Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Prof. Ulrich Kelber

„Digitalisierung first, Kopflos second“

bei Cyber Security Tech Summit Europe 2020

Hochschule Bonn-Rhein-Sieg, 20. August 2020

Es gilt das gesprochene Wort

Sehr geehrte Damen und Herren,

I. [Einleitung]

ich freue mich, dass es jetzt doch noch klappt, dass ich beim Cyber Security Tech Summit sprechen kann, auch wenn sich die Umstände und das Thema deutlich gewandelt haben.

Sich die Hände zu schütteln ist nur noch eine dunkle Erinnerung, wir halten Abstand zueinander, alle mit klarem Verstand und Verantwortungsbewusstsein tragen Masken. Auch der Arbeitsalltag hat sich komplett gewandelt: In meiner Dienststelle haben wir auch vor Corona schon mehrfach in der Woche Videokonferenzen genutzt, aber das war im Vergleich zu heute fast nichts. Heute sitzen meine Mitarbeiterinnen und Mitarbeiter an manchen Tagen mehrere Stunden in Telefon- und Videokonferenzen und es ist nicht absehbar, wann sich das wieder ändert. Es ist ja auch fraglich, ob sich das wirklich wieder ändern muss.

Wir haben im letzten Jahr mit unserem Personalrat beim BfDI eine Vereinbarung zum mobilen Arbeiten getroffen und wir haben im letzten Jahr fast alle Mitarbeiterinnen und Mitarbeiter mit sicheren Laptops (geeignet für VS-NfD) ausgestattet, um ihnen das Arbeiten von unterwegs und wenigstens an einigen Tagen im Quartal von Zuhause aus zu ermöglichen. Gleichzeitig haben wir beim BfDI vollständig auf die elektronische Akte umgestellt.

Das waren, wie sich in diesem Jahr zeigte, vorausschauende Entscheidungen, denn so konnte mein Haus, obwohl zum Teil zwischenzeitlich 90 Prozent der Belegschaft im Homeoffice arbeitete, völlig normal weiterarbeiten. Und das war sowohl für die Beratung bei Gesetzentwürfen als auch bei der Entwicklung der Corona-Tracing-App auch dringend notwendig.

Und damit sich niemand im Raum falsche Hoffnungen macht: Wir werden nun auch die Kontrollen vor Ort wieder aufnehmen

II. Was haben wir in den letzten Monaten gelernt?

Meine Lehren aus der Corona-Krise lauten:

- Wir benötigen mehr Digitalisierung!
- Wir müssen mehr Interoperabilität durchsetzen!
- Wir brauchen mehr Mut und Vertrauen!

Lassen Sie mich das im Einzelnen erläutern.

Mehr Digitalisierung umschreibt für mich eine Vielzahl von Dingen, die wir schnell umsetzen, starten und entwickeln müssen. Das geht über Breitbandausbau und den schnelle Aufbau der 5G-Netze hinaus.

Zeitgemäße und gewartete IT-Netze für alle Schulen und Hochschulen, eine vernünftige Ausstattung mit Laptops, Tabletts, Lernsoftware, Kollaborationstool und datenschutzgerechten Videoplattformen, damit Online-Learning und Webinare auch außerhalb von Corona-Zeiten eingesetzt werden können und die Lehrenden diese auch beherrschen.

Das bedeutet weiterhin, dass sich die Unternehmen intensiv und schnell darüber Gedanken machen müssen, an welchen Stellen in ihren Unternehmen Homeoffice möglich oder sogar sinnvoll sein kann und dies auch umgesetzt wird.

Ich bin sicher, dass schon heute in vielen Unternehmen darüber nachgedacht wird, wann und wie Videokonferenzen die Dienstreisen ersetzen können. Ich glaube nicht, dass dies immer möglich sein wird, weil man ab und zu auch das Gespräch am Rande braucht, um mehr zu erfahren, aber ich kenne Unternehmen, die heute schon ihre Dienstreiseetats deutlich kürzen und lieber vernünftige Videokonferenz-Technik einkaufen.

Das bedeutet weiterhin, dass auch der Staat und Verwaltungen massiv in die Digitalisierung einsteigen und investieren müssen. Wenn ich mir anschaue, wie lange manche Digitalisierungsprozesse in diesem Bereich bis zur Umsetzung brauchen, dann kann ich nur den Kopf schütteln. Und, ich sage es gleich, das liegt überhaupt nicht am Datenschutz, sondern am Beharrungsvermögen mancher Entscheider. Die elektronische Patientenakte ist da das aktuell gruseligste Beispiel, mit dem sich schon meine beiden Vorgänger herumschlagen mussten.

