# Digital, frei und gleich - Um was es geht

**Wenn ich die fünfeinhalb Jahre Arbeit mit meinem Team als Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) kurz zusammenfassen müsste, würde ich das wie folgt machen: Die Beratung für Digitalisierungsprozesse und Gesetzentwürfe, unsere Öffentlichkeitsarbeit, unser Engagement in europäischen und internationalen Gremien sowie der Einsatz der Instrumente als Kontroll- und Durchsetzungsbehörde hatten immer das Ziel, dass unsere Gesellschaft in der digitalen Transformation frei und gleich bleibt. Mehr noch, die Möglichkeiten der Digitalisierung aktiv dafür zu nutzen, dass Freiheit und Gleichheit zunehmen.**

Deswegen setze ich mich für eine grundrechtsgeleitete Digitalisierung ein. Deswegen lehne ich eine „Scheuklappen-Digitalisierung“ ab, bei der ohne Rücksicht auf die Auswirkungen nur auf die Umsetzung einer Funktionalität geschaut wird. Deswegen bekämpfe ich die demokratiegefährdenden Geschäftsmodelle des Überwachungskapitalismus. Deswegen werbe ich dafür, dass die digitalen Überwachungsbefugnisse von Sicherheitsbehörden und Nachrichtendiensten verhältnismäßig bleiben. Und deswegen habe ich immer wieder angemahnt, dass die Prozesse von politischen Entscheidungen hin zur digitalen Umsetzung sich völlig verändern müssen. Zumal der deutsche Föderalismus sich bisher bei der Digitalisierung des Staates eher nachteilig auswirkt, wie zuletzt die Vorgänge um das Online-Zugangsgesetz 2.0 gezeigt haben.

In den fünfeinhalb Jahren, die ich Bundesdatenschutzbeauftragter sein durfte, hat sich die Behörde massiv verändert. Dieser Umbau war notwendig, um mit der sich weiter beschleunigenden digitalen Transformation Schritt halten zu können. Ich blicke mit Stolz auf diesen gelungenen Prozess.

Prof. Ulrich Kelber war von 2019 bis 2024 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit. 2000 bis 2019 war er Mitglied des Deutschen Bundestages und Parlamentarischer Staatssekretär beim Bundesminister der Justiz und für Verbraucherschutz von 2013 bis 2018.

Kelber studierte Informatik (Vertiefungsgebiet Künstliche Intelligenz) mit Nebenfach Biologie (Genetik, Mikrobiologie). Von 1991 bis 1995 war er Mitarbeiter bei der Gesellschaft für Mathematik und Datenverarbeitung (heute Teil der Fraunhofer-Gesellschaft). Als Wissensmanagement-Berater war er von 1996 bis 2000 in einem mittelständischen IT-Unternemen tätig.

Manche Veränderung folgte auf neue Aufgaben, die der deutsche oder der europäische Gesetzgeber dem BfDI übertragen hat. Dabei bin ich dem Deutschen Bundestag sehr dankbar, dass er diese Aufgaben immer mit den entsprechenden Ressourcen, insbesondere auch den notwendigen Stellen, verbunden hat, ganz im Gegensatz zu anderen Parlamenten in Deutschland und der EU.

Der Anstoß zur Modernisierung der Strukturen und Verfahren beim BfDI kam jedoch vor allem aus der Behörde selbst. Wir haben beispielsweise im großen Maßstab zusätzliche technische Kompetenz aufgebaut. 2019 gab es ein technisches Referat und zwei Referate, in denen technische Fragen eine wichtige Rolle spielten. Heute ist daraus eine ganze „technische Abteilung“ mit acht Referaten geworden. Dazu kommen viele weitere technisch ausgebildete Kolleg:innen, integriert in den Fachreferaten der anderen Abteilungen.

Der BfDI hat seit 2019 einen deutlichen Zuwachs an Mitarbeitenden erfahren, heute sind es 360 Kolleg: innen in 30 Referaten. Das ermöglicht es uns, mehr Themen zu bearbeiten, eingereichte Beschwerden und Meldungen schneller zu verfolgen, besser zu beraten und insgesamt unsere Arbeit zu intensivieren. Übrigens sind noch offene Stellen zu besetzen. Wenn Sie also auf die „helle Seite der Macht“ kommen und sich für Grundrechte einsetzen wollen, nur zu, bewerben Sie sich gerne.

Die von uns beaufsichtigten Behörden und Unternehmen haben diese verbesserte Arbeitsfähigkeit erleben können, durch mehr Kontrollen, aber eben vor allem durch mehr und bessere Beratung. Unser messbarster Erfolg ist dabei ein Rückgang von Beschwerden und Datenschutzpannen bei beaufsichtigten Stellen mit einer besonders hohen Zahl gleichartiger Bearbeitungsfälle, also Jobcenter, Finanzämter, Telekommunikations- und Postdienstleistungsunternehmen, sowie — mit ein paar Einschränkungen — gesetzliche Krankenversicherungen und auch einige Bundesbehörden.

**Wir sind Fans der Digitalisierung**

Anders als oft unterstellt sind wir in den Datenschutzaufsichtsbehörden keinesfalls Gegner, sondern vielmehr Fans der Digitalisierung. Wie sollte es bei mir selbst als Informatiker auch anders sein, ich hatte mir mein Studienfach ja gerade aus Faszination am technischen Fortschritt ausgewählt?

Ich bin fest davon überzeugt, dass gut gemachte digitale Lösungen das Leben erleichtern, neue Erkenntnisse generieren, neue Möglichkeiten schaffen und sogar den Datenschutz verbessern helfen. Das alles geht, wenn die elende Zettelwirtschaft aufhört und nur die Daten ausgetauscht werden, die wirklich benötigt werden, statt z.B. Personalausweise zu kopieren oder Faxe zu versenden.

Apropos Fax: Wir Datenschützer:innen hassen Faxgeräte. Sie sind ein Symbol des Medienbruchs, der verlangsamt und fehleranfällig ist. Deswegen habe ich Faxgeräte beim BfDI schlicht abgeschafft.

Stattdessen haben wir als erste oberste Bundesbehörde schon 2019 konsequent auf die elektronische Akte und durchgängig digitale Meldewege gesetzt. Zusammen mit der frühzeitigen Umstellung aller Arbeitsplätze auf Laptops konnten wir daher auch sofort bei Beginn der COVID-Pandemie auf Home-Office umstellen. Manche, die uns beim BfDI als Bremser der Verwaltungsdigitalisierung verunglimpfen, haben bis heute noch nicht einmal diese Basisschritte bewältigt, während wir längst schon weiterdenken. Bis hin zur KI-Unterstützung unserer Mitarbeitenden zur schnelleren Bearbeitung von zuletzt 7.782 Bürger:innen-Eingaben und 9.263 Meldungen von Datenpannen im Jahr.

