Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz

und die Informationsfreiheit

Prof. Ulrich Kelber

Datenschutz in Zeiten der Infektionsbekämpfung

und weitere aktuelle Entwicklungen

14. Praxistage Datenschutz

Videobotschaft für den 17.02. 2021

Es gilt das gesprochene Wort

Sehr geehrte Damen und Herren,

ich danke Ihnen für die Einladung.

Auch wenn es bei dem heutigen Datum vielleicht durchaus stimmig wäre:

Mir geht es an diesem Aschermittwoch weder um eine Bußpredigt noch um einen datenschutzpolitischen Schlagabtausch, sondern schlicht um eine nüchterne Betrachtung und Einordnung des Datenschutzes in Zeiten von und teils nach Corona.

I. Einleitung

Dachten wohl die meisten von uns beim Schlagwort „**Virus“** bis vor einem Jahr eher an lästige Schadsoftware auf unseren Rechnern, ist der Begriff selbst für uns digitalaffine Datenschützerinnen und Datenschützer nun zu seiner ursprünglichen medizinischen Bedeutung zurückgekehrt und in seiner klassischen und damit analogen Form zum alltäglichen Begleiter geworden.

Ein unfreiwilliger und unheilvoller Begleiter, an dem es nichts zu verharmlosen, geschweige denn schön zu reden gibt:

Angesichts des Verlustes an Menschenleben, schwerer gesundheitlicher Folgen und tiefer Eingriffe in unser Sozial- und Wirtschaftsleben als unvermeidbare Notwendigkeiten im Kampf gegen die Pandemie erleben wir in der Nachkriegsgeschichte bisher beispiellose Eingriffe, auch und gerade in unsere Grundrechte.

Dies alles stellt den Rechtsstaat und unser gesamtes Gemeinwesen vor große Herausforderungen, gerade auch, was den gesellschaftlichen Zusammenhalt angeht. Bei aller unterschiedlicher Betroffenheit jedes Einzelnen von uns ist für das Fundament unseres Zusammenlebens wichtig, dass wir offen und ehrlich über Strategien zur Überwindung der Pandemie diskutieren; dem stellt sich auch der Datenschutz!

Die von uns allen geforderte Redlichkeit in der politischen Debatte gebietet dabei, den Diskurs gerade nicht den Corona-Leugnern, Verschwörungstheoretikern und Impfverweigerern zu überlassen, sondern Ihnen mit Fakten und gelebter Rechtsstaatlichkeit entgegenzutreten.

In diesem Kontext erfüllt auch der Datenschutz seine rechtsstaatliche Aufgabe und tritt den Beweis an, dass eine effektive Pandemiebekämpfung und ein effektiver Grundrechtsschutz keine Gegensätze sind.

Bei aller Frustration über diese Pandemie: Sie wird wie jede andere Pandemie in der Menschheitsgeschichte zuvor eines Tages enden!

Jeder von uns hat es in der Hand, seinen Beitrag dazu zu leisten, dass dieser Tag etwas schneller kommt! Jeder von uns hat es in der Hand, welchen langfristigen Kollateralschaden unser Gemeinwesen, gerade was seinen Zusammenhalt angeht, am Ende davonträgt.

Gleichzeitig sollten wir aber nach vorne schauen und uns jetzt Gedanken machen, wie es nach der Pandemie weitergeht.

II. Auswirkungen der Krise in unserem Alltag

Zweifelsohne: Noch ist Corona nicht vorbei

aber klar ist schon jetzt, dass sich trotz Rückkehr zur Normalität manches auch dauerhaft ändern wird und vielleicht auch ändern muss.

Eigentlich sollte es für jeden deutlich sein:

Die Erfahrungen und Veränderungen seit dem Frühjahr 2020 sind nicht nur einschneidend, sie sind auch nachhaltig.

Von daher erstaunt mich eine Umfrage des Instituts der deutschen Wirtschaft (IW) unter 1200 Firmen, die vor wenigen Tagen bekannt wurde:

Danach wollen zwei Drittel ihre Beschäftigten nach der Corona-Krise nicht mehr Homeoffice ermöglichen als vor der Krise. Das Gros der Mitarbeiter soll also wieder in die Büros zurückkehren, als wäre Nichts gewesen.

Die Bereitschaft zur Veränderung ist wohl doch schwächer, als die Einsicht, sich Neuem zu öffnen und aus Erfahrungen zu lernen.

Dabei steht nicht erst seit der Pandemie fest, dass Beschäftigte und ihre Interessenvertretungen sich mehr mobiles Arbeiten wünschen. Und dieser Wunsch ist in vielen Fällen erfüllbar. Außerdem wirkt sich gut gemachtes Homeoffice positiv auf das Betriebsleben aus.

Der zusätzliche Digitalisierungsschub durch die Pandemie lässt sich gewiss nicht mehr zurückdrehen - trotz aller Beharrungskräfte. Ohnehin wird die weiter fortschreitende Digitalisierung den Arbeitsalltag und so unsere Wirtschaft und Gesellschaft ungebremst weiter dauerhaft prägen.

- **Homeoffice**

Wie ist das aber mit dem Homeoffice aus Sicht des Datenschützers?