Mehr Interoperabilität heißt für mich, es muss bei der Neuentwicklung von Geräten und Software mehr darauf geachtet werden, dass diese nicht nur mit der Vorgängerversion kompatibel sind, sondern auch mit den “Nachbarn“. Es ist doch total nervig, wenn ich für jede geplante Videokonferenz erst einmal klären muss, mit welchem Tool diese durchgeführt werden soll. Haben Sie vor Corona gewusst, wie viele verschiedene Videokonferenz-Systeme es gibt? Und dass die fast alle nicht miteinander kompatibel sind? In meinem Büro steht mittlerweile ein Extra-Laptop auf dem nur die Videokonferenz-Software drauf ist, die ich nicht aus den sicheren Netzen des Bundes nutzen kann. Das ist absurd. Welcher normale Mensch, welches Unternehmen kann es sich leisten so viele unterschiedliche Systeme vorzuhalten, damit man sich auch mit jedem unterhalten kann?

Das Gleiche gilt auch für die Messenger und zum Teil auch für Kollaborationstool und Office-Anwendungen. Hier muss der Gesetzgeber Interoperabilität vorschreiben, auch damit freche neue Wettbewerber das Oligopol der Datenkonzerne herausfordern können.

Und damit komme ich zum nächsten Punkt: Die fortschreitende Digitalisierung braucht vor allem **Mut** sich auf Neues einzulassen und das begründete **Vertrauen**, dass die neuen Möglichkeiten keine Rückschritte in Sachen Arbeitsschutz, Datenschutz, Freiheit und Schutz der Kommunikation mit sich bringen.

Das Verlassen alter, festgetretener Pfade, sich auf Neues, Unbekanntes einlassen, erfordert Mut, das wissen Sie alle hier so gut wie ich. Und dieser Mut erfordert vor allem Vertrauen, in sich selbst aber auch in die Entwickler, Entscheider, Umsetzer, Aufsichtsbehörden, Sicherheitsbehörden und Gerichte.

Ich will das kurz am Beispiel der Corona-Tracing-App und der Corona-Gästelisten verdeutlichen:

Wie Sie wissen, gab es zunächst zwei andere Ansätz als den heutigen für eine Corona-Warn-App. Der erste entsprang völlig aus altem Denken, vorhandene Daten einfach für einen anderen Zweck zu verwenden. Gestoppt, weil ungeeignet und unverhältnismäßig. Der zweite Ansatz, der von einem Konsortium unterschiedlicher Firmen und Institute aus mehrern Staaten angeschoben wurde. In diesem Konsortium gab es schon bald höchst unterschiedliche Auffassungen über die Ausgestaltung, es wurde über die Medien ein ziemlicher Kleinkrieg geführt, der nicht einen Schritt weiterführte. Mein Haus, der BfDI, hat viele Manntage personelle Ressourcen in diesen Prozess als begleitende Beratung investiert. Wir wurden dabei von Tag zu Tag skeptischer, weil neben unserer Präferenz für eine

datenschutzfreundlichere Architektur auch Bedenken dazukamen, dass die Projektsteuerung nicht funktionieren könnte.

Ich fand es ziemlich mutig, das das RKI und das Bundesgesundheitsministerium irgendwann die Reißleine gezogen haben und gesagt haben „Stopp, wir fangen nochmal neu an“. Dass RKI und BMG und auf Grund der vorausgegangen Diskussion entschieden haben, wir wollen einen dezentralen Ansatz und wir wollen von Anfang an Transparenz in der Entwicklung und der Datenschutz wird von vorneherein mitbedacht. Genau das wurde dann auch gemacht, meine Mitarbeiterinnen und Mitarbeiter in den beteiligten Referaten haben erneut über Wochen in Telefon- und Videokonferenzen mit den Entwicklern und dem RKI gesessen und jeden Schritt begleitet, beraten und Umsetzungsvorschläge gemacht.

Der Quellcode der App wurde der Öffentlichkeit zur Überprüfung zur Verfügung gestellt und ich kann mich noch gut erinnern, dass selbst der Vertreter des Chaos-Computer-Clubs einen Tag vor der Freischaltung der App sagte „sie könnten daran nichts kritisieren“. All das, davon bin ich fest überzeugt, hat dazu geführt, dass die Menschen in unserem Land das notwendige Vertrauen in die App hatten und haben, um sie millionenfach herunterzuladen und zu nutzen. Sie wird von mehr Menschen genutzt als alle anderen europäischen Apps zusammen. Damit wurde aus meiner Sicht für staatliche IT-Projekte ein neuer Goldstandard geschaffen. Vertrauen, nicht Daten sind das neue Öl im Zeitalter der Digitalisierung.

Und deswegen beim Thema der Corona-Gästelisten die Bitte an alle Sicherheitsbehörden: Bitte halten Sie sich beim Zugriff auf die Listen auch im Rahmen des gesetzlich Erlaubten zurück. Es setzt sich sonst, wie bei Maut, SteuerID u.a.m. der Eindruck fest, dass man den Zusagen des Staates, wofür Daten verwendet werden, nicht glauben kann. Das wäre fatal für das Verhältnis zwischen BürgerInnen und Staat sowie fatal für das Vertrauen in Digitalisierung.