Der weit überwiegende Teil unserer Arbeit als Datenschutzbehörde besteht übrigens aus Beratung. Bei dieser Beratung zeigen wir auf, wie Prozesse digitalisiert werden können und welche zusätzlichen Datennutzungen grundrechtskonform möglich sind. Es war deshalb für mich immer frustrierend, wenn auf unsere Beratung nicht gehört und mit der Brechstange eine schlechte Digitalisierung durchgesetzt wurde. Oder sogar auf eine notwendige Digitalisierung verzichtet wurde, mit der faule Ausrede angeblicher Datenschutzhürden.

Der schlimmste Fall war in diesem Zusammenhang die lange verzögerte Einführung von Cell Broadcasting als schnelle Warnmöglichkeit bei Katastrophen. Cell Broadcasting erreicht alle eingeschalteten Mobilfunkgeräte in einem Gebiet, ohne dass man auf Apps oder eine gute Internetverbindung oder ein neues Gerät angewiesen ist, quasi wie eine SMS. Unsere Nachbarländer hatten bei dem Starkregen 2021, der u.a. in der Eifel und dem Ahrtal zu verheerenden Überflutungen führte, ihre Bevölkerung per Cell Broadcasting noch rechtzeitig warnen können, während in Deutschland die versuchten Warnungen per App die Menschen oft schlicht nicht erreichten.

Als es dann zur Debatte kam, warum es denn in Deutschland kein Cell Broadcasting gebe, schob der damalige Minister Andreas Scheuer den Datenschutzaufsichtsbehörden den Schwarzen Peter zu.[1] Nie war ich über einen politischen Winkelzug so wütend, gerade auch weil wir in Bonn alle viele Bekannte und Kolleg:innen im nahen Ahrtal haben, die Angehörige betrauern oder den Verlust ihres Hauses verkraften mussten. Denn das genaue Gegenteil der Scheuerschen Behauptung ist wahr: Sowohl meine Amtsvorgänger:innen als auch ich hatten die Bundesministerien immer wieder davor gewarnt, einseitig auf Apps zu setzen und die (Wieder-)Einführung von Cell Broadcasting angemahnt. Denn Cell Broadcasting ist nicht nur die zuverlässigste und schnellste Warn-Technologie, sondern auch die datenschutzfreundlichste.

**Zusammenarbeiten statt Goldplating**

Wie oft musste ich mir anhören, dass alle andere Datenschutzaufsichtsbehörden in Europa so pragmatisch seien und nur wir in Deutschland die Datenschutzgesetze besonders streng auslegen. Bei den monatlichen Treffen in Brüssel mit meinen europäischen Kolleg:innen sorgte das für viel Gelächter. Denn sie alle bekommen in ihren Heimatländern genau den gleichen Spruch zu hören.

Im Ernst: Geltendes Recht ist verbindlich und muss eingehalten werden. Allerdings nicht als „Goldplating“, also besonders datenschutzfreundliche Lösungen ausschließlich in Deutschland. Ich will vielmehr eine einheitliche Praxis der Datenschutzaufsicht in Europa. Das schafft einerseits Rechtssicherheit für Unternehmen und Behörden. Andererseits folgt daraus eine große Durchsetzungsstärke für die Rechte der Bürger:innen.

Deswegen habe ich mich für eine enge Zusammenarbeit mit den Landesdatenschutzbeauftragten eingesetzt. Außerdem haben meine Mitarbeiter: innen und ich viel Zeit und viel Arbeit im Europäischen Datenschutzausschuss (EDSA) und seinen Gremien investiert. Dies hat sich gelohnt: Immer mehr Rechtsauslegungen werden veröffentlicht, wichtige Datenschutzfälle abgeschlossen und die Betroffenenrechte, wenn nötig, auch mit hohen Bußgeldern durchgesetzt.

Zahlreiche Federführungen, Berichterstatter- und Koordinierungsfunktionen des BfDI in der Deutschen Datenschutzkonferenz (DSK) und im EDSA haben in den letzten Jahren geholfen, dass diese Institutionen leistungsfähiger wurden. Mit unserem Engagement, das allein 2023 die Teilnahme an 350 Gremiensitzungen auf europäischer Ebene bedeutete, haben wir auch geschafft, deutsche Rechtstraditionen einzubringen. Das ist ein nicht zu unterschätzender Wettbewerbsvorteil für deutsche Unternehmen.

Dazu kommen zahlreiche weitere internationale Gremien und Institutionen, wie die Global Privacy Assembly (GPA), die International Conference of Freedom of Information Commissioners (ICIC), die OECD, der Europarat, die Global Platform on Enforcement und nicht zuletzt unsere beratende Funktion für ein globales Datentransfer-Abkommen von Staaten außerhalb der EU (Global CBPR), übrigens als einzige Datenschutzaufsichtsbehörde aus der EU. In GPA und ICIC war ich Mitglied im Executive Committee, also dem Vorstand.

Ein freier Datenverkehr zwischen den demokratisch regierten Ländern der Welt, der Wettbewerb und Innovation stärkt und gleichzeitig Vertrauen durch hohe Datenschutzstandards schafft: Dieses Ziel haben wir mit unserer Unterstützung im Format des G7 Roundtable der Datenschutzaufsichtsbehörden der USA, Kanadas, Japans, Großbritanniens, Frankreichs, Italiens und Deutschlands vorangetrieben. Das erste persönliche Treffen fand 2022 auf meine Einladung hin in Bonn statt und war so erfolgreich, dass das Format als Teil des G7-Gipfel- Prozesses institutionalisiert wurde und nun jährlich stattfindet. Zwischen den Treffen im Roundtable- Format wird in virtuell organisierten Arbeitsgruppen an Positionspapieren geschrieben, die Diskussionen bei den Digitalminister:innen der G7 und in anderen Institutionen anregen sollen.

Besonders stolz bin ich auch auf die Ergebnisse aus der Leitung der International Working Group on Data Protection in

1 https://www.bild.de/politik/inland/politik-inland/nach-warn-desaster-bei-der-todesflut-scheuer-fordert-katastrophen-warnung-persm-77135752.bild.html

Technology (sogenannte Berlin- Group) die meine Behörde innehat. Die Gruppe, zusammengesetzt aus NGOs, Wissenschaftler:innen und Datenschutzaufsichtsbehörden von allen Kontinenten, gibt seit ihrer Gründung sehr praxisnahe Empfehlungen, worauf Anbietende, Gesetzgebende, Nutzende und Aufsichtsbehörden beim Einsatz einer Technologie achten sollten. Zusätzlich haben wir in der Berlin-Group und beim BfDI ein Future Foresight Programm für Technologien geschaffen, bei denen wir einen Markteintritt in den nächsten Jahren erwarten. Hier sprechen wir frühzeitig Empfehlungen aus, um „privacy by design“ und „security by design“ zu erreichen.