Klar ist: Das mobile Arbeiten wirft naturgemäß Fragen zur Überwachung Beschäftigter und zur Datensicherheit auf.

Ich appelliere daher zunächst ganz grundsätzlich an Arbeitgeber und betriebliche Datenschutzbeauftragte, gemeinsam mit den Betriebs- oder Personalräten genau aufzupassen, dass nicht alles pauschal Einzug

hält, was technisch möglich oder nicht auf den ersten Blick ausdrücklich verboten ist; da hilft schon eine Portion gesunder Menschenverstand.

Das gilt auch und gerade für den Einkauf und Einsatz von Software, mit der Arbeitgeber ihre Arbeitnehmer am Heimarbeitsplatz unmittelbar oder mittelbar überwachen und kontrollieren können.

Wie Sie wissen, liegt die Aufsicht über den nicht-öffentlichen Bereich weitgehend nicht beim Bund, sondern bei den Datenschutz-Aufsichtsbehörden der Länder. Dennoch hat der Bund bei der Gestaltung des Arbeitsrechts ebenso Verantwortung und wird von mir entsprechend beraten. Deshalb bin ich derzeit auch Mitglied im Beirat des BMAS zu Vorschlägen für den künftigen Beschäftigtendatenschutz.

Mit Blick auf meine Kolleginnen und Kollegen aus den Ländern kann ich nur darum bitten, deren Arbeit als Hilfe anzusehen und anzunehmen; sie ist gewiss keine ungebetene Einmischung in den betrieblichen Alltag!

Unsere neue Arbeitswelt sollte von einer „gesunden“ Mitarbeiter- und Führungskultur“ geprägt sein – und nicht durch Ausspionieren.

Die rechtlichen Vorgaben sind dabei ganz klar:

Das datenschutzrechtliche Schutzniveau für mobile Arbeit muss ohne Abstriche dem des Arbeitsplatzes im Betrieb entsprechen. Ein wirksames und bewährtes Instrument, um dieses zu gewährleisten, sind und bleiben hier Zielvereinbarungen im Betrieb, auch im Bereich des Homeoffice.

Denn schließlich auch im Homeoffice gilt, was das Bundesarbeitsgericht etwa in seiner Keylogger-Entscheidung vom 27. Juli 2017 – 2 AZR 681/16 –, BAGE 159, 380-394 festgehalten hat:

Eine anlasslose Überwachung – hier eben durch Keylogger – kann Beweisverwertungsverbote zur Folge haben.

Wegen des Digitalisierungsschubs in der Arbeitswelt nimmt gerade durch die Pandemie die Diskussion über einen effektiven Beschäftigtendatenschutz aktuell wieder an Fahrt auf. Der Gesetzgeber sollte künftige Entwicklungen der Digitalisierung und der KI jedenfalls regeln, bevor in der digitalen Arbeitswelt Beschäftigteninteressen unter die Räder kommen. Der gegenwärtige § 26 Bundesdatenschutzgesetz reicht jedenfalls so nicht aus.

- **Was macht der Datenschutz in der Krise und danach?**

In einer Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 03.04.2020 haben wir Aufsichtsbehörden wichtige Grundsätze festgehalten.

Sie gelten für den Bereich der Arbeit ebenso wie für andere Bereiche. Sie gelten auch für den Gesundheitsschutz, den ich noch im Einzelnen ansprechen werde.

Das Grundrecht der informationellen Selbstbestimmung steht dabei für uns an keiner Stelle zur Disposition; so ist auch der Rechtsrahmen:

Die DSGVO stellt insbesondere in Artikel 5 europaweit verbindlich einheitliche Grundsätze auf; sie sind ein guter Leitfaden, nicht nur in Krisenzeiten, sondern auch für die Zeit danach.

Diese Grundsätze blockieren keineswegs – und dies muss man leider angesichts einiger Talkshow- und Leitartikler-Legenden immer wieder wiederholen – eine effektive Bekämpfung der Corona-Pandemie. Sie gefährden auch nicht die wirtschaftliche Erholung nach deren Ende. Warum sollten wir diese Grundsätze auch aufgeben?

- **Feste Grundsätze des Datenschutzes**

Auch in Krisenzeiten hat eine Verarbeitung personenbezogener Daten stets auf einer **gesetzlichen Grundlage** zu erfolgen. Die verfolgten Zwecke müssen möglichst genau bezeichnet werden. Soll das weg?

- **Eignung**

Die geplanten Maßnahmen müssen in jedem Fall geeignet sein, etwa um beispielsweise Infektionen zu erfassen, infizierte Personen zu behandeln oder Neuinfektionen zu verhindern. So kann es beispielsweise in Notfalllagen eine geeignete Maßnahme sein, Hilfsorganisationen zu verpflichten, medizinisch ausgebildetes Personal an die für die zuständigen Gesundheitsbehörden zu melden.

Hingegen habe ich durchgreifende Zweifel an der Eignung von Maßnahmen, die allein mithilfe hierfür ungeeigneter Telekommunikationsverkehrsdaten individuelle Infektionswege nachvollziehen sollen.

Will man auf die Geeignetheit verzichten?

