Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

Prof. Ulrich Kelber

„Perspektiven der Datenschutzaufsicht“

- Datenschutz als Sündenbock
- Aufsichtsbehörden in der Pandemie

Kölner Tage Datenschutzrecht 2021
Verlag Dr. Otto Schmidt

Hybridveranstaltung, 07.10.2021

Es gilt das gesprochene Wort

I. Einleitung

Sehr geehrter Herr Prof. Härting,
sehr geehrter Herr Dr. Moos,
liebe Kolleginnen und Kollegen,
sehr geehrte Damen und Herren,

ich danke für die Einladung zu dieser Tagung.

Es ist den Veranstaltern gelungen, an beiden Veranstaltungstagen wieder viele ausgewiesene Praktikerinnen und Praktiker des Datenschutzes zu versammeln. Ich bin mir sicher, dass die fachlichen Impulse aus dieser Runde in der Öffentlichkeit und der Politik wichtige Anstöße geben werden. Vor allem aber würde ich es sehr begrüßen, wenn sie auch zur Versachlichung der bisweilen etwas aufgeregten Debatte über die Praxistauglichkeit datenschutzrechtlicher Regelungen beitragen könnten.

Herr Prof. Härting, Herr Dr. Moos, Sie haben mir neben dem Titel meines Beitrags zwei Stichworte mit auf den Weg gegeben:

Die Stellung der Aufsichtsbehörden und die Schuldzuweisungen in Richtung Datenschutz.

Gerne komme ich Ihrer Anregung nach, mir die allseits beliebte öffentliche Schuldzuweisung gegenüber dem Datenschutz zur Brust zu nehmen.

„**Der Datenschutz ist schuld“** oder „Das geht nicht wegen Datenschutz“ ist bekanntlich nicht nur beim Umgang mit Covid 19 ein ebenso beliebtes wie untaugliches Mittel, eigenes Versagen zu kaschieren oder unliebsame Auskünfte zu verweigern. Das geht sogar bis zur Flut-Katastrophe, dem Afghanistan-Einsatz und Maskendeals.

II. Datenschutz und Datenschutzaufsicht in der Pandemie

Seit eineinhalb Jahren befindet sich die Republik im organisatorischen Krisenmodus. Die Staatskassen leeren sich und wir sehen uns überwiegend nur noch im Kachelformat. Viele Menschen hatten die Hoffnung, dass es diesen Sommer endlich vorbei sein könnte; leider blieb es bei der Hoffnung.

Was sich während all dieser Zeit gezeigt hat ist, dass die vielfältigen Folgen der Pandemie konsequent auch Fragen des Datenschutzes tangieren. Standen noch bis zum Frühjahr die Warn-Apps im Mittelpunkt der Aufmerksamkeit, rücken 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 COVID-19-Pandemie spielt eine wichtige Rolle in unserem Leben – und für die tägliche Arbeit der Datenschutz-Aufsichtsbehörden. Das wird sich auch so schnell nicht ändern.

1. Arbeitsstruktur im Umbruch

Wie in allen anderen Behörden und private Unternehmen wandeln sich die internen Arbeits- und Kommunikationsformen auch in meinem Haus ziemlich rasant. 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 Videokonferenzen. 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.

Die Krise hat somit – wie fast überall – auch beim BfDI Veränderungen des bisher bekannten Arbeitsalltags erzwungen. Und ich bin mir sicher, dass diese Umwälzungen nachhaltig sein werden – und zwar überall. Meine ganz persönlichen Erfahrungen als Leiter einer 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.

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.

Zudem hat Corona unsere Arbeit nicht nur nach innen verändert. Die Pandemie hat auch unsere Arbeit nach außen umgekrempelt und an einigen Punkten mitunter erheblich erschwert.

Seit dem Frühjahr 2020 können wir mit den unserer Aufsicht unterfallenden Stellen fast ausschließlich nur noch elektronisch kommunizieren. Die Kontroll- und Beratungstätigkeit und die Gespräche mit den jeweiligen Fachleuten und Behördenleitungen vor Ort machen aber gerade einen wichtigen Teil meiner Arbeit aus.

Wie Sie wissen, umfasst mein Aufgabenbereich als Bundesbeauftragter auch die Informationsfreiheit des Bundes. Gerade hier haben die vielen Besuche vor Ort und die Gespräche mit den zuständigen Kolleginnen und Kollegen die Sensibilität für Transparenz deutlich geschärft.