Der Umfang dieser internationalen Kooperationen ist im Verhältnis zur Größe meiner Behörde immens und die Erfolge hart erarbeitet. Doch ist es der beste Weg, um Freiheit und Gleichheit in einer globalisierten Welt zu schützen und zu fördern. Denn die neuen Herausforderungen sind längst da.

**Von KI und PETs und gefährlicher Beharrung**

Ich hatte das Glück, schon ab 1989 in meinem Informatik- Studium und anschließend in meiner Arbeit in einer KI-Forschungsgruppe, deren Schwerpunkt Neuronale Netze, Genetische Algorithmen und andere spannende Technologien waren, mit exakt den Themen in Berührung zu kommen, die uns jetzt, Mitte der 2020er Jahre, so umtreiben.

KI wird die Digitalisierung noch einmal wesentlich beschleunigen, gigantische neue Möglichkeiten eröffnen, aber auch neue Risiken schaffen. Beim BfDI haben wir diese Herausforderung angenommen, längst beraten wir die von uns beaufsichtigen Behörden und Unternehmen auch beim Thema KI.

Eine menschenzentrierte KI „made in Europe“ ist möglich, ohne im Wettbewerb der globalen Wirtschaftsregionen (noch weiter) zurückzufallen. Eine hohe Rechtssicherheit durch Beratung von Aufsichtsbehörden für Anbieter und Unterstützung bei der Produktentwicklung ist eine Stärke, die es zu nutzen gilt.

KI ist eine Herausforderung für Datenschutzrecht und Datenschutzaufsichtsbehörden. So wie KI auch für viele andere gesellschaftlichen Bereiche und viele andere Rechtsfragen eine große Herausforderung darstellt, wenn man nur an Haftungsfragen und Urheberrecht denkt. KI muss rechtskonform eingesetzt werden, daran führt kein Weg vorbei. Aber selbstverständlich werden sich auch Prinzipien des Datenschutzes weiterentwickeln müssen, um in einer KI-geprägten Welt noch zu funktionieren und akzeptiert zu werden. Insbesondere Zweckbindung und Datenminimierung müssen als Grundprinzipien unbedingt erhalten bleiben. Aber sie brauchen auch eine Weiterentwicklung, z.B. bei der Nutzung von Daten zu Trainings- und Testzwecken oder für die Datenverarbeitung in besonders gesicherten Umgebungen, z.B. Forschungsdatenoder Mikrodatenzentren.

Worauf wir alle wirklich nicht hören sollten, sind die Stimmen, die Grundrechte schleifen, Beschäftigtendatenschutz verringern und eine dauerhafte Überwachung der Bürger:innen durch Privatunternehmen ermöglichen wollen, nur damit ein „anything goes“ eventuell zur Gründung von KI-Start- Ups und verstärktem KI-Einsatz führt. Das würde unsere Gesellschaft sehr zum Negativen verändern.

Und es ist auch nicht nötig: Die meisten KI-Anwendungen sind aus Datenschutzsicht unkritisch, kommen ohne personenbezogene Daten aus. Bei einigen müssen allerdings Entwickler:innen und Anwender:innen verstärkte Sorgfalt an den Tag legen, sei es bei der Modellierung des Systems, der Auswahl der Trainingsdaten, dem Monitoring des Systems oder Schutzmaßnahmen für personenbezogene Daten. Nur wenige KI-Anwendungen brauchen eine enge Begleitung durch Aufsichtsbehörden und das immer wieder thematisierte Verbot bestimmter Anwendungen wird nur eine verschwindend kleine Zahl betreffen.

Was ich mir überhaupt wünsche: Wenn nicht nur immer schnellere Computer und immer mehr Daten eingesetzt würden, sondern auch konsequent solche Technologien, die gleichzeitig mehr Nutzung von Daten und einen besseren Datenschutz ermöglichen. Wir nennen das Datenschutz durch Technik.

Dabei meine ich grundlegende Methoden wie Verschlüsselung, Signierung, Pseudonymisierung, Anonymisierung sowie gute Rechte- und Rollenkonzepte. Es ist ermüdend, diese bei Digitalisierungsprojekten immer wieder einfordern zu müssen, obwohl sie doch schon lange etabliert sind. Hier wünsche ich mir mehr Unterstützung durch Wirtschaftsverbände und Politik, um die Akzeptanz der Bürger:innen bei der Digitalisierung zu sichern.

Für mehr Datennutzung bei starkem Datenschutz stehen längst weitere spannende Technologien bereit, die so weiterentwickelt werden sollten, dass sie in Programmbibliotheken und Cloud Services für alle verfügbar sind. Ich spreche von privacy enhancing technologies, kurz PETs.

Unter PETs fallen Ansätze wie homomorphe Verschlüsselungen, wo personenbezogene Daten für ihre Verarbeitung nicht entschlüsselt werden müssen. Oder multiparty computing, wo die Daten an verschiedenen Stellen verbleiben, dort auch verteilt verarbeitet werden und am Ende alle Beteiligten vom Ergebnis profitieren, ohne die Daten der anderen zu kennen. Dazu kommt förderales Lernen, z.B. wenn eine KI jeweils lokal auf Millionen Wearables arbeitet, dort die lokalen Daten für die Inhaber:innen analysiert, hinzulernt und nur diese Verbesserung der Analysequalität mit den anderen teilt. Es wäre so schön, wenn der Staat bei Projekten die Nutzung solcher spannenden Technologien vorschreibt, statt z.B. bei der elektronischen Patentenakte (ePA) Verschlüsselungen abzuschaffen, damit PDF-Dateien durchsucht werden können.

**Digitalisierung des Staates neu denken**

Überhaupt habe ich bei allen sich bietenden Gelegenheiten eines immer wieder betont: Deutschland ist gefährlich unterdigitalisiert. Diese Warnung gilt vor allem für die Digitalisierung des Staates und anderer öffentlicher Bereiche. Mit einem

allzu oft zur Kleinstaaterei mutierten Föderalismus (z.B. vierzehn Krankenhaus-Gesetze mit unterschiedlichen Regelungen zur Digitalisierung, dutzende Projekte zur IT-Umgebung in Schulen oder ein Online- Zugangsgesetz ohne gemeinsame Standards), anhaltender Unterfinanzierung und fehlendem konsentiertem Plan, was zuerst getan werden muss als Basis für weitere Schritte, wird es mit dem Aufholen allerdings sehr schwierig.