III. Was folgt daraus, was muss sich ändern

Ich denk, wir müssen die richtigen Lehren aus den letzten Monaten ziehen und die lauten:

- Privacy by design
- Transparenz
- Weg mit alten Hüten, die nicht zur Zukunft passen

Wer mir schon öfter zugehört hat, kennt mein Mantra, das wirden Datenschutz von Anfang an mitdenken müssen. Das ist es ja, was mit „**privacy by design**“ gemeint ist. Sowohl Geräteherstellen wie auch Softwareentwickler wie auch Prozessverantwortliche müssen den Datenschutz und die Datensicherheit schon in den ersten Entwicklungsstufen mitdenken und umsetzen. Jeder von uns weiß doch, dass nachträglich hinzugefügte Teile, Aufgaben, Anforderungen nicht nur mehr Geld kosten, sondern auch zu mehr Fehlern führen.

Deshalb ist es so wichtig Datenschutz und Datensicherheit von Anfang an zu beachten. Wenn Sie so wollen, sind IT-Sicherheit und Datenschutz unmittelbar miteinander verzahnt – zwei Seiten derselben Medaille. Denn IT-Sicherheit soll den Missbrauch, unberechtigten Zugang und die unberechtigte Nutzung personenbezogener Daten ausschließen. IT-Sicherheitsrisiken sind damit regelmäßig auch Datenschutzrisiken. Alle Mehrwerte für IT-Sicherheit kommen deshalb auch dem Datenschutz zugute. Mit der Ausnahme, wenn die IT-Sicherheitsleute mal wieder große Sammlungen mit personenbezogenen Daten anlegen und auswerten wollen, um ihre Sicherheitsmechanismen zu verbessern.

Aus datenschutzrechtlicher Sicht ist der Anspruch auf **Transparenz** fundamental. Er wird explizit in Art. 5 Abs. 1 a) der Datenschutzgrundverordnung genannt. Im Kern geht es darum, dass eine betroffene Person nachvollziehen können muss, wie und von wem die sie betreffenden personenbezogenen Daten verarbeitet werden.

Dieses Wissen ist die Basis für eine selbstbestimmte Entscheidung über die Datennutzung. Denn nur mit dieser Transparenz kann es gelingen, die Kontrolle über die Verwendung eigener (personenbezogener) Daten zu behalten. Und diese Kontrolle ist eine zwingende Voraussetzung für den effektiven Schutz der eigenen Daten.

Meine Forderung nach mehr Transparenz geht aber noch darüber hinaus. Ich möchte Transparenz eben nicht nur im datenschutzrechtlichen Sinne, sondern auch im Sinne der vertrauensbildenden Maßnahmen verstanden wissen. Ob die Menschen die Corona-App nutzen, ob sie die elektronische Patientenakte und ihre Möglichkeiten nutzen, ob sie Gesundheitsdaten oder die ihrer Fahrzeuge „freigeben“ und nutzbar machen lassen, alles das hängt ganz wesentlich davon ab, dass die Gründe und Verfahren ihnen ordentlich und transparent erklärt werden und auch nur so genutzt werden, wie angegeben. Jeder Missbrauch von Daten, gerade im besonders sensiblen Gesundheitsbereich, wird zur Folge haben, dass die Menschen den Verantwortlichen und den Nutzern der Datensammlungen nicht vertrauen und ihre Daten sperren.

Wie komme ich jetzt zu den alten Hüten?

Die sichere Anonymisierung von personenbezogenen Daten ist in vielen Bereichen essentiell, um Vertrauen zu schaffen und den Menschen die datenschutzrechtliche oder politische Einwilligung zur Nutzung dieser Daten zu erleichtern.

Wenn dann aber zum gleichen Zeitpunkt aus anderen Politikfeldern so Scheintote wie „Verschlüsselungsverbot“ und „Vorratsdatenspeicherung“ wieder ins Licht gezerrt werden, dann frage ich mich schon, wie lange manche Entscheidungsträger auf Zukunftsfragen mit veralteten Lösungen antworten wollen. Willy Brandt hat einmal ganz richtig gesagt „jede Zeit braucht ihre eigenen Antworten“ und dies gilt gerade im Zeitalter der Digitalisierung.

Ich komme zum Schluss:

Wenn Deutschland und Europa anderen Wirtschaftsräumen bei der Digitalisierung hinterherhinken, dann fast nie, weil es Probleme mit Datenschutzvorschriften gibt, sondern weil Ressortdenken, Föderalismus oder Unterfinanzierung vorherrschen.

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

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

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

Ich danke Ihnen für Ihre Aufmerksamkeit.