Ich bin daher sehr froh darüber, dass so langsam die direkte Arbeit vor Ort wieder anlaufen konnte. Die Ergebnisse können Sie in meinen Jahresberichten nachlesen.

2. Neue Herausforderungen für die Datenschutzaufsicht

Die Hektik in der Gesetzgebung im Zusammenhang mit der Pandemie hat auch mich persönlich und meine Mitarbeiterinnen und Mitarbeiter ordentlich auf Trab gehalten.

Allein die Beratung von Normgebern und öffentlichen Stellen wie auch die Bearbeitung von Beschwerden mit diesem Kontext nahm einen nicht unerheblichen Teil der verfügbaren zeitlichen Ressourcen in Anspruch. Die Gesetzgebung verlief recht hektisch. Oft mussten wir binnen Stunden, manchmal sogar am Wochenende, Stellung beziehen. Der Negativrekord steht bei zwei Stunden Frist zur rechtlichen Prüfung einer komplexen Veränderung einer Rechtsordnung.

Ich nenne nur die Stichpunkte:

- die Erhebung von Gesundheitsdaten durch Arbeitgeber und dessen **Auskunftsanspruch** über den Impfstatus.
- und die Entwicklung und Anwendung der verschiedenen **Corona--Apps und -Systeme, seien es Gesundheitsdatenteilung, Kontakt-Tracing, Unterstützung Gesundheitsämter, neue Register oder Zertifikate.**

- **Darf der Chef wissen, ob ich geimpft bin?**

Im Zuge der stockenden Impfkampagne ist in den letzten Wochen die Abfrage des Impfstatus durch die Arbeitgeber in die Debatte geraten. Die Bundesvereinigung der deutschen Arbeitgeberverbände hat diese Forderung maßgeblich vorangetrieben.

Die Gewerkschaften wiederum sind strikt dagegen und warnen vor der Ermöglichung solcher Fragen nach gesundheitlichen Daten der Beschäftigten. Ich kann diese Besorgnisse gut nachvollziehen. So könnte eine schwangere Mitarbeiterin – lange Zeit ohne Impfempfehlung durch die STIKO - genötigt werden, ihre Schwangerschaft zu offenbaren. Wie soll sie sonst begründen, warum sie nicht impfen lässt und dass sie nicht zur Spezies der Impfverweigerer gehört? Was ist mit dem Rheuma-Erkrankten, der eine Booster-Impfung erhalten hat oder demjenigen, der wegen einer Erkrankung und möglicher Long-Covid-Symptome noch keine Impfung erhalten hat. Alles das sind Informationen, die man sich nicht beim Arbeitgeber wünscht.

Andererseits verstehe ich natürlich – nicht zuletzt auch in meiner Funktion als Behördenleiter – den Wunsch von Arbeitgebern, Bedingungen schaffen zu können, in denen ein sicheres Arbeiten für Mitarbeitende auch in Pandemiezeiten bestmöglich gewährleistet werden kann. Denn letztendlich ist es für Arbeitgeber und -nehmer gleichermaßen von Interesse dafür zu sorgen, dass der Arbeitsplatz kein Ort ist, der neue Infektionsketten schafft.

Ich plädiere daher für eine sachbezogene und lösungsorientierte Diskussion ohne falsche Frontenbildung. Betriebe und Behörden sind verpflichtet, den Gesundheitsschutz der Beschäftigten sicherzustellen. Es darf auch nicht sein, dass in einem Land der Impfstatus erfragt werden darf, in anderen wiederum nicht. Die Regelung muss daher in jedem Fall Rechtssicherheit für alle Beteiligten bringen.

Keinesfalls unter die Räder kommen darf der Grundsatz, dass wir es mit sensiblen gesundheitsbezogenen Daten zu tun haben. Eine saubere rechtliche Regelung und in jedem Fall eng befristete Regelung muss daher verhindern, dass schutzwürdige Daten gegen den Willen der Betroffenen zur Firmen- oder Behördenleitung gelangen wie durch eine Katzenklappe.

Ich kann mir ein solches rechtssicheres Arbeitgeber-Auskunftsrecht durchaus vorstellen, aber nur in einer Übergangszeit der Pandemie und auch nur, wenn dies erforderlich ist und wenn es kumuliert auf „3G“ oder – wenn begründet notwendig – „2G“ angewandt wird. Es darf daher ausschließlich darum gehen, ob jemand eines der drei bzw. zwei Kriterien „geimpft“, „genesen“ oder „getestet“ erfüllt oder nicht. Der Status im Detail muss vertraulich bleiben.