Immer wieder müssen wir erleben, wie lange gar nichts passiert und dann mit Hauruck-Methoden eine schlechte Digitalisierung und rechtswidrige Datennutzungen etabliert werden, auch weil man die Beratung von BfDI und BSI nicht wirklich in Anspruch nimmt. Wie die lange Unterfinanzierung der Digitalisierung zu Verzögerungen führt, so dass am Ende auf die Nutzung anderswo längst eingeführter Sicherheitstechnologien verzichtet wird. Und der Unwille, als Staat einheitliche Datenformate, durchgängige digitale Übertragungswege und hohe Sicherheitsstandards vorzugeben und durchzusetzen, wird mir immer ein Rätsel bleiben.

Wenn die angebotene frühe Beratung nicht in Anspruch genommen und erst spät der Kontakt zu BfDI (und BSI) gesucht wird, dann ist die Gegenseite leider oft nur auf einen schnellen (politischen) Teilerfolg aus. Die Scheuklappen, die die politische Verantwortlichen dann zu diesem späten Zeitpunkt des Projektes anlegen, führen in der Konsequenz zur Ablehnung alternativer, technisch ausgereifterer, sicherer und datenschutzfreundlicherer Umsetzungsmöglichkeiten.

Nicht selten kippen als Konsequenz übrigens Gerichte ganze Projekte, die solche alternativen Umsetzungsmöglichkeiten ungenutzt lassen. Der Verlust an Zeit und Geld ist dann immens. Eine von Anfang an auf guten Datenschutz und hohe IT-Sicherheit ausgerichtete Digitalisierung ist damit am Ende schneller und preisgünstiger, selbst wenn sie zu Beginn zunächst mehr Aufwand und Vorbereitung für die Beteiligten bedeutet.

Der eigentliche Grund hinter dieser Verweigerungshaltung ist wohl, dass zahlreiche etablierte politische Prozesse nicht kompatibel sind mit den Anforderungen der Digitalisierung. Getrieben durch externe Erwartungshaltung, oft nach einer Krise oder einem Skandal, ist für eine kluge und umfassende Digitalisierungsplanung nicht ausreichend Zeit. Umgekehrt wird an vielen Projekten nicht mehr weitergearbeitet, wenn der öffentliche Druck oder die Aufmerksamkeit von Parlamenten und Medien nachlässt.

Wenn in politischen Diskussionen, Arbeitskreisen, Koalitionen oder im Vermittlungsausschuss mühsam nach Kompromissen gesucht werden muss, dann wird leider oft zu wenig mitbedacht, was sich denn digital umsetzen ließe und was nicht. Welche Daten stehen z.B. für eine automatische Bearbeitung zur Verfügung und auf welche Sonderregelungen sollte man verzichten, um nicht einen riesigen Aufwand zur Datenerhebung und manuellen Bearbeitung zu erschaffen? Wo müssen unterschiedliche Lösungen standardisiert werden, um überhaupt interoperabel zu sein und die vorhandenen Daten auch austauschen zu können?

Daher mein Hauptplädoyer: Während Gesetzgebung heute oft nach wie vor als ressortinternes Geheimprojekt abläuft, bei dem sich auf vielen Stufen abgesichert wird (auch aus Angst vor verzerrter medialer Darstellung) und Beratungsinstitutionen erst (zu) spät beteiligt werden, müssen die Digitalisierungsvoraussetzungen in Zukunft zu Beginn der Projekte bedacht werden. So fordert es ja eigentlich auch der eingeführte Digital-Check des Nationalen Normenkontrollrats.

Die Voraussetzungen dafür sind gut, denn BSI und BfDI beraten absolut vertraulich. Niemand muss Angst davor haben, eine schlechte Idee nicht wieder unbemerkt begraben und eine neue Richtung einschlagen zu können. Hier müssen die Prozesse in den Behörden vollständig neu ausgerichtet, die Beteiligung der Beratungsinstitutionen zum frühestmöglichen Zeitpunkt zum Standard werden.

Um als BfDI unser Beratungsangebot weiter verbessern zu können, haben wir es in den Mittelpunkt unserer Strategie gestellt. Mit der Vision „Wir sind gefragte Ansprechpartner für alle Fragen von Gesetzgebung und Digitalisierung …“ haben wir unsere Arbeit so ausgerichtet, dass wir rechtlich und technologisch beraten können, dass wir verbindliche Antworten auf Fragen geben und nicht zuletzt sogar unsere Kontrollen gleichzeitig auch immer Beratungs- und Informationsbesuche sind. Damit unsere Beratung als Vorteil und nicht als Einschränkung wahrgenommen wird.

**Sicherheit und Freiheit sind vereinbar**

Man muss einfach immer wieder eine Lanze für die Mitarbeiter:innen brechen, die in den Sicherheitsbehörden und den Nachrichtendiensten Deutschlands tätig sind. Sie werden täglich mit erschreckenden, aber durchaus realistischen Bedrohungsszenarien konfrontiert. Sie müssen die Beweismittel auch der widerwärtigsten Straftaten sichern. Und sie müssen eine (unnötigerweise) unzureichende Ausstattung sowie auch (notwendige) gesetzliche Grenzen für ihre Werkzeuge zur Abwehr und Aufklärung hinnehmen.

Vorneweg auch noch dies: Sind die Grenzen für die Werkzeuge und Arbeitsformen einmal unmissverständlich geklärt, sei es durch Gesetze, Gerichtsurteile oder unsere Beratungsarbeit, werden diese nach meiner Erfahrung bis auf wenige Ausnahmen akzeptiert und respektiert. Nicht selten wird durch die Behörden und die jeweiligen Mitarbeiter:innen ein hoher Aufwand betrieben, um die Grundrechte der Bürger:innen zu wahren.

Es ist allerdings die vom Gesetzgeber und dem Bundesverfassungsgericht vorgesehene Aufgabe für die Datenschützer:innen, die Einhaltung der bestehenden Gesetze bei den Sicherheitsbehörden und Nachrichtendienste zu überwachen, die seit den Anschlägen vom 11. September 2001 so massenhaft geschaffenen zusätzlichen Überwachungswerkzeuge zu hinterfragen sowie auf die Gefahren einer immer dichteren und tiefgreiferenden Überwachung der Bürger:innen hinzuweisen.