- **Erforderlichkeit der Maßnahmen**

Die geplanten Maßnahmen müssen zudem stets erforderlich sein. Stehen andere, ebenfalls geeignete Maßnahmen zur Zweckerreichung zur Verfügung, die weniger, oder - wie eine vorherige Anonymisierung - sogar gar nicht in die Rechte der Menschen eingreifen, müssen diese zunächst umgesetzt werden.

Was sollen auch nicht erforderliche Maßnahmen für einen Zweck haben?

- **Grundsatz der Verhältnismäßigkeit**

Nicht mehr für die benannten Zwecke benötigte personenbezogene Daten sind unverzüglich zu löschen.

Die Verarbeitung von speziell zur Pandemiebekämpfung erhobenen sensiblen Daten ist nach dem Ende der Krise also wieder zu beenden.

Generell sollten ohnehin alle pandemiespezifischen Maßnahmen befristet werden.

Ich würde gerne wenigstens einmal hören, warum diese Grundsätze angeblich behindern!?

III. Besonderer Schutz der Gesundheitsdaten

Gesundheitsdaten zählen zu den besonders sensiblen Daten, weil ihre Verwendung für die betroffenen Personen besondere Risiken nicht zuletzt in ihrem gesellschaftlichen Umfeld begründen können.

Darunter fallen all jene personenbezogenen Daten, die Rückschlüsse auf körperliche oder geistige Gesundheit zulassen.

Sie wissen selbst, dass manche Arbeitgeber nur zu gerne wissen wollen, wie gesund Beschäftigte sind, wenn sie sich um eine Stelle bewerben oder eine Beförderung ansteht. Das Wissen um genetische Dispositionen für eine Krebserkrankung oder eine HIV-Infektion hat auf den Fluren der Chefetage aber schlicht Nichts zu suchen.

Ein aktuelles Beispiel von H&M hat da wieder aufhorchen lassen. Gut, dass mein Kollege Prof. Caspar aus Hamburg hier eine Geldbuße in Höhe von 35,5 Millionen Euro durchsetzen konnte.

Die Datenschutz-Grundverordnung schützt aus gutem Grund diese sensiblen Daten ganz besonders in Art. 9 Abs. 1 DSGVO.

Sie verlangt geeignete Garantien zum Schutz der betroffenen Personen sowie technisch-organisatorische Maßnahmen zum Schutz der Integrität und Vertraulichkeit der Gesundheitsdaten. Nur so lassen sich Missbräuche verhindern und Fehler in der Verarbeitung vermeiden.

Großen Wert lege ich auch darauf, dass im Sinne des Grundsatzes der Transparenz betroffene Personen in verständlicher Weise über die Verarbeitung ihrer Daten informiert werden.

Sie sehen, meine Damen und Herren, Datenschutz-Grundsätze bieten auch in Krisenzeiten eine hinreichende Orientierung und eröffnen trotzdem Gestaltungsmöglichkeiten für eine rechtskonforme Verarbeitung personenbezogener Daten.

- **Die Gesetzgebungsverfahren**

Leider ist es zum Ritual in Talks-Shows geworden, den Datenschutz als Klotz am Bein der Pandemie-Bekämpfung zu verteufeln. Ministerpräsidenten, Minister, Philosophen, Chefredakteure und andere Nachplapperer. Je deutlicher die Versäumnisse bei der Pandemiebekämpfung öffentlich werden, umso mehr wird der Datenschutz zum Prügelknaben.

Wer aber hat denn die Gesundheitsämter kaputt gespart, Personal gekürzt und die technische Ausstattung sträflich vernachlässigt: **Doch nicht der Datenschutz!**

Was in der Gesetzgebung los ist, möchte ich Ihnen an der Flut der Pandemie-Gesetze erläutern. In dem Zusammenhang möchte ich auch ein paar Anmerkungen zu Corona-Warn-App machen.

- **Eine Flut an Gesetzen**

Die Anzahl der Gesetze und Verordnungen aus dem BMG wurde im Laufe der Pandemie endgültig rekordverdächtig. Diese Flut hält auch meine Mitarbeiterinnen und Mitarbeiter auf Trab, zunehmend jenseits der Belastungsgrenzen. Man darf ja nicht vergessen, dass mit jeder Gesetzesinitiative Beratungen, Prüfungen, Stellungnahmen und viele Zuschriften Betroffener verbunden sind.

Gleichzeitig wird oft unnötiger Zeitdruck erzeugt, weil nicht rechtzeitig Kontakt aufgenommen wird.

Ein Beispiel:

- Für die Befassung des Entwurfs zum (Ersten) „Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite“ gab es am Freitagnachmittag eine Vorwarnung. Möglicherweise komme in den nächsten Stunden der Gesetzentwurf vom Bundesgesundheitsministerium.

- Am Samstagmorgen, dem 21. März 2020, war es dann soweit. Der reichlich opulente Gesetzentwurf kam - mit einer Frist von vier (!) Stunden für eine Stellungnahme.

- Am folgenden Tag, einem Sonntag, wurde gegen 13.00 Uhr ein überarbeiteter Entwurf durch das Bundesgesundheitsministerium zu fachlichen Beratung versandt.

- Am Mittwoch darauf, am 25. März 2020, wurde das Gesetz vom Deutschen Bundestag beschlossen und der Bundesrat stimmte am 27. März 2020 zu, so dass das Gesetz am 28. März 2020 in Kraft treten konnte.