Bundestag und Bundesrat haben Anfang September schließlich entschieden, ein Fragerecht für bestimmte Arbeitsbereiche einzuführen. Dabei wurde es über den bisher geltenden Bereich der Krankenhäuser und Arztpraxen auf weitere Tätigkeiten, z.B. in Pflegeheimen, Schulen und Kindergärten, ausgeweitet.

Gerade weil ein von vielen gewünschtes umfassendes Fragerecht nicht durchgesetzt wurde, würde ich mich sehr wundern, wenn die Debatte über die Offenlegung des Impfschutzes mit dem aktuellen Gesetz beendet ist.

- **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 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 schutzwürdigen 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 Datenschutz-beauftragten sowie die Betriebs- und Personalräte einzubinden.

Die Aufsichtsbehörden sind gerne bereit, beratend Hilfestellung zu leisten. Denn – dies möchte ich ohne Umschweife klar herausstellen – der Teufel liegt in den vielen rechtlichen und technischen Details, die hier

jeweils zu regeln sind. Handreichungen helfen, sind aber auch keine Zauberbücher, die auf alles eine eindeutige Antwort parat haben.

4. Immer mehr Beschwerden zu Datenschutzverstößen

Ich habe in meinen Überlegungen primär die beratende und helfende Hand der Datenschutzaufsicht in den Mittelpunkt gestellt. Es ist nicht unser Anspruch, möglichst viele und schlagzeilenträchtig hohe Sanktionen zu verhängen. Ganz im Gegenteil, Prävention und Positivbeispiele sind uns das Allerliebste.

Klar ist aber, dass der Schutz persönlicher Daten nicht zum unverbindlichen Small Talk werden darf, nicht zum Nice-to-have – und auch nicht werden wird!

Bei allen Datenschutz-Aufsichtsbehörden führte die Corona-Pandemie zu steigenden Fallzahlen. Zahlreiche Betroffene beschwerten und beschweren sich über den unsachgemäßen Umgang mit ihren Daten. Die Masse an Einzelfällen gepaart mit der ungenügenden personellen Ausstattung vieler Landesdatenschutzbehörden stellen uns immer wieder vor die Herausforderung, nicht für andere wichtige Aufgaben gelähmt zu werden.

Dass der Schutz der Grundrechte während der Pandemie weiter an Bedeutung und Aufmerksamkeit gewonnen hat, verdanken wir dem europäischen Datenschutzrecht. Die DSGVO verknüpft die erweiterten Rechte der betroffenen Personen und die neuen Pflichten der Verantwortlichen endlich mit wirksamen Handlungs- und Sanktionsmöglichkeiten.

Wer auch nach 5 Jahren DSGVO die Daten Betroffener noch immer nicht schützen kann – oder vereinzelt sogar will, muss mit Konsequenzen rechnen. Ultimativ können das dann auch empfindliche Bußgelder sein. Das ist die moderne Variante der alten Volksweisheit „Wer nicht hören will muss fühlen“.

5. Elektronische Patientenakte darf Patientinnen und Patienten nicht entmündigen

Meine Damen und Herren,

Ich habe versucht, die an mich gestellte Frage nach den Auswirkungen der Pandemie auf meine Behörde anhand einiger Beispiele zu erläutern. Aber sogar im Gesundheitsbereich bleiben Fragen auf dem Tisch, die mich schon lange vor Corona seit vielen Jahren beschäftigen.

Lassen Sie mich einen Klassiker herausgreifen: die elektronische Patientenakte.

Da fehlt mir schlicht jedes Verständnis. Ich habe die meiner Zuständigkeit unterstehenden gesetzlichen Krankenkassen angewiesen, die neue ePA um zusätzliche Datenschutzfunktionen zu erweitern. Passiert da nichts, verstößt die digitale Patientenakte ohne Zweifel gegen die europäische Datenschutz-Grundverordnung.

Ich bin dafür zuständig, dass die Datenschutzrechte von rund 45 Millionen Versicherten bei 63 gesetzliche Krankenkassen gewahrt werden. Und ich bin entschlossen, meinen Teil beizutragen, dass dies auch wirklich geschieht.