Wenn nämlich jedes Wort, jeder Schritt, jede Handlung und umgekehrt sogar das Unterlassen von durch Datenauswertung eigentlich vorhergesagter Kommunikation, Bewegungsmuster und Aktionen ausgewertet werden, dann stirbt die Freiheit. Das Bundesverfassungsgericht hat das richtig analysiert: Schon das Gefühl beobachtet zu werden, kann einem daran hindern, seine Freiheitsrechte auszuüben. Wenn man sich immer beobachtet fühlen muss, was löst das aus? Gehen wirklich noch alle auf Demonstrationen, wenn ihre Anwesenheit dort stets gefilmt und durch Gesichtserkennung festgehalten wird? Redet man noch offen über alles, wenn jeder Halbsatz ausgewertet und in neue Zusammenhänge gestellt werden könnte?

Deutschland benötigt eine Überwachungsgesamtrechnung, wie sie BfDI und DSK schon so oft gefordert haben. Und wie sie im Koalitionsvertrag vereinbart ist. Damit klar wird, wie stark die Menge der einzelnen Überwachungsmaßnahmen schon in die Grundrechte eingreifen und nicht immer nur die einzelne Maßnahme bewertet wird. Damit bei einzelnen Werkzeugen für die Auswertung von Daten und der Überwachung von Verhalten evaluiert wird, welchen Beitrag diese wirklich für die Sicherheit leisten und wie stark dafür in die Freiheitsrechte der Bürger:innen eingegriffen wird. Denn seit 2001 kennt die Gesetzgebung nur eine Richtung: Mehr Überwachung und Ausweitung einmal ergriffener Maßnahmen. Ohne den — wegen den meist übereilten Gesetzgebung häufigen — Eingriffen der Gerichte wäre keine einzige Maßnahme wieder aufgehoben oder eingeschränkt worden.

Im Gegenteil: Oft genug wird die Eingriffstiefe von Überwachungsmaßnahmen als Reaktion auf Berichte über Anschläge oder (vermeintliche) Kriminalitätsentwicklungen massiv ausgeweitet, obwohl noch nicht einmal die im Gesetz vorgeschriebene Evaluation, ob die Maßnahme wirklich positive Ergebnisse gebracht hat, überhaupt begonnen wurde. Und das selbst in Bereichen, wo sowohl die Kriminalitätsrate rückläufig ist, als auch andere Vorgehensweisen erfolgversprechender wären. Was nutzt die Ausweitung der Telefonüberwachung bei Einbrüchen, wenn nicht einmal mehr verlässlich Spuren vor Ort gesichert werden, um später Taten miteinander in Zusammenhang zu bringen? Und wäre nicht ein Förderprogramm sinnvoller, um Wohnungen in Mehrfamilienhäuser mit sicheren Türriegeln zu versehen, denn daran scheitern die meisten Täter:innen schon?

Die Überwachung von immer mehr Kommunikation in sozialen Netzwerken und bei Messengern wird von denen gefordert, die Datenschutz als „Täterschutz“ diffamieren, gerade auch bei Hassrede und Beleidigungen. Aber wo sind denn die Stellen, bei denen sich Geschädigte oder Zeugen überhaupt mit einer Anzeige hinwenden können? Wo sind ausreichend Spezialist:innen und die notwendige Ausrüstung, um die verschiedenen, oft getarnten Accounts der Täter:innen zusammenzuführen, um so auf ihre Identität zu schließen?

Ich bin überzeugt, dass Freiheit, im Sinne der Freiheit von staatlicher Überwachung, und Sicherheit miteinander vereinbar sind. Wenn transparente und verhältnismäßige Gesetze die Arbeit gut ausgestatteter Sicherheitsbehörden und Nachrichtendienste regeln. Wenn es eine starke und unabhängige Aufsicht wie den BfDI gibt, die nicht als Hindernis verstanden wird, sondern gerade auch als Kompensation und Legitimation für die zwangsläufig meist verdeckt stattfindende wichtige Arbeit der deutschen Sicherheitsbehörden und Nachrichtendienste. Wenn alle möglichen Maßnahmen zur Erhöhung der Sicherheit betrachtet werden und nicht immer nur der scheinbar einfache Weg von mehr Überwachung gewählt wird. Und wenn Überwachung, die sich als ineffizient herausgestellt hat oder für die es Alternativen gibt, aktiv von staatliche Seite zurückgenommen wird.

**Gegen den Überwachungskapitalismus**

Mindestens genauso wichtig wie der Kampf gegen überzogene staatliche Datensammlung ist der Kampf gegen den umfassenden Überwachungskapitalismus der Tech-Giganten und Datenhändler.

Natürlich stehen diesen Firmen nicht staatliche Repressionsmaßnahmen wie Gefängnis oder Geldbußen zur Verfügung. Aber die Datensammlung zur Profilbildung von allen Bürger:innen hat längst eine Dimension angenommen, die unsere freiheitliche Demokratie aufs Äußerste gefährdet. Diese Datensammlung und die Profilbildung schaffen Möglichkeiten zur wirtschaftlichen Ausbeutung, Diskriminierung, Marktverzerrung und Manipulation. Vor allem aber fördern die auf diese Überwachungsmethoden aufbauenden Geschäftsmodelle längst die Radikalisierung der Gesellschaften weltweit.

Was war das noch für eine Zeit in den 1990er Jahren, als wir alle glaubten, mit dem Internet käme die große Freiheit und Gleichheit, würden kleine Inhalts- und Serviceanbieter sowie zivilgesellschaftliche Organisationen gleichberechtigt neben großen Firmen bestehen können. Dann aber haben sich die Datenkraken des Internets bemächtigt, Digitalisierung und Ausspähen gleichgesetzt, und viel zu vielen eingeflüstert, dass ohne die allumfassende Datensammelei die ganze Digitalisierung nicht bezahlbar und nicht machbar sei.

Dabei geht es bei der Kritik am Überwachungskapitalismus nicht darum, ob einem „auf Sie zugeschnittene Angebote“ oder „auf Sie passende Anzeigen“ im Internet angezeigt werden. Das Grundübel ist vielmehr, dass diese umfassende Sammlung der Daten Methoden nutzt, die unsere freiheitliche Gesellschaft unterminieren und einigen wenigen Akteuren immens große Macht zur Manipulation in die Hand geben.

Und deswegen werden alle politischen Bemühungen, die großen Plattformen zu zähmen, sie zur mehr gesellschaftlicher Verantwortung zu zwingen und Radikalisierungstendenzen im Netz zu bekämpfen, maximal begrenzte Erfolge aufzeigen. Es sei denn, man bekämpft das Grundübel, das Sammeln von personenbezogenen Daten, die für die Bereitstellung eines Services nicht benötigt werden, sowie die Nutzung bereits gesammelter Daten für andere Zwecke. Also das „Bezahlen mit persönlichen Daten“, wie es oft genannt wird.

