Lutz Hasse

Vertrauen – Fortschritt – Kontrolle[1]

Ein funktionierendes rechtliches System zum faktischen Garantieren des Datenschutzes für die Bürger eines Staats kann einen Zuwachs an Vertrauen gegenüber staatlichen Autoritäten bewirken. Versagt das System jedoch, verkehrt sich dieser Effekt ins Negative. Wie steht die Bundesrepublik Deutschland diesbezüglich derzeit da? Was wurde bereits erreicht? Was ist noch zu tun? Welche prinzipiellen Gefahren drohen dem Grundrecht auf informationelle Selbstbestimmung?

Was schafft Vertrauen bei Bürgern?

Lassen Sie mich zunächst mit einigen problematischen Beispielen beginnen, die veranschaulichen, wie es nicht gemacht werden sollte: Die zwischenstaatlichen Abkommen zum grenzüberschreitenden Datentransfer *Safe Harbor* und *Privacy Shield* tragen vielversprechende Namen, schaffen aber nur scheinbar Vertrauen. Denn diese Verträge leisten datenschutzrechtlich nicht, was die Bürger von ihnen erwarten, und sind überdies mit geltendem europäischem Recht nicht vereinbar. *Safe Harbor*, ein Abkommen zum sicheren Datentransfer zwischen EU und USA nach Art. 25 Abs. 6 der EU Datenschutzrichtlinie, wurde deshalb am 6. Oktober 2015 vom EuGH wieder aufgehoben. Und auch gegen das Nachfolge-Abkommen *Privacy Shield* wird bereits gerichtlich vorgegangen, das wird nach meinem Dafürhalten höchstens noch zwei Jahre halten. Zwar fordert die Wirtschaft derartige Instrumentarien, damit der Eindruck erweckt wird, Daten könnten rechtskonform in die USA übermittelt werden. Auf lange Sicht sind solche Systeme aber kontraproduktiv, weil ihr Zusammenbruch voraussehbar ist und dann zu einem tiefsitzenden Vertrauensverlust bei den Bürgern führt.[2]

Kurz noch ein anderes zwiespältiges Szenario: Viele Online-Handelsplattformen stellen Bewertungssysteme zur Verfügung, die Vertrauen bei zukünftigen Käufern schaffen sollen. Die Anzahl der *Sternchen* misst angeblich die Zufriedenheit anderer Käufer des Produkts und soll so eine schnelle Kaufentscheidung begünstigen. Aber kann man sich auf ein derartiges System auch verlassen?

Was schafft nun wirklich nachhaltig Vertrauen? Dies sind zunächst einmal tragfähige und für den Bürger verständliche Rechtsgrundlagen. Zu nennen ist hier vor allem das *Grundrecht auf informationelle Selbstbestimmung,* das ich seit meiner Wahl vor mehr als sechs Jahren täglich gegen seine immer schneller voranschreitende Entwertung verteidige.

Der Durchsetzung dieses Grundrechts dienen sollen u. a. das *Bundesdatenschutzgesetz* (in neuer Fassung) und die (teilweise noch zu novellierenden) *Datenschutzgesetze der Länder* sowie die ab dem 25. Mai 2018 unmittelbar und EU-weit geltende *Datenschutz-Grundverordnung (DS-GVO),* die nach Meinung des EuGH auch Anwendungsvorrang vor den entsprechenden nationalen Normen besitzt. Der *Verständlichkeit* der DS-GVO abträglich sind jedoch von ihr verwendete *unbestimmte Rechtsbegriffe,* die zunächst von den Aufsichtsbehörden, und mit ziemlicher Sicherheit dann auch von Gerichten, konkret auszulegen sind. Dies ist nicht ungewöhnlich für neue rechtliche Normen, aber es wird Jahre bis Jahrzehnte dauern, hier einigermaßen Klarheit zu schaffen.[3]