Ich bestehe ohne Wenn und Aber auf dem Recht der Versicherten, selbst zu bestimmen, welche Stelle welchen Teil der Daten aus ihren eigenen Unterlagen zu sehen bekommt. Versicherte haben einen Anspruch darauf zu entscheiden, welches Dokument von welchem Arzt, Therapeuten oder anderen Beteiligten einsehbar ist. Man ist sicherlich gut beraten, in der Regel den Ärztinnen und Ärzten seines Vertrauens Einblick in alle Unterlagen zu geben. Aber es mag, je nach Situation (Zweitdiagnose) oder persönlicher Betroffenheit (Wozu muss der Krankengymnast etwas über eine Psychotherapie wissen?), davon eben auch Ausnahmen geben.

Ich werde es nicht zulassen, dass die Kassen nach einem „Alles-oder-Nichts-Prinzip“ verfahren, weil sie nur die Mindestanforderungen der nationalen Gesetzgebung umsetzen. Das ist weder Stand der Technik noch entspricht es den Vorgaben der DSGVO.

Ich habe auch Anstoß daran genommen, dass die ePA von den Versicherten nur mit einem geeigneten Smartphone, Tablet oder ähnlichem Gerät eingesehen und verwaltet werden kann. Selbst wenn das bedeutet, dass ab 2022 rund 90 Prozent der Versicherten mit mobilen Endgeräten Einblick nehmen und den Zugriff auf die Inhalte steuern können, bleiben die restlichen zehn Prozent auf der Strecke.

Eine solche Zwei-Klassen-Gesellschaft können wir uns – und zwar erst Recht, wenn es um sensibelste Gesundheitsinformationen geht – nicht leisten. Wer hier auf die Möglichkeit hinweist, dass man ja einen Vertreter beauftragen könnte, mit seinem Gerät die ePA zu verwalten, macht es sich zu einfach.

Nicht zuletzt weil es sicherlich Menschen gibt, die auch „Vertrauten“ nicht intimste Details ihrer höchstpersönlichen Krankenakte anvertrauen möchten geschweige denn (halb)fremden Personen, weil sie einfach keine „Vertrauten“ haben.

Unter dem Strich sollte eigentlich jedem klar sein, dass wir ein Grundrecht nicht unter Handy-Vorbehalt stellen können und dürfen. Und es kann doch nicht der Ernst des Bundesamts für die soziale Sicherung und der Krankenkassen sein, dass die Alternative nur der Verzicht auf die Vorzüge der ePA ist. Das ist der Grund, warum ich auf eine Regelung bestehe, die das Bundesgesundheitsministerium übrigens im ursprünglichen Gesetzentwurf vorgesehen hatte und die im parlamentarischen Verfahren wohl aufgrund des Lobbyierens der Krankenkasse gestrichen wurde.

Das jetzt das BAS als dem BMG unterstellte Behörde die Krankenkassen auffordert, gegen eine Regelung zu klagen, die das BMG zuvor, sicherlich mit Beratung des BAS, für richtig erachtet hatte, ist tragisch-komisch.

III. „Der Datenschutz ist an allem Schuld“

Die Arbeit der Aufsichtsbehörden unter den besonderen Bedingungen der Pandemie steht in einem Spannungsfeld tiefgreifender politischer Entscheidungen und einer entsprechend erhitzten öffentlichen Debatte. Hinzu kommen noch die Zuspitzungen durch den Bundestagswahlkampf.

Die Veranstalter haben dies erkannt und mit der Themenstellung meines Vortrags verbunden.

Politisch haben wir da so einiges im Sortiment.

So fordert die AfD die Abschaffung der DSGVO. Die ist ihr schlicht zu komplex. Das europäische Recht soll „durch ein neues, schlankes Datenschutzgesetz zur Wahrung informationeller Selbstbestimmung“ ersetzen werden. Ob auf europäischer oder – nach Austritt aus der EU – nationaler Ebene wurde nicht bestimmt.

Wie man in Zeiten von Open Data und künstlicher Intelligenz und nach wie vor exponentiellem Wachstum bei der Verarbeitung von Daten mit simplen Grundsätzen die personenbezogenen Daten schützen können sollte, bleibt mir ein Rätsel.