Um möglichst viele dieser Daten sammeln zu können, werden die Menschen möglichst lange und möglichst eng an die je-

weiligen Services der Unternehmen gebunden. Auch die Verleitung zu möglichst vielen Interaktion durch hohe Emotionalität oder Bedienen des Belohnungsgefühls dient dazu. Ob das dann suchtsteigernd wirkt wie bei Tik-Tok oder wie beim Meta- und X/Twitter-Algorithmus radikale Inhalte und Fake News befördert, weil diese die Nutzer:innen besonders emotional berühren, ist den Leitungen dieser Unternehmen am Ende egal, wenn nur die Kasse stimmt und an der Börse weiter Wachstum vermeldet werden kann.

All das wäre zu Ende, wenn Meta, Tik-Tok & Co. nur die wirklich für den Service benötigten Daten sammeln und selbst diese nicht mehr an Dritten weitergeben dürften. Ihre Macht zur Manipulation, sei es für den chinesischen Staat oder ihre Shareholder, würde sofort sinken. Mit der Datenschutz- Grundverordnung gibt es dafür schon eine gute Regelung, die ergänzt und deren Durchsetzung politisch unterstützt werden muss.

Damit das noch einmal gesagt ist: Es gibt keine aus Sicht der informationellen Selbstbestimmung absolut unkritischen personenbezogenen Daten. Natürlich ist ein einzelnes Datum in der Regel für sich unproblematisch, wenn es nicht schon direkt eine schützenswerte persönliche Eigenschaft darstellt. Aber die Datenkraken sammeln tausende solche Daten, kombinieren diese und erhalten ein persönliches Profil, dass unser Verhalten ausleuchtet und leider auch extrem gut voraussagt.

Diese Profile sind so umfangreich und aussagekräftig, dass sich natürlich längst die Sicherheitsbehörden vieler Staaten der Datentöpfe der Privatunternehmen bedienen und dabei Einblicke gewinnen, die staatliche Maßnahmen eigentlich nicht erlauben und die unverhältnismäßig sind.

Die Profile der großen Tech-Firmen und der Datenhändler werden täglich umfangreicher und detaillierter, weil die Datenquellen zunehmen, seien es Apps, Betriebssysteme, Kameras, Online-Konten oder Sensoren. Deswegen sind Ansätze wie „Datensouveränität“, „data literacy“ oder „risikobasierte Ansätze“ nicht geeignet, Grundprinzipien des Datenschutzes wie Zweckbestimmung und Datenminimierung zu ersetzen, sie können diese maximal ergänzen.

Die rechtliche Durchsetzung dieser vom Gesetzgeber beschlossenen Grundprinzipien sollte stattdessen sogar verstärkt werden. Dazu müsste der Grundsatz gesetzlich verankert werden, dass jegliche Profilbildung, ob privatwirtschaftlich oder staatlich, nur auf einer Rechtsgrundlage wie einer informierten, freiwilligen Einwilligung oder einer klaren gesetzlichen Regelung erfolgen darf.

Zumindest die EU versucht im digitalen Raum Regeln durchzusetzen, u.a. mit dem Digital Services Act, der KI-Verordnung oder auch dem Digital Markets Act. Die großen Anbieter müssen zur Rechtskonformität ihrer Angebote und vor allem auch zur Interoperabilität gezwungen werden, damit neue Unternehmen überhaupt Chancen mit innovativen und durchgängig rechtskonformen Angeboten haben. Dies ist aus meiner Sicht auch die einzige Chance, das Übergewicht US-amerikanischer und chinesischer Anbieter jemals wieder auszuhebeln.

Äußerst dankbar bin ich deshalb dem deutschen Bundeskartellamt und seinem Präsidenten, Andreas Mundt. Es nimmt in Europa und weltweit eine Schrittmacherrolle dabei ein, die ungehemmte Datensammlung von Großkonzernen zu verhindern. Diese Cross Sector Regulierung, die Zusammenarbeit zwischen Regulierungsbehörden, ist ein zunehmend wichtigeres Thema, dass wir als BfDI auf allen internationalen Ebenen einbringen.

Die Notwendigkeit einer engeren Zusammenarbeit war der Anstoß für die Gründung des Digital Cluster Bonn aus BfDI, BSI, Bundeskartellamt, BAFin, Bundesnetzagentur und Bundesamt für Justiz. Andere Staaten brauchen dafür Gesetze und in Großbritannien wurde sogar eine Koordinierungsbehörde geschaffen. In Bonn haben die „Digitalbehörden“ des Bundes auf Anregung des BfDI das Thema in die eigene Hand genommen.

Im Kampf gegen den Überwachungskapitalismus braucht es aber auch die nachhaltige Unterstützung von Regierungen und Parlamenten. Diese sollten selbst bei der Nutzung von Produkten und Services als Vorbild vorangehen und nicht noch zum Komplizen der Datenkraken werden. Das gilt im Großen, wenn Facebook-, TikTok- Twitter-/X oder Instagram-Auftritte dazu führen, dass alle Nutzungsdaten von den Datenkraken gesammelt werden: Für welche Inhalte interessieren sich die einzelnen Bürger:innen, wo regen sie sich besonders auf (Teilen, Schreibfehler, Kommentare), etc. Alles das darf der Staat den Datenkraken doch nicht noch auf dem Silbertablett servieren.

Und es geht bis ins Detail: Warum nutzen staatliche Websites und Apps immer wieder Services der Datenkraken, die am Ende Standortdaten, Interessensgebiete und eventuell sogar Kommunikationsinhalte der Bürger:innen bei der Nutzung staatlicher Angebote und Apps an diese Firmen übertragen? Als BfDI haben wir so oft beraten, wie man diese Angebote anders gestalten kann, investieren gemeinsam mit den Behörden viel Zeit, diese nachträglich rechtskonform zu gestalten, um dann eine Woche später beim nächsten Projekt die gleichen Muster und Fehler wieder vorzufinden.

Besonders gefährlich wird es dann, wenn aus der Politik (und aus den Medien) die Forderung kommt, rechtlich besonders problematische Angebote ohne Einschränkungen nutzen zu dürfen. So wurde zuletzt lautstark verlangt, die aus meiner Sicht völlig rechtswidrig zusammengeklau(b)te Fotosammlung von Clearview über alle Bürger:innen zur Jagd auf gesuchte Verdächtige wie untergetauchte frühere Terroristen zu verwenden, obwohl man doch lesen konnte, dass die Firma mit diesem Service auch Despoten und Stalker bedient, die damit völlig unschuldige Opfer verfolgen.