Die in der Gemeinsamen Geschäftsordnung der Bundesregierung hierfür vorgegebenen Fristen waren eine ferne Erinnerung an frühere Zeiten.

Da waren es noch bei einfachen Gesetzen **vier Wochen** und bei komplizierten oder sehr umfangreichen Gesetzentwürfen **acht Wochen**. Davon blieben gerade mal **vier Stunden** übrig**!**

Unter solchen Bedingungen verkümmert Beteiligung zu einem formalen Ritual, das man ohne Federlesen abwickeln will. Die gesamte Zeit, in der der Entwurf erarbeitet wurde, hat man für die datenschutzrechtliche Begleitung durch Nichtbeteiligung einfach vergeudet.

Trotz dieser äußerst schwierigen Bedingungen haben wir uns im Interesse der Sache dieser Herausforderung gestellt und im Rahmen des Möglichen auch bewältigt. Klar aber auch, dass eine sorgfältige Prüfung anders aussieht.

Nachdem bereits im Januar 2020 die Meldepflicht für Erkrankungen und Krankheitserreger nach dem Infektionsschutzgesetz durch Verordnung auf CoViD-19 und SARS-CoV-2 ausgedehnt worden war, wurde das Infektionsschutzgesetz im März, April und November in drei „Etappen“ geändert.

Neben weitreichenden Eingriffs- und Verordnungsbefugnissen für das BMG sah dieses „**Erste Pandemiegesetz“** Pflichten für Beförderungsunternehmer und Fluggesellschaften vor, wobei ich erhebliche Zweifel an der Verfassungsmäßigkeit geltend gemacht habe, insbesondere hinsichtlich der Geeignetheit der Maßnahmen. Leider wurden meine Bedenken überwiegend nicht berücksichtigt. Weder die erforderliche Nachbesserung der Begründung oder die von mir geforderte Evaluation, noch die nötigen Löschvorgaben oder die zielführende datenschutzrechtliche Begleitung landesübergreifender Forschungsvorhaben zentral durch mich wurden vorgesehen.

Geändert wurde auch das Gesetz zur Durchführung der Internationalen Gesundheitsvorschriften. Die nunmehr vorgesehenen Abfragen beim Fluggastdaten-Informationssystem verstoßen gegen die EU-Richtlinie über PNR-Daten.

Ohne „Vorwarnung“ wurde der Entwurf des „**Zweiten Gesetzes zum Schutz der Bevölkerung** bei einer epidemischen Lage von nationaler Tragweite“ am Nachmittag des 20. April 2020 vom Bundesgesundheitsministerium mit der Bitte um Stellungnahme bis zum 22. April 2020 versandt – immerhin statt vier Stunden nunmehr zwei Tage Frist zur Stellungnahme.

Auch in diesem Gesetzentwurf waren weitgehende Veränderungen des Infektionsschutzgesetzes enthalten. Nicht alle waren eilbedürftig: Ohne Bezug zur aktuellen Lage wurde die namentliche Meldepflicht bei neuen, bislang unbekannten Erkrankungen bereits auf den Verdachtsfall ausgeweitet.

Konkret auf alle Corona-Viren bezogen wurde eine Meldepflicht bei negativem Testergebnis an das Robert Koch-Institut (RKI) eingeführt. Die Begründung dafür enthielt jedoch ausschließlich statistische Erwägungen. Dass die Meldungen an das RKI pseudonymisiert abgegeben werden sollten und daher die Vorgaben der DSGVO einzuhalten waren, wurde im Gesetz und seiner Begründung nicht berücksichtigt.

Das Infektionsschutzgesetz dient der Gefahrenabwehr, konkret dem Schutz vor Ansteckung mit einer infektiösen Krankheit. Die Negativ-Getesteten sind jedoch nicht ansteckend. Ich hielt die Meldungen in dieser Form daher für nicht erforderlich und damit für unzulässig. Leider blieb die Regelung dennoch zunächst im Gesetz.

Immerhin konnte ich erreichen, dass eine vorgesehene Regelung zu einem Immunitätspass zurückgezogen wurde: Ein Immunitätspass würde eine gesundheitsbezogene Angabe enthalten, die ärztliche Bewertung der Immunität. Damit würde er sich wesentlich vom Impfpass unterscheiden, der die Tatsache der Impfung dokumentiert. Für den Impfpass gilt, dass nur in bestimmten Fällen eine Einsicht verlangt werden darf. Da im April die Immunität bezüglich SARS-CoV-2 wissenschaftlich noch nicht geklärt war (ist sie das eigentlich heute?), wurde die Regelung wieder zurückgezogen. In meinen Augen wäre es mit dem Recht auf informationelle Selbstbestimmung nicht zu vereinbaren, sollte ein Immunitätsnachweis allgemein als „Eintrittskarte“ eingesetzt werden. Das würde umgekehrt zu einer Diskriminierung derjenigen führen, die einen derartigen Nachweis nicht erbringen können. Das Zweite Pandemiegesetz trat am 23. Mai 2020 in Kraft.