Leider finden Schuldzuweisungen an den Datenschutz aber auch in der Mitte unserer Gesellschaft statt. Datenschutz wird zum Hemmschuh der Pandemie-Bekämpfung erklärt. Er untergräbt nach diesen Mythen einen wirksamen Katastrophenschutz und er beglückt sogar die Taliban. Ja, Sie haben richtig gehört!

Verlassen wir aber jetzt das Reich der Legenden und wenden uns den Tatsachen zu.

Wer hat denn versäumt, einheitliche IT-Systeme in den Gesundheitsämtern einzuführen und sie so leistungsfähig zu machen? Da klappern noch immer die Faxgeräte.

Warum wurden in der Vergangenheit nach und nach die Sirenen abgestellt oder sie funktionieren nicht?

Warum haben wir mehr Funklöcher als andere Länder mit deutlich geringerer Wirtschaftskraft?

Das war doch nicht der Datenschutz! Ganz im Gegenteil!

Was glauben Sie, wie viele E-Mails ich bekomme, in denen mir die Corona-Toten zur Last gelegt werden. Einige wollen mich vor Gericht sehen oder – wohl in Unkenntnis meiner Körpergröße - mir nachts auflauern. Und das sind noch die eher harmlosen Zuschriften.

Sicherlich nicht ganz unschuldig daran ist eine leider nicht kleine Gruppe von Politikern, Wirtschaftsvertretern und sogar Wissenschaftlern – teilweise wider besseren Wissens – die kontinuierlich 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 aktuell bei der Auskunftspflicht zu Impf- und Serostatus.

Aber im Zeitalter der alternativen Fakten halten sich auch Märchen und Mythen vom angeblich so unantastbaren Datenschutz zäh wie eingetrockneter Himbeersirup. Da können wir das Gegenteil noch so oft anhand von Fakten widerlegen.

Doch woher kommt diese Kampagne?

Da ist viel „Nachplappern“ falscher Informationen im Spiel – gerne gepaart mit allgemeiner und spezieller Unkenntnis. Bei denen, die es aber wissen sollten, drängt sich die Vermutung auf, dass hier mit Fehlinformationen der Datenschutz ganz gezielt in Misskredit gebracht werden soll, um dadurch von andere Verfehlungen – nicht nur bei der Pandemiebekämpfung - abzulenken oder einen für die eigenen Geschäftsmodelle hinderlichen Schutz von Grundrechten loszuwerden.

1. Der Datenschutz muss sich nicht verstecken

Nach den sogenannten Corona-Verordnungen waren unter anderem Restaurants verpflichtet, zur Nachverfolgung möglicher Kontakte mit durch den Corona-Virus infizierten Personen Kontaktdaten aller Besucherinnen und Besucher zu erfassen. Das hat sich durch die neuen G2- oder G3-Regelungen inzwischen geändert.

In den Medien wurde nach der Einführung dieser Pflicht vermehrt darüber berichtet, dass die Polizei zur Aufklärung von Straftaten mehrfach auf diese Gästelisten zugegriffen habe. In der Folge war uns auch ein erster entsprechender Fall aus Nordrhein-Westfalen bekanntgeworden.

Tatsächlich war die Nutzung der Corona-Kontaktlisten zur Strafverfolgung nach der Strafprozessordnung bisher **unter bestimmten Voraussetzungen zulässig.**

Dass die Corona-Kontaktlisten schon kurz nach ihrer Einführung zur Strafverfolgung genutzt wurden, zeigt wieder einmal: Wo Daten erhoben werden, wachsen neue Begehrlichkeiten wie Osterglocken im Frühling.

Aus Sicht der Betroffenen wussten im Fall der Zugriffe auf Corona-Kontaktlisten die Betroffenen nichts von der Möglichkeit einer zweckändernden Verwendung zur Strafverfolgung. Dies schürte Unmut und kostete Vertrauen. Erschwerend kommt hinzu, dass öffentliche Stellen zuvor noch den Eindruck erweckt hatten, dass diese Daten ausschließlich für die Bekämpfung der Corona-Pandemie genutzt werden dürften.

Aus einem solchen Vorgehen können Risiken für die Akzeptanz der Bevölkerung entstehen, einschneidende Maßnahmen, wie die im Zusammenhang mit der Corona-Pandemie, weiter hinzunehmen oder wahrheitsgemäße Angaben zu machen.