Noch problematischer sind zahlreiche Öffnungsklauseln in der Datenschutz-Grundverordnung; das sind quasi bewusste Gesetzeslücken, die es dem nationalen Gesetzgeber ermöglichen, eigene Regelungen zu treffen.[4]

Eine prinzipiell vertrauensbildende Maßnahme im elektronischen Geschäftsverkehr sind *Datenschutzerklärungen.* Doch während die DS-GVO für das Ersuchen um Einwilligung ausdrücklich eine verständliche und leicht zugängliche Form in einer klaren und einfachen Sprache vorschreibt, trifft auf die Belehrungen gerade durch große bekannte Unternehmen eher das Gegenteil zu. Derartige Intransparenz, gleichfalls durch lange AGB mit schwammigen Formulierungen, die mitunter wöchentlich geändert werden, ist keinesfalls Ungeschicklichkeit, sondern beabsichtigt: Wir sollen gar nicht genau verstehen, was wir da unterschreiben und welche Verwendung unserer Daten wir damit erlauben!

Für aussichtsreich, um Vertrauen zu gewinnen, halte ich dagegen u. a. folgende Ansätze:[5] Gütesiegel durch unabhängige (!) Prüfer, zuverlässige Verschlüsselung im Browser und in mobilen Netzen, ISO-Normen und nicht zuletzt ein leistungsfähiges Transparenzgesetz, wie es in Thüringen demnächst verabschiedet werden soll.[6]

Fortschritt

Ohne Quellenrecherche, belastbare Aussagen etc. ist die fundierte Beurteilung einer Aussage (und damit das Vertrauen in diese) nicht möglich. Was fehlt also? Das Wissen um Fakten … im Zeitalter der sozialen Medien nicht einfach zu erlangen. Bildung ist also eine zentrale Vertrauenskomponente, und die gute Nachricht ist: Schon ein bisschen Bildung hilft! Grundlagen können in der Bildung einfach vermittelt werden, durch ein Grundverständnis wächst auch Vertrauen.

Medienbildung und Informatikunterricht könnten das notwendige Wissen vermitteln.[7] Laut der ICILS-Studie 2013[8] hat Deutschland im Bereich der computer- und informationsbezogenen Kompetenzen international aber einen erheblichen Rückstand aufzuholen.[9] Die Strategie der Kultusministerkonferenz (KMK) *Bildung in der digitalen Welt* vom Dezember 2016 thematisiert das[10] und setzt dabei auf einen integrativen Ansatz zum Erreichen digitaler Medienkompetenz: Statt in einem neuen, eigenen Fach werden entsprechende Inhalte in jedem der vorhandenen Fächer geeignet gelehrt.[11]

Ohne Prüfungsrelevanz, mit teilweise sehr abstrakten Kompetenzbeschreibungen im Kursplan und inhaltlich wie auch vom Umfang her stark abhängig von schulinterner Planung, bleibt

die Wirkung bisher jedoch beschränkt. Zudem werden Fachlehrer nicht grundständig auf diese Aufgabe vorbereitet und generell fehlen Lehrkräfte für das Schulfach Informatik. Immerhin bekennt sich die KMK in Übereinstimmung mit der ICILS-Studie zur Herausforderung, die Schulen anforderungsgerecht auszustatten und die Lehrerausbildung im Bereich des Studiums, des Referendariats und der Fortbildung anzupassen. Richtungsweisend verfolgt die Medienbildung in der Thüringer Schule einen bildungsgangübergreifenden Ansatz, inhaltlich werden auch Recht, Datensicherheit und Jugendmedienschutz berührt.[12]

Die Auswirkungen fehlender Bildung und dadurch bedingten unberechtigten Vertrauens sind vielfältig und gerade für die digitale Lebenswelt von Kindern und Jugendlichen gravierend.[13] Dazu gehören Cybermobbing, Umgehung der Altersverifikation für Medieninhalte, Verstöße gegen das Urheberrecht, unbedarfte Preisgabe persönlicher Daten bis hin zu freizügigen Fotos. Nicht alles ist da vermeidbar, aber Aufklärung zu richtigem Umgang auf jeden Fall dringend geboten. Die Landesdatenschutzbehörden stellen hierfür umfangreiches Material kostenlos zur Verfügung.[14]