Der gesamte Ablauf dieses Gesetzgebungsvorhabens zeigte, dass die pandemische Lage auch bei der Regierung große Unsicherheit ausgelöste. Es fehlten belastbare wissenschaftliche Erkenntnisse zu Infektionswegen und -gefahren, zur Erkrankungswahrscheinlichkeit und Wiederansteckungsgefahr und zu zielführender medikamentöser Behandlung.

Je geringer das Wissen im Detail, umso höher die Versuchung flächendeckender Beschränkungen. Das Rezept gegen die eigene Unsicherheit war dann die umfassende und gesetzlich verpflichtende bundesweite Erhebung personenbezogener Gesundheitsdaten.

Das **„Dritte Gesetz** zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Bedeutung“ wurde am Abend des 14. Oktober 2020 mit Frist zur Stellungnahme bis zum 16. Oktober 2020 vorgelegt.

Erneut wurden verschiedene Meldepflichten und Übermittlungen personenbezogener Daten eingeführt oder erweitert. So wurde eine Verfeinerung der Angaben zum Wohnort der Infizierten vorgesehen. Übersehen wurde dabei, dass dadurch das Re-Identifikationsrisiko steigt.

Denn diese Regelung gilt nicht nur für CoViD-19, sondern auch für andere, wesentlich seltenere Erreger.

Zudem sollten ohne ausreichende Begründung pseudonyme Meldungen zur Impfung und zu Impffolgen nun an zwei verschiedene Stellen gehen. Einmal an das Robert Koch-Institut und zusätzlich noch das Paul-Ehrlich-Institut. Beides sind zwar Bundesoberbehörden im Geschäftsbereich des Bundesgesundheitsministeriums, aber es sind unterschiedliche Behörden. Die Verdoppelung der Datenmenge sehe ich datenschutzrechtlich sehr kritisch.

Problematisch waren auch im Dritten Pandemieschutzgesetz wieder die Regelungen über die Pflichten und Befugnisse von Beförderungsunternehmen und Bundespolizei bei der Einreise. Durch Verordnung kann vorgesehen werden, dass den Beförderern Nachweise über Meldepflichten, Impfungen und Gesundheitszustand vorzulegen sind. Die müssten dann ihrerseits Daten der Passagiere übermitteln. Die Bundespolizei soll die Erfüllung der Pflichten aus der Verordnung überwachen und Verstöße melden.

Die Grundrechtseingriffe wurden nicht ausreichend abgewogen und gerechtfertigt. Insbesondere **Geeignetheit** und **Erforderlichkeit** der Maßnahmen werden nicht dargelegt. Im Kontext der EU bedarf eine Unterscheidung zwischen grenzüberschreitenden und innerdeutschen Reisen einer besonderen Begründung. Die nach Artikel 9 Absatz 2 DSGVO für die Verarbeitung von Gesundheitsdaten notwendigen besonderen Schutzmaßnahmen werden nicht erwähnt.

Weitere Vorgaben für die Beförderer fehlen. Dabei ist für diese privaten Unternehmen zu regeln, ob und wie sie die Daten erheben und wie lange, in welchem Umfang und mit welchen Schutzvorkehrungen sie sie speichern dürfen.

Als Erfolg konnte ich wenigstens verbuchen, dass die Meldepflicht der Negativ-Getesteten wieder gestrichen wurde, bevor mit ihrer Umsetzung begonnen wurde.

Das Dritte Pandemiegesetz wurde am 28. Oktober 2020 durch das Bundeskabinett gebilligt und in den Deutschen Bundestag zur Beratung eingebracht. Am 9. November 2020 wurden 17 Seiten Änderungsanträge, am 12. November 27 Seiten Änderungsanträge und

am 13. November nochmals 29 Seiten Änderungsanträge vom Bundesgesundheitsministerium als Formulierungsvorschläge von Abgeordneten in den Gesundheitsausschuss eingebracht.

Sie sehen an dieser Abfolge, mit welcher Hektik in der Krise Gesetze gemacht werden. Sie sehen aber auch: schnelles Recht ist nicht immer auch gutes Recht.

- **Die Corona-Warn-App**

Ich habe dieses Projekt von Beginn an beratend begleitet. Ich nehme zudem auch die Datenschutzaufsicht über das Projekt des Robert Koch-Institut wahr.

Als die Corona-Warn-App (CWA) der Bundesregierung am 16. Juni 2020, nach etwas mehr als zwei Monaten Entwicklungszeit, durch das Robert Koch-Institut (RKI) veröffentlicht wurde, war das Medieninteresse war von Anfang an riesig.

Der Hype machte fast den Eindruck, mit der App in der Hand könne die Bundesregierung im Alleingang das Coronavirus besiegen. Das lag auch an Berichten über App-Lösungen in Japan, China, Taiwan und vor allem

Südkorea. In den Medien wurde dabei häufig übersehen, dass auch in diesen Ländern die App-Lösungen eingebunden waren in weitere Maßnahmen zur Eindämmung der Pandemie durch gut ausgestattete Gesundheitsbehörden, wie etwa das disziplinierte Tragen des Mundschutzes, effiziente Quarantänemaßnahmen und das „Social Distancing“.