Der Bundesgesetzgeber hat meine Kritik an der bisherigen Rechtslage aufgegriffen und in § 28a Abs. 4 des Infektionsschutzgesetzes eine enge Verwendungsbeschränkung der Corona-Kontaktlisten eingeführt. Danach dürfen die Listen nur noch für die Zwecke verwendet werden, für die sie erhoben wurden sowie ergänzend für die besonderen im Landesrecht vorgesehenen Fälle. Eine Nutzung zu Strafverfolgungs-zwecken ist danach ausgeschlossen.

Auf die diversen Märchen, wie der Datenschutz eine Weiterentwicklung der Corona-Warn-App behindert habe, werde ich an dieser Stelle erst gar nicht weiter eingehen. Genauso wenig wie auf die von den Datenschutzkritikern hochgelobten asiatischen Corona-Warn-Apps, die aber in der Realität nie existiert haben.

Fast die Hälfte der Talkshow-Teilnehmer und viele Leitartikelschreiber plappern dieses Märchen aber bis heute nach. Recherche-Kompetenz null.

Zusammenfassend kann auf jeden Fall festgehalten werden:
Aus datenschutzrechtlicher Sicht gab es bei der Prüfung der verschiedenen Maßnahmen zur Pandemiebekämpfung keine wirklich unlösbaren Probleme.
Und keine einzige geeignete und effektive Maßnahme, ich wiederhole: keine einzige geeignete und effektive Maßnahme zur Pandemiebekämpfung ist am Veto der Datenschutzaufsicht oder an richtig verstandenen Datenschutzregelungen gescheitert!

2. Hochwasser: der Datenschutz ist schuld

Lassen Sie mich noch ein weiteres, sehr aktuelles und tragisches Beispiel nennen, wie gegen den Datenschutz mit falschen Behauptungen Stimmung gemacht wird.

Während Corona noch wütet, hat unser Land eine Hochwasserlage getroffen, deren Ausmaß vieles des bisher Dagewesenen sogar noch übersteigt. Angesichts der dramatischen Folgen der Katastrophe mit über 180 Toten müssen wir die Frage nach der Krisentauglichkeit dieses Landes und seiner Bürokratie diskutieren.

Umso empörender, wenn hier mal wieder dem Datenschutz die Schuld für Versagen in die Schuhe geschoben wird.

Der Glaube an die Wirksamkeit der bestehenden Warn-Apps wie Katwarn und Nina wurde jedenfalls auf dramatische Weise widerlegt. Nur eine Minderheit der Deutschen lädt sie überhaupt runter. Zusammen erreichen die Warn-Apps gerade einmal rund 15 Prozent der Mobilfunknutzerinnen und Nutzer.

Erfolgversprechender sind in derartigen Notsituation Cell-Broadcast-Warnsysteme. Diese lassen jedes Handy jederzeit Alarm schlagen - auch die stummgeschalteten und nicht aktualisierten.

Im Gegensatz zur SMS werden beim Cell Broadcasting die Textnachrichten an alle Empfänger einer Funkzelle gleichzeitig geschickt. Die Technik wird von fast allen Handys unterstützt, auch von älteren Geräten aus der Zeit vor den Smartphones. Und in vielen anderen Ländern, wie z.B. den Niederlanden, Japan und den USA wird Cell-Broadcasting daher schon lange zu Zwecken des Katastrophen-schutzes eingesetzt.

Wenn in diesen Staaten eine Behörde die Menschen in einer bestimmten Region dringend warnen will, kann sie eine identische Nachricht an alle Mobiltelefonnutzer schicken, die sich gerade in der Region befinden. Dabei spielt es keine Rolle, welche Apps der Nutzer installiert hat. Das Verfahren ist einfach und datensparend. Es braucht nicht einmal eine Internetverbindung.

Die Niederlande beispielsweise mussten dank „NL Alert“ beim Hochwasser an der Maas keine Menschenleben beklagen. Sogar hochwassergeplagte Staaten wie Bangladesch sind hier weiter als wir in Deutschland.

Japan gibt den Mobilfunkbetreibern vor, dass die Weiterleitung einer Warnmeldung maximal vier Sekunden dauert. An der Ahr dauerte die Warnung viele Stunden. In Bad Neuenahr gingen die Leute noch an der Ahr spazieren, als in Schuld die Menschen auf den Dächern um ihr Leben kämpften.

Die vielen Toten und die gewaltigen Zerstörungen haben die Diskussion über wirksamen Katastrophenschutz aus ihrem Wachkoma gerissen. Die riesigen Versäumnisse liegen eigentlich auf der Hand.