Kontrolle – Die Möglichkeiten der Aufsichtsbehörden

Das Grundrecht auf informationelle Selbstbestimmung gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Und unter den Bedingungen der automatischen Datenverarbeitung gibt es kein belangloses Datum mehr, sagt das Bundesverfassungsgericht. Auch, dass dieses Grundrecht in der Menschenwürde wurzelt. Die Menschenwürde zu schützen, ist Aufgabe aller staatlichen Gewalt, so steht es im Grundgesetz. Leider kann ich nicht erkennen, dass unser Staat bemüht ist, einen tatsächlichen, einen wirksamen Schutz dieses Grundrechts zu garantieren. Stattdessen sagt (nicht nur) unsere Bundeskanzlerin, Daten seien der Rohstoff der Zukunft, und verklärt dazu passend in zeitgemäßem Neusprech die Aushöhlung effektiven Datenschutzes als „Datenreichtum".

Wie das beispielsweise praktisch gehandhabt werden soll, zeigt der Vorschlag[15] des Bundesministeriums für Verkehr und digitale Infrastruktur. In einem „Datengesetz" soll geregelt werden, dass derjenige, als dessen „Verdienst" die Generierung von Daten anzusehen ist (im Automobil wäre das beispielsweise der Hersteller des Fahrzeugs), die Verfügungsgewalt über diese Daten erhält. Er (!) ist der „Dateneigentümer". Und wenn das so klappt, sollen als nächstes sogar Gesundheitsdaten an die Reihe kommen.[16] Deutlich wird hier, dass die Politik den Weg frei machen soll für eine ungehinderte Datenverwertung durch die Wirtschaft.

Trotz der beschriebenen Unzulänglichkeiten stellen die Datenschutz-Grundverordnung und die nachrangige nationale Gesetzgebung eine Reihe von Kontrollrechten für die Betroffenen zur Verfügung, die auch mittels der Aufsichtsbehörden ausgeübt werden können. Es kommt nun darauf an, noch bestehende nationale Freiräume klug für den Datenschutz zu nutzen und ggf. Fehlentscheidungen der Vergangenheit rückgängig zu machen. Landes- und Bundesdatenschützer sind auch in dieser Hinsicht verlässliche Partner der Bürgerinnen und Bürger und bürgerrechtlich orientierter Organisationen und Bewegungen.

Fazit

Die Politik sollte sich rasch von dem Konstrukt des „Datenreichtums" verabschieden und wieder zu einem nachhaltigen Schutz des Grundrechts auf informationelle Selbstbestimmung zurückkehren. Andernfalls riskiert sie, bei den Bürgern weiteres Vertrauen zu verspielen.

Anmerkungen und Referenzen

1 *Siehe vertiefend den gleichnamigen Vortrag auf der FIfF-Konferenz 2017, Video unter fiff.de/r/181007, Vortragsfolien fiff.de/r/181008*
2 *Vertiefung: Vortragsfolien fiff.de/r/181010, Vortragsvideo fiff.de/r/181009*
3 *Vertiefung: Vortragsvideo fiff.de/r/181011*
4 *Vertiefung: Vortragsfolien fiff.de/r/181012, Vortragsvideo fiff.de/r/181013*
5 *Vertiefung: Vortragsfolien fiff.de/r/181014*
6 *Vertiefung: Vortragsfolien fiff.de/r/181016, Vortragsvideo fiff.de/r/181015*
7 *Vertiefung: Vortragsfolien fiff.de/r/181017, Vortragsvideo fiff.de/r/181018*
8 *International Computer and Information Literacy Study, 2013, https://www.waxmann.com/fileadmin/media/zusatztexte/ICILS_2013_Berichtsband.pdf*
9 *Vertiefung: Vortragsfolien fiff.de/r/181019*
10 *Strategie der Kultusministerkonferenz Bildung in der digitalen Welt, Dezember 2016, https://www.kmk.org/fileadmin/Dateien/pdf/PresseUndAktuelles/2016/Bildung_digitale_Welt_Webversion.pdf*
11 *Vertiefung: Vortragsfolien fiff.de/r/181020*