Insbesondere in Südkorea wird eine Tracking-App eingesetzt, die per GPS und anderen Daten Bewegungsprofile der Nutzer erstellt und an die Behörden übermittelt. Die Gesundheitsbehörden sollen daraus schließen können, so wird oft behauptet, wer sich mit wem wann und wo getroffen hat.

Der Netzaktivist Markus Beckedahl bringt es auf den Punkt, wenn er von der Tracking-App Südkoreas als "Talkshow-Mythos" spricht. Er weist darauf hin, dass die App in Südkorea vor allem zu Kontrolle der Quarantänebestimmungen eingesetzt wird. Es geht weniger darum, Infektionsketten nachzuverfolgen und zu unterbrechen. GPS-Daten können nämlich auch nicht aussagen, ob sie vor oder im Gebäude waren, in der Tiefgarage oder im obersten Stockwerk.

Das Gerede über „Lebensschutz statt Datenschutz“ soll allzu oft nur von eigenen Versäumnissen ablenken, etwa bei der Digitalisierung von Gesundheitsämtern.

Als Contact-Tracing-App ermöglicht die Corona-Warn-App der Bundesregierung die datenschutzfreundliche Erfassung von möglicherweise infektionsrelevanten Begegnungen zwischen Nutzerinnen und Nutzern der App unter Verwendung des Bluetooth-Standards. Bei einem positiven COVID-19-Testbefund können Nutzerinnen und Nutzer ihre Kontakte über die Corona-Warn-App schnell warnen, ohne dabei ihre Identität offenlegen zu müssen. Die so gewarnten Kontaktpersonen haben dann die Möglichkeit, sich an Ärzte und Gesundheitsämter zu wenden und sich selbst testen zu lassen. Durch ihr umsichtiges Verhalten leisten die gewarnten Kontaktpersonen einen effektiven Beitrag zur Vermeidung weiterer Infektionen. Über 250.000 Mal ist das bisher passiert.

Um effektiv zu sein, ist die Corona-Warn-App darauf angewiesen, dass sie von möglichst vielen Bürgerinnen und Bürgern genutzt wird. Datenschutz ist auch hier ein wesentlicher Faktor für die Akzeptanz. Sie wurde mit Stand vom 5. Februar 2021 insgesamt 25.4 Millionen Mal

heruntergeladen; 11.4. Millionen aus dem Apple- App-Store und 14 Millionen bei Google Play Store.

Aufgrund der datenschutzfreundlichen Ausgestaltung ist die Corona-Warn-App in der Bevölkerung weitgehend akzeptiert. Das französische Pendant mit seinem weniger datenschutzfreundlichen Ansatz einer zentralen Datenverarbeitung gilt mit gerade einmal rund 2 Millionen Downloads als gescheitert.

Bereits zum Start der Corona-Warn-App war klar, dass mangels der hierfür erforderlichen technischen Ausstattung bei weitem nicht alle beteiligten Labore ihre Testergebnisse für die Nutzerinnen und Nutzer der App bereitstellen können. Dies führt zu einem Datenschutzrisiko. So konnten nicht alle Nutzerinnen und Nutzer der App, deren Tests von diesen Laboren ausgewertet wurden, den datenschutzfreundlichen Workflow zur Bereitstellung der Ergebnisse in der CWA nutzen und ihre Kontakte schnell warnen

Stattdessen musste für diese Fälle ein alternativer Prozess unter Verwendung sogenannter „Tele-TANs“ etabliert werden. Um diese Tele-TAN zu erhalten, müssen sich die positiv getesteten Nutzerinnen und

Nutzer an eine Freischalt-Hotline wenden, was zu einem unerwünschten Medienbruch führt. Bei der Hotline werden nämlich kurzzeitig personenbezogene Daten vorgehalten, die eine Identifikation der Anruferinnen und Anrufer ermöglichen.

Dem Robert Koch-Institut ist es gelungen, einige der festgestellten datenschutzrechtlichen Mängel bei der Corona-Warn-App zeitnah zu beheben.

Das Problem der fehlenden Laboranbindungen ist aber weiterhin nicht gelöst. Der aus Sicht des Datenschutzes problematische Medienbruch und aus Sicht der Pandemiebekämpfung langsame Meldeweg besteht weiter fort.

Den anfangs angesprochenen Kritikern an der Corona-Warn-App gestehe ich zu, dass diese hinsichtlich der fehlenden Fähigkeiten und Funktionen teilweise berechtigt ist. Oft basiert diese Kritik allerdings auch auf Unwissenheit über die bewusst gewählte Zielsetzung und die Grenzen der technischen Möglichkeiten des gewählten Ansatzes. So wurde die Corona-Warn-App ganz bewusst für den Zweck des datensparsamen Contact-Tracing (Rückverfolgung) entwickelt. Ein

Contact-Tracking (Verfolgung) ist daher von Anfang an nicht geplant worden und daher technisch in dieser App nicht möglich. Im Gegenteil, das Tracking würde zu großen technischen Problemen und einem Start von Null führen.

Allerdings gibt es natürlich Potenzial für eine Weiterentwicklung der Corona-Warn-App. So wurde diese beispielsweise nachträglich mit einem Kontakt-Tagebuch versehen. Auch eine Clustererkennung ist sinnvoll und möglich.