Doch was fällt einem Bundesminister dazu ein? Es sei „mal wieder“ der Datenschutz, der ein effektives Krisenmanagement blockiere. In „Bild Live“ verbreite er die alternative Wahrheit, die Ausspielung von Warn-SMS direkt an die Bürger sei am Datenschutz gescheitert. Obwohl in seinem Ministerium Briefe meiner Behörde aus der Vergangenheit vorliegen, wo wir die Einführung von Cell Broadcasting dringend empfehlen.

Mittlerweile hat das Kabinett sich auf eine „Formulierungshilfe“ zur Änderung des Telekommunikationsgesetzes (TKG) verständigt und so die Einführung von Cell-Broadcast beschlossen. Natürlich rühmt sich die Regierung nun mit der Entscheidung. Dass die Einführung schon deshalb erforderlich wird, weil man damit die Vorgaben einer europäische Richtlinie umgesetzt, wird dabei irgendwie immer unerwähnt gelassen.

Ebenso wie der Fakt, dass sich Deutschland auf europäischer Ebene massiv dafür eingesetzt hat, in eben diese Richtlinie die Möglichkeit hinein zu verhandeln, die Vorgaben auch mit alternativen Modellen zum Cell-Broadcast erfüllen zu können, weil man sich erhoffte, ausschließlich auf die NINA-App setzen zu können.

Der jetzige Schwenk sagt natürlich auch viel über das hiesige Krisenmanagement aus. Dies dem Datenschutz und damit einem Grundrecht in die Schuhe schieben zu wollen, ist unanständig.

3. Die Taliban: Auch ein Geschöpf des Datenschutzes

Ich hatte eingangs schon angedeutet, dass auch am Afghanistan-Debakel der Datenschutz mit verantwortlich sein soll.

Mit dieser äußerst eigentümlichen Aussage hat der frühere Präsident des BND Schindler die Diskussion bereichert.

Den Spionen sei durch das höchste deutsche Gericht ein juristischer Stein nach dem anderen in den Weg gelegt worden. Man dürfe nicht einmal mehr Terrororganisationen mit eigenen Leuten infiltrieren, weil die dadurch eine Straftat begingen. Seit einem Urteil aus dem vergangenen Jahr seien die Taliban „sogar durch unser Grundgesetz geschützt“, so Ex-Präsident Schindler.

Mit einer solchen Aussage will er wohl Nachrichtendienste reinwaschen von ihrer Mitverantwortung für das kollektive westliche Organversagen am Hindukusch. Merke: Ohne die Datenschützer hätte der BND alle anderen westlichen Geheimdienste überflügelt und den Ernst der Lage erkannt.

Das erinnert mich ein wenig an den völlig unterschätzten Film „Mr. Dynamite“ mit Lex Barker als BND-Agent, der bei einer Krise mit entführten Atomwaffen die versammelten Weltführer beruhigt: „Keine Angst, der BND kümmert sich darum“.

III. Schlussbemerkung

Die Auseinandersetzung um das Verhältnis vom Schutz personenbezogener Daten und einer vermeintlich guten Lösung von Problemen wird uns auch weiterhin begleiten, da bin ich mir leider ziemlich sicher.

Gerade in einer aufgewühlten Stimmung scheint bereits eine Mutmaßung zu genügen, mit Schuldzuweisungen um sich zu werfen wie mit Kamelle im hoffentlich 2022 wieder stattfindendem Karneval.

Dagegen zu halten, ist nicht immer einfach. Aber es lohnt sich, auch bei Gegenwind beharrlich zu bleiben. Eines macht mich optimistisch: Umfragen mit offenen Fragestellungen ergeben immer eine deutliche Mehrheit für mehr Datenschutz und nicht etwa für weniger.

Die öffentliche Meinung ist da weiter als Teile der veröffentlichten Meinung.

Und zusammen mit den zusätzlichen Ressourcen, die uns der Deutsche Bundestag gegen den Trend der eben angeführten Beispiele mit Entschlossenheit und mit großer Mehrheit gegeben hat, nehmen wir diese Aufgabe an.

Dabei bitte ich Sie auch künftig um Ihre Unterstützung.

Ich danke für Ihre Aufmerksamkeit und freue mich auf Ihre Fragen und Anmerkungen.