Wenn Politiker:innen eine freiheitliche und gleiche digitale Gesellschaft erreichen wollen, dann müssen sie das Übel der permanenten Überwachung durch Datenkonzerne an der Wurzel bekämpfen und nicht nur die sichtbarsten Auswüchse kappen. Dazu muss man aufhören, Lobbyisten nachzugeben, die entweder direkt am Überwachungskapitalismus verdienen, oder, wie z.B. die deutschen Medienverlage, längst in ein Stockholm-Syndrom verfallen sind. Stockholm-Syndrom, weil sie die Methoden der Tech-Giganten verteidigen in der Hoff-

nung, dass ein kleiner Teil deren finanzieller Gewinne auch für sie abfällt. Dabei geben sie aber alle Steuerungsmöglichkeit ihres Geschäftsmodells aus der Hand und sehen zu, wie alle lukrativen Bestandteile Schritt für Schritt durch die großen Plattformen übernommen werden.

**Aufklärung tut not … und macht Spaß**

Um zu erläutern, warum eine grundrechtsgestützte Digitalisierung eine bessere Digitalisierung ist, warum „Ich habe nichts zu verbergen“ heute eine noch schlechtere Einstellung als früher darstellt, warum wir die Tech-Giganten zur Einhaltung der Spielregeln zwingen müssen und nicht etwa unsere Werte aufgeben sollten, machen wir eine immer intensivere Öffentlichkeitsarbeit.

Ganz vorne steht, mit gutem Vorbild und merkbaren Erläuterungen zu veranschaulichen, welche Bedrohung für unsere Gesellschaft eine schlecht gemachte Digitalisierung ist und dass es Alternativen dazu gibt. Und ja, ich glaube, da müssen wir Datenschutzaufsichtsbehörden noch alle besser werden, noch deutlich besser, unsere Erläuterungen sind oft viel zu kompliziert und praxisfern.

Aber es gibt auch schon Bereiche, in denen wir in den letzten fünfeinhalb Jahren richtig gut geworden sind beim BfDI, dazu zwei Beispiele:

Wir wollten einfach nicht die sozialen Netzwerke der Tech-Giganten für unsere Öffentlichkeitsarbeit nutzen, weil diese wie gesagt die Bürger:innen ausspionieren und schädliche Inhalte durch ihre Algorithmen verbreiten. Daher haben wir uns entschieden, das Fediverse zu nutzen. Also statt Monopol- Apps, die die Regeln vorgeben, ausspionieren und einen in einen digitalen Käfig stecken, ein offenes, technisch und organisatorisch föderiertes System von Apps und Services, die interoperabel sind. Im Fediverse kann man mit seinem Netzwerk an Kontakten übrigens ziemlich einfach weiterziehen, wenn einem ein Anbieter nicht mehr gefällt.

Entschieden haben wir uns für ein Angebot bei Mastodon (funktional wie Twitter/X, nur in schön, freundlich und offen) und dafür nicht nur einen Account angelegt, sondern direkt einen Server, um auch anderen Bundesbehörden diese Möglichkeit zu geben. Heute sind über einhundert Behörden auf unserem Server @social.bund.de aktiv. Den größten Account hat der BfDI selbst (@bfdi@social.bund.de), wobei unsere 45.000 Follower nicht mit den höheren Zahlen bei Twitter/X & Co. verglichen werden dürfen. Denn bei Mastodon sehen alle, die einem folgen, auch wirklich alle veröffentlichten Inhalte. Denn hier steht zwischen Behörde und Bürger:in nicht ein Algorithmus, der statt des abonnierten Inhalts auch mal Werbe-Beiträge oder häufig geklickten Fake-Videos anzeigt. Unsere Follower, die Bürger:innen, entscheiden selbst, was sie sehen wollen, nicht Elon Musk oder andere.

Einen besonders schönen Erfolg haben wir bei dem Bemühen erreicht, Kinder, Jugendliche sowie ihre Eltern über ihre Rechte, ihre Möglichkeiten und Risiken zu informieren. Ganz vorne ist unsere Reihe aus Pixi-Büchern und Videos zu nennen. Im März 2024 konnten wir Bundestagspräsidentin Bärbel Bas das millionste Exemplar der Bücher überreichen. Und die Nachfrage reißt weiter nicht ab, Einzelpersonen, Kindergärten und Grundschulen geben uns tolles Feedback.

**Und der Datenschutz, der hat Zähne**

Beratung und Information sind unsere klar bevorzugten Instrumente, aber wir sind nicht darauf beschränkt. Die Datenschutz-Grundverordnung (und auch zusätzlich einige nationale Gesetze) geben dem BfDI durchaus starke Instrumente zur Durchsetzung der Grundrechte der Bürger:innen. Davon machen wir Gebrauch:

So habe ich die Bundesregierung angewiesen, den Betrieb ihrer Facebook Fanpage einzustellen. Denn es kann nicht verhindert werden, dass die Tech- Giganten dabei im großen und aus unserer Sicht eben nicht legalem Umfang Daten über die Bundesbürger: innen sammeln. Bundesregierung und Meta haben gegen diese Weisung geklagt, ein Gericht wird nun entscheiden.

Angewiesen hat der BfDI auch die gesetzlichen Krankenkassen, damit diese allen Versicherten eine Möglichkeit geben, selbständig in die Daten ihrer eigenen elektronischen Patientenakte Einsicht zu haben und auch steuern zu können, wer darauf Zugriff nehmen darf. Bis jetzt ist dies nämlich unproblematisch nur für diejenigen möglich, die über ein geeignetes mobiles Endgerät verfügen und dieses nutzen können und wollen. Auch hier klagen die Krankenkassen gegen unseren Bescheid, ein Urteil wird für Klarheit sorgen.

Umfangreich durchgesetzt und damit eine Blaupause für ähnliche Fälle geschaffen haben wir im medial umfangreich begleiteten Rechtsstreit mit 1&1. Das Unternehmen hatte Daten seiner Kunden nicht ausreichend gegen Zugriff von Dritten über die Hotline des Unternehmens geschützt, war aber gegen unser Bußgeld gerichtlich vorgegangen.

Strittig wurde gestellt, ob wir, europäischem Recht folgend und entgegen deutschen nationalen Gesetzen, eine Geldbuße direkt gegen das Unternehmen verhängen durften. Wir durften! Es wurde bezweifelt, dass wir ein Bußgeld gegen das Versäumnis grundlegender Schutzstandards aussprechen durften, ohne diese vorher explizit als Leitlinie veröffentlicht zu haben. Wir durften! Und es ist nun auch klar, dass der Umsatz des Unternehmens eine entscheidende Größenordnung für die Höhe des Bußgelds ist. Zwischenzeitlich haben auch die obersten Gericht der Europäischen Union unsere Rechtsauffassung bestätigt. Besonders schön: Neben 1&1 haben auch andere Unternehmen in der Zwischenzeit ihre Schutzmaßnahmen optimiert.