Ich würde mich übrigens sehr freuen, wenn ich solche Ideen nicht erst aus der Presse erfahren würde. Ich appelliere daher an das Bundesgesundheitsministerium und das Robert Koch-Institut, mich möglichst frühzeitig über Erweiterungspläne für die Corona-Warn-App zu informieren. Es sollte doch dort langsam klar geworden sein, dass ich das Projekt Corona-Warn-App konstruktiv begleite.

Meine Lehre ist jedenfalls: Pandemiebekämpfung ist auch unter Beachtung datenschutzrechtlicher Vorgaben machbar und ich bin stets bereit, über digitale Lösungen zur Pandemiebekämpfung nachzudenken.

IV. Die Krise als Prozessbeschleunigerin

Die Pandemie ist endlich, aber der Datenschutz sollte ihr dabei keine Gesellschaft leisten.

Dazu möchte ich drei Thesen entwickeln:

1. Die Digitalisierung in Deutschland hinkt hinterher und gefährdet so auch den Datenschutz.

2. Die DSGVO steht der Digitalisierung nicht im Weg und hat sich als grundrechtliche Leitlinie auch in der Notstandslage bewährt.

3. Der europäische Datenschutz muss die Auseinandersetzung mit den US-Internetkonzerne und dem chinesischen Repressions- und Überwachungsstaat bestehen.

Zu These 1: Mängel der Digitalisierung in Deutschland:

Die aktuelle Krise hat neben den vielen Misslichkeiten und Herausforderungen im Alltag aber noch ein zweites Gesicht. Sie treibt viele Prozesse voran, die schon viel zu lange vor sich hindümpeln.

Ein Musterbeispiel ist die seit Jahr und Tag verschleppte Digitalisierung in allen Bereichen des Staates, der Wirtschaft und der Gesellschaft.

Da wurde in der Vergangenheit vieles verschlafen, was uns jetzt krachend auf die Füße fällt.

Ein besonders drastisches Beispiel für alte Versäumnisse ist der Bereich Schule:

Dort fehlt es trotz einiger Anstrengungen der letzten Monate noch immer:

- an technischem Gerät und geeigneten Lösungen,
- geschultem Fachpersonal,
- sowie der Aus- und Fortbildung des Lehrpersonals.

Diese unzureichende Digitalisierung verstärkt die schon vorhandene soziale Kluft im Lande immer weiter. Kinder mit schwierigem familiärem Hintergrund werden angesichts dieser Defizite und Versäumnisse immer weiter abgehängt.

Der Datenschutz in der aktuellen Situation ist darauf angewiesen, diese Nachholprozesse bei der Überwindung alter Versäumnisse in die richtige Richtung zu lenken.

Sonst wird der Datenschutz in der Krisenlage sehr schnell zu einer Krise des Datenschutzes.

Zu 2. Die DSGVO hat sich als grundrechtlich vorbildliche Leitlinie auch ökonomisch bewährt.

Der Datenschutz steht selbst knapp 3 Jahre nach dem „Scharfstellen“ im Mai 2018 nach Meinung vieler Beobachter und Akteure noch immer unter „Bewährung“.

Für die einen steht die DSGVO wegen vermeintlich zu viel Bürokratie dem wirtschaftlichen Aufschwung im Wege - andere wiederum beklagen, der Datenschutz sei - wie andere Grundrechte auch - „unter die Räder“ eines Notstandsregimes geraten.

Die Vorwürfe aus der Wirtschaft begleiten die DSGVO seit ihrer Entwicklung.

Sie sind wie eh und je meist frei von empirisch belegbaren Fakten.

Mit der Pandemie mehren sich bereits Stimmen, die sich das „Hochfahren“ der Wirtschaft nicht ohne eine gründliche Entsorgung von Datenschutzvorschriften vorstellen können.

So der BDI.

Es ist das gleiche Lamento wie beim Klimaschutz, Diversität, Mindestlohn und einer wertegeleiteten Außenpolitik.

Zukunftsgewandt und nachhaltig sind solche Forderungen nicht: Ganz im Gegenteil.

Ich sehe in der Krise und der Zeit danach eine 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. Voraussetzung dafür sind jedoch Lösungen im Sinne von **privacy by design und privacy by default**. Die müssen datenschutzfreundlich ausgestaltet werden.

Datensparsame Konzepte blockieren und hemmen die Krisenbewältigung nicht. Sie tragen vielmehr zur besseren Effektivität und Effizienz des jeweiligen Datenverarbeitungssystems bei.

Das wäre auch gut für die Bilanzen.

Die Menschen werden nur digitalen Systemen vertrauen, die sie nicht ausspähen und in deren Folge keinerlei Repressalien zu erwarten sind.

Transparenz ist eine zwingend notwendige Voraussetzung für die Unterstützung der Bevölkerung. Sonst wird das nichts.

Zu 3. Der Datenschutz und die internationale Machtfrage USA und China

Die Macht der US-Konzerne bleibt eine unbewältigte Herausforderung des europäischen Datenschutzes.

Auch die Corona-Warn-App ist technisch von den Smartphone-Systemen von Apple und Google abhängig.

Mit den neuen Bußgeldvorschriften der DSGVO lassen sich zwar bestimmte Folgen dieses ökonomischen Machtgefälles abmildern.

