiben an Unternehmen in Europa und den USA. Nach Einschätzung von Noyb hatten die Unternehmen mit Cookie-Bannern rechtswidrig eine Zustimmung zum Datentracking eingeholt.

Die europäische Datenschutz-Grundverordnung (DSGVO) gibt Anwenderinnen und Anwender eine klare Auswahl "Ja oder Nein" zu sagen. Dieses Recht darf nicht mit Tricksereien umgangen werden. In der Tat sind Cookie-Banner allgegenwärtig. Es ist nicht nur für Laien kompliziert, etwas anderes als den "Akzeptieren"-Knopf anzuklicken.

Noyb hat eine Software entwickelt, die verschiedene Arten von rechtswidrigen Cookie-Bannern erkennt und automatisch Beschwerden generieren kann. Nach dem Start mit rund 560 großen Websites - darunter auch die Angebote der US-Internetkonzerne Facebook, Google und Twitter - will der Verein bis zu 10.000 der meistbesuchten Websites in Europa unter die Lupe nehmen. Ein Bußgeld von bis zu 20 Millionen Euro könne dann verhängt werden.

Ich bin dankbar, dass sich Noyb an dieser Stelle klar von Abmahnvereinen distanziert und mit den Beschwerden kein Geld verdienen will. Es war gerade die Sorge vor diesen kommerziellen Abmahnkanzleien, die der Akzeptanz der DSGVO in der Öffentlichkeit immer sehr geschadet hat.

Ich bin sehr gespannt, wie sich die Dinge auch vor Gericht entwickeln. Da ist Max Schrems kein Unbekannter. Bekannt wurde er vor allem durch seine Auseinandersetzung mit Facebook. Vor dem Europäischen Gerichtshof konnte er erreichen, dass im Oktober 2015 die Vereinbarung "Safe Harbor" mit den USA verworfen wurde. Im vergangenen Juni brachte er vor dem EuGH auch die Nachfolgeregelung "Privacy Shield" zu Fall.

Wir sehen nicht zuletzt an diesen Beispiele, dass die Europäische Datenschutz-Grundverordnung im Interesse der Menschen nicht nur in Europa eine positive Wirkung hat.

Und noch einmal zu den Cookie-Bannern: An denen trägt nicht der Datenschutz Schuld, der Datenschutz verlangt gar keine Cookie-Banner. Und unklare Cookie-Banner braucht nur, wer Menschen ausspionieren will. Dem müssen wir ein Ende setzen.

III: Corona als Muntermacher der Digitalisierung

1. Die Arbeitswelt

Statt den Datenschutz zu beklagen, sollten sich manche Unternehmens- und Behördenleitungen vorhalten lassen, warum sie sich so lange gegen mobiles Arbeiten gewehrt und dabei die Digitalisierung ihrer Unternehmen vernachlässigt haben.

Homeoffice, Videokonferenzen und gemeinsames digitales Arbeiten wurden stärker denn je zu einer Notwendigkeit für viele von uns. Mittlerweile dämmert es vielen Arbeitgeber, dass man mit der neuen Art des Arbeitens besser klar kommt als gedacht.

Der BfDI hat bei der Umsetzung, der datenschutzkonformen Umsetzung übrigens, gar kein Problem gehabt. Weil wir uns schon vor der Pandemie um die entsprechenden Prozesse gekümmert haben.

Ich kann dieses Gejammer von Digitalisierungs-Versagern, man möge doch jetzt für mobiles Arbeiten auf Datenschutz verzichten, nicht mehr hören. Die haben früher ihren Job nicht gemacht und sind auch jetzt nicht auf der Höhe der Zeit.

Auch hier weist die Datenschutz-Grundverordnung den Weg in die richtige Richtung. Artikel 88 Abs.1 spricht hier von „*spezifischere (n) Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verbreitung personenbezogener Beschäftigtendaten im Beschäftigungskontext*“. Bewährte Verfahren zur Regelung des Beschäftigtendatenschutzes in Tarifverträgen und Betriebsvereinbarungen bleiben so bestehen.

Darüber hinaus kann der nationale Gesetzgeber auch noch „spezifischere Vorschriften“ erlassen. Alle Regelungen müssen aber die – zugegebenermaßen recht abstrakten – Vorgaben des Artikels 88 Abs. 2 DSGVO beachten.