Der Datenschutz hat also Zähne, wenn das Gespräch, wenn die Beratung nicht zur Beendigung rechtswidrigen Verhaltens führt. Und die Datenschutzaufsichtsbehörden sollten keine Angst davor haben, diese Zähne zum Einsatz zu bringen.

Weitere Bescheide des BfDI werden sich dabei damit auseinandersetzen müssen, dass nationales deutsches Recht an

einigen Stellen versucht, im europäischen Recht vorgesehene Durchsetzungsmöglichkeiten der Datenschutzaufsichtsbehörden einzuschränken: Das nationale Recht untersagt den Datenschutzaufsichtsbehörden beispielsweise die Anordnung sofortigen Vollzugs gegen Behörden. So gehen selbst eklatante Datenschutzverstöße während Gerichtsverfahren eventuell jahrelang weiter. Und auch Geldbußen sind gegenüber Behörden und Krankenkassen untersagt, obwohl Datenschutzverstöße gerade Letztgenannten Wettbewerbsvorteile verschaffen können. Sollte die Politik nicht selbst diese Einschränkungen beseitigen, werden es wohl Gerichte aufgrund von Maßnahmen des BfDI tun müssen.

**One more thing: Ohne Transparenz ist alles nichts**

So viel zum Datenschutz. Zu den Aufgaben des BfDI gehört noch „one more thing", wie Steve Jobs gesagt hätte: Transparenz, oder wie es etwas weniger weitgehend im Namen der Behörde steht, Informationsfreiheit.

In einer modernen demokratischen Gesellschaft sind Menschen keine Untertanen und auch nicht getrennt von staatlichen Institutionen zu verstehen. Sie bilden vielmehr als Bürger:innen den Staat. Daher sind staatliche Institutionen verpflichtet, Bürger:innen über ihr Handeln zu unterrichten und ihnen alle vorhandenen Informationen zur Verfügung zu stellen.

Wir haben unsere Arbeit auch in diesem Bereich ausgebaut, sowohl bei der Beratung von Bürger:innen, die staatliche Informationen haben wollen, als auch bei der Beratung der Behörden. Außerdem konnten wir die Zahl der Kontrollen erhöhen und häufiger zwischen beiden Seiten vermitteln.

Der BfDI geht selbst mit gutem Beispiel voran. Wir veröffentlichen viele Informationen schon von Beginn auf unserer Website, z.B. Briefe, Stellungnahmen und Kontrollberichte. Wir stellen Informationen, die wir auf eine individuelle Anfrage herausgegeben, sofort für alle Bürger:innen öffentlich. Beide Prinzipien empfehlen wir auch allen Bundesbehörden, erste positive Entwicklungen gibt es.

Diese Vorbildfunktion des BfDI war mir persönlich besonders wichtig. Als Parlamentarischer Staatssekretär beim Bundesminister der Justiz und für Verbraucherschutz hatte ich erreicht, dass alle Stellungnahmen von Verbänden zu Gesetzentwürfen öffentlich gemacht wurden. Damit konnten interessierte Bürger:innen, die Medien und engagierte Nichtregierungsorganisationen nachprüfen, wessen Anregungen übernommen wurden und wessen nicht. Außerdem hatte ich, wie schon zuvor als Bundestagsabgeordneter, auch jedes Gespräch mit Interessenvertretern inklusive Namen und Thema öffentlich gemacht. Was ich dabei gelernt habe: Transparenz schafft Vertrauen und stärkt damit demokratische Institutionen.

Grundlage für die Verpflichtung von Bundesbehörden zur Herausgabe von solchen Informationen ist seit 2006 das Informationsfreiheitsgesetz. Damals ein wichtiger Schritt, der auch heute noch bei vielen Sachverhalten hilft, ist es aber in die Jahre gekommen und fällt weit hinter die Regelungen in anderen Staaten und Bundesländern zurück. Wir brauchen, wie im Koalitionsvertrag versprochen, ein Update, ein wirkliches „Transparenzgesetz".

In diesem Gesetz sollten die Behörden verpflichtet werden, wichtige Informationen unmittelbar zu veröffentlichen, am besten auf einem einheitlichen Transparenzportal. Es sollte deutlich weniger Ausnahmen für die Verweigerung einer Auskunft geben, die Gebühren sollten hinterfragt werden und eine anonyme Auskunft möglich sein. Diese lehnen viele Behörden heute ab, obwohl dieser Schutz für einige Auskunftssuchende doch so wichtig ist.

Und es braucht Durchsetzungsmöglichkeiten, wenn Behörden Auskünfte rechtswidrig verweigern sollten. Wo der BfDI heute nur beraten und Rechtsverstöße „beanstanden" kann, müsste ein Transparenzgesetz vorsehen, dass eine Behörde angewiesen werden kann, Informationen herauszugeben.

**Ganz zum Schluss ein großer Dank**

Bedanken möchte ich mich vor allem und zuallererst bei den tollen Mitarbeiter:innen des BfDI für 2.008 Tage spannender Zusammenarbeit. Es war für mich beeindruckend, so außergewöhnliches Engagement für die gemeinsame Sache zu erleben und sich im Team für eine grundrechtsgeleitete Digitalisierung einsetzen zu können.

Mein Dank gilt auch den vielen Partner:innen des BfDI, die an unserer Seite gestanden haben. Damit meine ich die internationalen Kolleg:innen, die Landesdatenschutzbeauftragten, die Datenschutzbeauftragten in Behörden und Unternehmen, Wissenschaftler: innen und Zivilgesellschaft.

Und noch einmal: Ein herzlicher Dank an den Deutschen Bundestag, der uns ermöglicht hat, mit ausreichenden Ressourcen, hoher Kompetenz und noch höherem Engagement unseren Aufgaben nachzugehen, auch wenn wir nicht allzu selten eine Gegenstimme zur Gesetzgebung im Parlament selbst waren und sind und bleiben werden. Danke, dass der BfDI als unabhängige Aufsichtsbehörde diese Unterstützung erhalten hat.

Unsere Demokratie ist lebendig und soll es bleiben. Es wird weiterhin viel Einsatz benötigen, damit eine zunehmend digitalisierte Gesellschaft nicht zwischen Überwachungskapitalismus und staatlicher Überwachung zerrieben wird. Daten sind nur Mittel zum Zweck. Eine digitale, freie und gleiche Zukunft muss den Menschen in den Mittelpunkt stellen. Darum geht es.