Lutz Hasse

Dr. **Lutz Hasse** legte die Juristischen Staatsexamina in Niedersachsen ab. Es folgten Assistenzen an der Universität Osnabrück und ab 1992 an der Friedrich-Schiller-Universität Jena. Die Promotion erfolgte während der „Jenenser Phase" an der Universität Osnabrück. Anschließend erfolgte der Wechsel zur Thüringer Verwaltungsfachhochschule – Fachbereich Polizei; dort wurde er Leiter der Rechtsausbildung. Nach Tätigkeiten als Referatsleiter im Thüringer Innenministerium, beim Thüringer Landesbeauftragten für den Datenschutz und im Thüringer Sozialministerium wurde er 2012 und 2018 vom Thüringer Landtag zum Landesbeauftragten für den Datenschutz und die Informationsfreiheit gewählt.

12 *Vertiefung: Vortragsfolien fiff.de/r/181021*

13 *Vertiefung: Vortragsfolien fiff.de/r/181022*

14 *Beispielsweise die Broschüre Digitale Selbstverteidigung des TLfDI, https://www.tlfdi.de/mam/tlfdi/wir-ueber-uns/digitale_selbstverteidigung_broschuere_4web2018.pdf. Vgl. auch die Übersichten auf den Vortragsfolien fiff.de/r/181023. Besonders empfohlen sei das Jugendportal youngdata der unabhängigen Datenschutzbehörden des Bundes und der Länder, sowie des Kantons Zürich, https://www.youngdata.de/.*

15 *Studie „Eigentumsordnung" für Mobilitätsdaten?, http://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile*

16 *Vgl. a. a. O., S. 119f.*

Thomas Gruber

Die Marschrichtung im Cyber- und Informationsraum

Im April 2017 wurde das neue Kommando Cyber- und Informationsraum (CIR) *am Standort Bonn aufgestellt. Mit ihm existiert nun die Führungsstruktur für den militärischen Bereich Cyber- und Informationsraum, der voraussichtlich 2021 personell vervollständigt wird. Knapp 14.000 SoldatInnen sollen dann an verschiedenen deutschen Standorten arbeiten, bisher sind es etwa 12.500. Die Bundeswehr muss sich innerhalb kurzer Zeit um mehr als 1.000 IT-Fachkräfte, bevorzugt mit militärischer Ausbildung, bemühen – keine leichte Aufgabe.*

Doch auch ohne die volle Truppenstärke ist der neue Organisationsbereich bereits einsatzfähig: Zum Großteil wurden bereits bestehende Kommandos und deren untergeordnete Bataillone dem Kommando CIR unterstellt. In den Arbeitsbereich CIR fallen nun beispielsweise die psychologische Kriegsführung *(Zentrum Operative Kommunikation der Bundeswehr)*, die Störung feindlicher und Sicherung eigener Kommunikationsnetze *(Bataillone Elektronische Kampfführung)*, die Vernetzung und technische Ausstattung der Kriegseinheiten *(Kommando Informationstechnik der Bundeswehr)* sowie Angriff und Verteid[illegible] *Netzwerk Operationen*, bald: *Zen[illegible]*