Der Bundesgesetzgeber hat mit seinem § 26 BDSG eine solche nationale Regelung getroffen. Die wird aber nicht ausreichen. Ich sehe aber gerade beim Beschäftigtendatenschutz auch die Gefahr einer Wiederkehr nationaler Flickenteppiche. Sinnvoller wäre eine europäische Regelung des Arbeitnehmerdatenschutzes. Dann hätten Beschäftigte internationaler Unternehmen einheitliche Rechte, ob sie nun in Portugal, Lettland oder Deutschland tätig sind.

Dass die Entwicklungen der Digitalisierung und der KI im Bereich der Arbeitswelt weitreichende gesetzliche Anpassungen – auf welcher Ebene auch immer - erfordern, hat für das hier versammelte Fachpublikum gewiss keinen Neuigkeitswert.

Die pandemiebedingte weitere Verbreitung von mobiler Arbeit ist nur ein weiterer Punkt, der die Notwendigkeit weiterer Schritte unterstreicht. Er macht zum anderen klar, dass wir bei unseren Überlegungen auch zwingend die „neuen“ Arbeitsformen unserer Zeit jenseits der Tätigkeit im Betrieb oder der Behörde mitdenken müssen.

2. Der Datenschutz als Sauerteig der Digitalisierung

Welche Rolle spielt nun der Datenschutz in diesen Prozessen?

Er darf die Dinge nicht vom Rand her mit verschränkten Armen beklagen. Er muss vielmehr seinen ureigenen und energischen Beitrag leisten, die anstehenden technischen und rechtlichen Nachholprozesse in die richtige Richtung zu lenken. Gerade meine Kolleginnen und Kollegen in den hier zuständigen Ländern tun dies nach meinem Verständnis auch mit Nachdruck.

Allerdings können sich die Verantwortlichen, die nunmehr gezwungen sind, teilweise schnell neue Lösungen zur Behebung des Digitalisierungsdefizits zu präsentieren, nicht hinter der Pandemie verstecken.

Sie dürfen gerade nicht auf datenschutzrechtlich fragwürdige Produkte setzen, nur weil sie von weiten Teilen der Bevölkerung ohnehin schon genutzt werden.

Es gibt nicht nur alternative datenschutzfreundliche Angebote am Markt. Die Notwendigkeit, etwas Neues aufsetzen zu müssen, bietet gleichermaßen die Möglichkeit, essentielle Dinge wie **Privacy by Default und Design vom Start weg** mit zu implementieren.

Für den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen hat die DSGVO die Weichen gestellt. Die entsprechenden Anforderungen des Artikels 25 DSGVO sind zwar direkt verbindlich nur an die Verantwortlichen, nicht aber an die Entwicklung von Software und IT-Systemen gerichtet. Wenigstens spricht aber der Erwägungsgrund 78 auch diese Gruppe an. Ich hoffe, dass die betroffenen Unternehmen dennoch – auch im eigenen wirtschaftlichen Interesse – die Chancen datenschutzfreundlicher Produkte auf den Märkten dieser Welt erkennen und nutzen.

Richtig geplant und in der Praxis angewandt, kann der Datenschutz die technische Entwicklung voran bringen wie der Hefepilz den Kuchenteig.

Die Arbeit von Staat und Aufsichtsbehörden allein wird nicht ausreichen. Auch die Wirtschaft ist gefordert, die internationale Herausforderung anzunehmen.

Ich sehe gerade jetzt in der Krise auch 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 oder ganz aktuell dem Digitalen Impfpass zeigen:

Datenschutz ist für Bürgerinnen und Bürger ein äußerst wichtiges Entscheidungskriterium.

Datensparsame Konzepte tragen 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 datenschutzfreundlichen 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 Repressalien zu erwarten sind. Transparenz und ein wahrnehmbarer datenschutzrechtlicher Einfluss sind zwingend notwendige Voraussetzungen für die Unterstützung der Bevölkerung.

Die Datenschutzaufsichtsbehörden des Bundes und der Länder arbeiten fieberhaft daran, mit vielfältigen Hinweisen, fachlichen Anleitungen und Telefonberatungen den Behörden ihres Landes und den vielen privaten Unternehmen zu helfen.

IV. Neue Gesetze mit viel Schatten

Die Veranstalter haben mir die Frage vorgelegt, wie es auch nach Corona mit dem Datenschutz weitergeht. Statt falscher Schuldzuweisungen an den Datenschutz ist vielmehr dessen konstruktive Weiterentwicklung nötig. Der Gesetzgeber macht aber oft genug das Gegenteil.

1. Die Steuer-ID als Bürgerkennzeichen

So ist auf leisen Sohlen und leider weitgehend unbemerkt von der breiten Öffentlichkeit das hübsch bürokratisch klingende „Registermodernisierungsgesetz“ in Kraft getreten.