Dennoch bleibt die Achillesferse des europäischen Datenschutzes bestehen, ihre chronische Abhängigkeit der Digitalisierung in Europa von den führenden US-Konzernen Apple, Amazon, Facebook und Google.

Über die Entwicklung der Warn-App hinaus sind diese als Monopolanbieter in der Folge der Krise noch mächtiger geworden. Das zeigen die geradezu explodierten jüngsten Börsenwerte von Apple und Amazon in den letzten Tagen eindrucksvoll.

Apple, Google, Facebook, Microsoft und Amazon waren schon vor der Krise die teuersten Unternehmen der Welt.

Die US-Konzerne verfügen jetzt über noch mehr Finanzressourcen und Datenmassen, mit denen sie Einfluss ausüben und Konkurrenten verdrängen können.

Wer über die persönlichen Daten verfügt, übernimmt auch mit die Lenkung und Kontrolle ganzer Branchen und darüber hinaus der Gesellschaft.

Betroffen sind der Rechtsstaat und die Demokratie in ihrer Gesamtheit.

Deshalb müssen die Datenschutzbehörden der EU-Mitgliedsstaaten die Möglichkeiten der DSGVO tatsächlich nutzen.

Auch die Zusammenarbeit im Europäischen Datenschutzausschuss muss besser genutzt werden. Das Verfahren ist auch bei großen, grenzüberschreitenden Verfahren mit Leben zu füllen.

Datenschutzverstöße müssen zeitnah und so effektiv wie möglich von der zuständigen federführenden Behörde geahndet werden. Nur so können wir globale Technologie-Konzerne auf die Einhaltung von Spielregeln verpflichten.

Um aber überhaupt Grenzen setzen zu können, wird auch die Zusammenarbeit von Wettbewerbsschutz und Datenschutz immer wichtiger werden.

Europa muss sich vor allem technologisch emanzipieren und eine eigene Datensouveränität entwickeln. Das ist aus Sicht des Datenschutzes unverzichtbar. Sonst geraten wir in die Situation „Vogel friss oder stirb“.

Ich will mit aller Klarheit deutlich machen: Bekommt Europa mit seinem Datenschutzrecht die Datenriesen und ihre Geschäftsmodelle nicht in den Griff, ist die DSGVO gescheitert.

- **Die Herausforderungen durch China**

Die Herausforderung aus China wird zumindest längerfristig sogar noch größer als die durch die genannten Internetriesen aus den USA.

Die USA sind eine Demokratie und auch nach 4 Jahren Trump ein funktionierender Rechtsstaat. Die Struktur der dortigen Unternehmen ist zumindest im Vergleich zu China transparent und bei aller Kritik gibt es bekannte Rechtswege.

Dem gegenüber werden wir von chinesischer Seite über die Strukturen der dortigen Internetfirmen und deren Verflechtungen zum Staatsapparat bewusst im Unklaren gelassen.

Die dortige Staats- und Parteiführung nutzt Digitalisierung und Künstliche Intelligenz zum Schutz vor der Demokratie. Das ist der große Unterschied zu den USA.

So fördert die chinesische Regierung die Künstliche Intelligenz nicht nur zur Schaffung besserer Wettbewerbsbedingungen, sondern auch mit dem Ziel, die eigene Bevölkerung und die Zivilgesellschaft wirkungsvoller zu überwachen.

Wegen der engen Verflechtungen zwischen dem chinesischen Staat und seiner herrschenden Partei mit Teilen der chinesischen Wirtschaft ist daher höchste Vorsicht geboten, wenn es um digitale Infrastruktur, Soziale Medien und Bezahlsysteme geht.

Wir müssen hier stets Sicherheitserwägungen im Hinterkopf haben, wenn wir es mit der Expansion chinesischer Unternehmen in Europa zu tun haben. Datenschutzversprechen einfach zu glauben, wäre einfältig.

Auch hier schaffen wir es nicht im nationalen Alleingang. Wir brauchen ein gemeinsames Vorgehen aller europäischen Partner. Nur so können wir Europa im globalen Wettbewerb stärken und zugleich unsere bürgerrechtlichen Standards schützen.

V. Schlussbemerkung

Die Digitalisierung ist nicht aufzuhalten. Sie darf jedoch nie zum Selbstzweck werden. Sie soll vielmehr dem Menschen dienen und ihre Spielregeln müssen Rechtsstaat und der Demokratie verpflichtet bleiben.

Ich wünsche mir, dass Datenschutzaspekte gerade auch bei den Digitalisierungsprojekten endlich von Anfang an mitgedacht werden.

Digitale Technologien müssen den Grundsätzen der Selbstbestimmung und der Privatheit, der Sicherheit und der Nachhaltigkeit genügen.

Nur, wenn die Menschen darauf vertrauen können, werden sie den digitalen Wandel als Chance sehen und mitgehen.

Als Deutsche und als Europäer stehen wir für eine andere Digitalisierung als autoritäre Überwachungsregime in China oder Laissez-faire-Ansätzen wie in den USA.

Wir in Europa kämpfen für eine Digitalisierung, die unsere Werte widerspiegelt.

Ich danke Ihnen für Ihre Aufmerksamkeit und freue mich auf Nachfragen und Anmerkungen.