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Die genaue Struktur des neuen[illegible] Zielsetzung der Bundeswehr im Cyber- und Informationsraum sind unter anderem dem Abschlussbericht *Aufbaustab Cyber- und Informationsraum*[1], der *Strategischen Leitlinie Cyber-Verteidigung* des Bundesministeriums der Verteidigung (BMVg)[2] und dem *Weißbuch der Bundeswehr 2016*[3] zu entnehmen. Einen kurzen Überblick geben beispielsweise die Artikel *Es cybert bei der Bundeswehr*[4] und *Onlineoffensive*[5]. Jene thematischen Umrisse sollen im Folgenden um einige Gedanken zur deutschen Strategie im Cyber- und Informationsraum ergänzt werden, die während der FIfFKon 2017 angeregt wurden.[6]

Werbung, Wirkung, Widerstand

Die Aussetzung der Wehrpflicht ab dem Jahr 2011 beschränkt die Bundeswehr in ihrer wichtigsten Ressource: SoldatInnen. Gleichzeitig steigt die Zahl der deutschen Kriegseinsätze und damit auch der benötigten Truppenkontingente. In diese Zeit fällt nun noch der Aufbau des neuen Cyberkommandos – der Personalmangel ist programmiert. Das Gegenmittel der Wahl ist für das BMVg großflächige, bundesweite, zielgruppenorientierte Werbung. Von der Plakatkampagne „Mach, was wirklich zählt" über Werbeveranstaltungen in Schulen, auf Jobmessen und in Arbeitsagenturen bis zu YouTube-Serien („Die Rekruten", „Mali") – die Bundeswehr ist inzwischen omnipräsent. Zunehmend versucht sie dabei auch „Erstkontakt" zu jungen Menschen noch weit jenseits des Rekrutierungsalters aufzunehmen: Eigene Websites für Jugendliche, Werbung in Jugendmagazinen, gezielte Postsendungen, Abenteuercamps und vieles, vieles mehr. Etwa 35 Millionen Euro kostet die Nachwuchswerbung für das deutsche Militär jährlich. Immer dabei: Ein starker Fokus auf den neuen Organisationsbereich CIR. So macht beispielsweise das *Projekt Digitale Kräfte* zur Gewinnung von IT-Fachpersonal gut ein Viertel der Kosten der gesamten „Mach, was wirklich zählt"-Kampagne aus; in den vergangenen Jahren war die Bundeswehr wiederholt auf der Computerspiele-Messe *gamescom* mit einem Stand vertreten, 2017 sogar mit einer eigenen *Challenge-App* für Mobilgeräte; und im Rahmen der sogenannten *Cyber-Days* und eines *IT-Camps* gab es neben einer [illegible] und Lagerleben auch noch eine [illegible] die TeilnehmerInnen.

[illegible] deswehr hat in den letzten Jahren durchaus Wirkung erzielt. 2017 vermeldete das Verteidigungsministerium begeistert, dass es „im Sendezeitraum der Serie *Die Rekruten* […] 40 Prozent mehr Zugriffe auf die Karriere-Website, ein Viertel mehr Anrufe bei der Karriere-Hotline und 21 Prozent mehr Bewerbungen bei Mannschaften und Unteroffizieren"[7]gab. Auch danach stieg das Interesse am SoldatInnenberuf weiter: Im ersten Halbjahr 2017 gab es beim deutschen Militär fast so viele Einstellungen wie im ganzen Jahr 2016.[8] Die *Castenow*-Werbeagentur, welche den Auftrag des Verteidigungsministeriums bekommen hat, erhält seitdem einen Preis der Werbebranche nach dem anderen.[9]

Die Sprüche (wie „Deutschlands Freiheit wird auch im Cyberraum verteidigt" und „Wir kämpfen auch dafür, dass du gegen uns sein kannst") und die Maßnahmen der Nachwuchswerbung sind oftmals sehr forsch bis provokativ – und das ist ohne Frage auch Kal-

Abbildung 1: Kind mit Waffe am Tag der Bundeswehr 2016 in Stetten am kalten Markt (Quelle: DFG-VK)[10,11]