Das Gesetz sieht vor, die Steuer-ID als eindeutiges Personenkennzeichen in diversen öffentlichen Registern zu verwenden, um einen Austausch von Informationen aus diesen Einzelregistern zu ermöglichen.

Nicht wenige – mich eingeschlossen – haben allerdings erhebliche Bedenken, dass das Gesetz einer sicherlich anstehenden Überprüfung durch das Bundesverfassungsgericht standhalten wird. Dann wären Jahre verloren. Und das, obwohl es eine funktionsgleiche, datenschutzfreundlichere und verfassungskonforme Lösung gegeben hat.

Ich habe nach Kräften im Gesetzgebungsverfahren dafür gekämpft, dieses Schaufenster in Richtung gläserner Bürger und gläserne Bürgerin so gut es geht wieder zuzumauern oder wenigsten zu verhängen. Mit der Eingrenzung der Zweckbestimmung der Identifikationsnummer ist grundsätzlich eine wichtige Forderung erfüllt worden. So konnte wenigstens die unkontrollierte Ausbreitung dieses Instruments im Rahmen der öffentlichen Verwaltung verhindert werden.

Ich will aber meine Skepsis gar nicht verbergen. Trotz Einwilligungs-vorbehalts hab ich Zweifel, ob sich das Einsickern der Identifikationsnummer in alle Gesellschaftsbereiche gerade auch in die Privatwirtschaft verhindern lässt. Ich kenne aus meiner Datenschutz-aufsichtspraxis nur zu gut den rechtlich fragwürdigen Umgang mit Einwilligungen.

Ist aber die Identifikationsnummer erst einmal in der Wirtschaft als Hilfsmittel etabliert, ist der Damm gebrochen. Dann werden Datenlecks wie jüngst in Brasilien auch in Deutschland zum Alltag gehören. Dort waren die Steuernummern nahezu der gesamten arbeitenden Bevölkerung an die Öffentlichkeit geraten.

Einen gewissen Erfolg sehe ich in dem Ausbau des Datencockpits. Das ist ein durchaus wichtiger Schritt für die Transparenz. Das Instrument hat nach meinem Dafürhalten das Potential, die Bürgerinnen und Bürger endlich auf Augenhöhe mit dem Staat zu bringen. Der Zugriff auf die übermittelten Daten reicht allerdings nicht aus. Nötig ist der Zugriff auf die Bestandsdaten, so wie sie im jeweiligen Register liegen.

2. ePrivacy-Verordnung

Lange Zeit brütete der Rat der Europäischen Union über eine gemeinsame Position zum Schutz der Privatsphäre und der Vertraulichkeit digitaler Kommunikation. Das wollte und wollte nicht gelingen.

Eigentlich hätte die sog. ePrivacy-Verordnung Hand in Hand mit der DSGVO in Kraft treten sollen. Aber es kam anders. Und aktuell kommt es noch schlimmer.

Was der Rat nun am 10. Februar 2021 beschlossen hat, ist ein schlimmer Rückfall, noch vor den Richtlinien der 1990er Jahre. Der aktuelle Ratsentwurf macht Datenschutz zur Lachnummer. So soll beispielsweise die Vorratsdatenspeicherung mal wieder aus dem Papierkorb hervorgeholt werden.

Auch bei den Regelungen zum Internet geht es aus der Sicht des Datenschutzes im schnellen Galopp rückwärts. Beispielhaft sei an dieser Stelle nur die Zulassung der berüchtigten „Cookie Walls“ genannt.

So ganz nebenbei wurden wichtige Garantien für Nutzerinnen und Nutzer gestrichen. Das Widerspruchsrecht oder die Datenschutz-Folgenabschätzung landeten in der Ablage P wie Papierkorb.

Sogar der Rückgriff auf die Garantien der DSGVO wurde aus dem Text verbannt.

Bleibt es bei dieser Fassung der ePrivacy-Verordnung, könnten personenbezogene Daten ohne Einwilligung der Nutzenden auch relativ einfach zweckentfremdend weiterverarbeitet werden.

Das sind leider keine guten Nachrichten aus Brüssel.

V. Der Datenschutz als internationale Machtfrage

1. Die Macht der US-Konzerne

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 – und damit auch unser Demokratieverständnis – vor dieser Macht zu schützen.

Die DSGVO hat zwar national und weltweit viel bewegt. Die Macht der dominierenden US-Technologie-Konzerne ist und bleibt aber die unbewältigte Herausforderung für Wirtschaft und Datenschutz gleichermaßen. Sogar die viel besprochene und sehr gute Corona-Warn-App ist technisch von den Smartphone-Systemen von Apple und Google abhängig.

Alle europäischen Aufsichtsbehörden müssen 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 noch über keine der datenschutzrechtlich problematischen Verhaltensweisen der großen internationalen Datenkonzerne entschieden werden konnte. Das liegt daran, dass die federführenden Aufsichtsbehörden aus Irland und Luxemburg schlichtweg zu langsam agieren.

Gelingt es nicht bald, die bereits seit fast drei Jahren anhängigen Verfahren gegen Facebook, Amazon und Co auf nationaler Ebene und sodann im Rahmen der EDSA-Beratungen abzuschließen, können wir Reputation und Akzeptanz des gesamten Regelwerks in den Wind schießen. Die DSGVO schafft den Rechtsrahmen. Der muss aber auch durch konkretes Handeln durchgesetzt werden.

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.

Erfreulicherweise arbeiten meine Behörde und das Bundeskartellamt daher auch immer öfter eng zusammen. Ich bin Herrn Prof. Mundt sehr dankbar für seine Initiativen, die ihm der Deutsche Bundestag hier mit einer datenschutzfreundlichen Gesetzesregelung ermöglicht hat.

Erfreulich, dass auch in den USA die Macht der Technologiekonzerne auf immer mehr Widerstand stößt, nicht zuletzt im Kongress. Auch hier spielen wettbewerbsrechtliche Argumente eine entscheidende Rolle. Ich wünsche mir hier ein international abgestimmtes Vorgehen.

Bekommt Europa die Datenriesen und ihre Geschäftsmodelle nicht in den Griff, ist die DSGVO gescheitert und wir werden wirtschaftlich weiter zurückfallen. Hier sind Regierungen, Parlamente und Aufsichtsbehörden in der Verantwortung für einen wirksameren Schutz der Bürgerinnen und Bürger vor der Übermacht der Datenkraken.

Ich begrüße sehr, dass die EU-Kommission eine förmliche Untersuchung gegen Facebook wegen des Verdachts auf Wettbewerbsverstöße im Zusammenhang mit dem Kleinanzeigendienst „Facebook Marketplace“ einleitet. Die Meldung vom 4. Juni zeigt, dass die Kommission und die EU-Wettbewerbskommissarin Margrethe Vestager entschlossen ist, die Auseinandersetzung aufzunehmen.

VI. Schlussbemerkung

Das Grundrecht der informationellen Selbstbestimmung steht für die behördlichen Datenschutzbeauftragten in der Bundesrepublik und in Europa an keiner Stelle zur Disposition.

Die Bürgerinnen und Bürger müssen sich darauf verlassen können, dass ihre Freiheitsrechte nur so weit und so lange eingeschränkt werden, wie es zwingend erforderlich und angemessen ist, um die Gesundheit der Bevölkerung wirksam zu schützen.

Stehen wir zu dem Fortschritt, den wir der DSGVO verdanken. Ich erwähne beispielhaft die Bestimmungen zur „offensiven Transparenz“. Gerade diese eignen sich vorzüglich, Ängste zu nehmen und Vorurteile zu überwinden.

Die Sensibilisierung für datenschutzrechtliche Fragen ist eine wichtige Aufgabe nicht nur der Datenschutzaufsichtsbehörden, sondern auch all derer, die beim Datenschutz in der Verantwortung stehen.

Wirken wir gemeinsam selbstbewusst und entschlossen auf den europäischen und den nationalen Gesetzgeber ein, dass die Digitalisierung nie zum Selbstzweck verkommt. Jeder technische Fortschritt hat dem Menschen zu dienen. Er muss stets dem Rechtsstaat und der Demokratie verpflichtet bleiben.

Als Deutsche und als Europäer stehen wir für eine andere Digitalisierung als autoritäre Überwachungsregime in China oder Laissez-faire-Ansätze wie in den USA. Das gilt während der Pandemie und auch für die Zeit danach.

Wir in Europa kämpfen für eine Digitalisierung, die unsere Werte wiederspiegelt. Mit diesem Credo können wir in den wissenschaftlichen, technologischen, gesellschaftlichen und wirtschaftlichen Wettbewerb eintreten und die harte Auseinandersetzung der politischen Systeme bestehen.

Dazu müssen wir das europäische Datenschutzrecht konsequent anwenden, umsichtig weiterentwickeln und konsequent gegen die Angriffe seiner Gegner verteidigen.

Ich danke für Ihre Aufmerksamkeit.