Informationelle Selbstbestimmung im 21. Jahrhundert

Wir müssen eingestehen, dass es anders gekommen ist, als Helmut Bäumler, der langjährige schleswig-holsteinische Datenschutzbeauftragte vor 15 Jahren forderte: Datenschutz müsse sexy sein. Der Sexappeal des Datenschutzes hält sich auch im Jahr 2017 in Grenzen. Die Datenschutzgrundverordnung wird daran nicht viel ändern, auch wenn der neue Europäische Rechtsrahmen den Datenschutz aufwertet.

Vielleicht ist es auch der falsche Ansatz, von gesetzlichen Regelungen – welcher Art auch immer – zu erwarten, dass sie die Menschen begeistern.

Das ist bei der Technik anders: Viele Menschen sind bereit, große Unannehmlichkeiten in Kauf zu nehmen, um möglichst frühzeitig das jeweils neueste Modell des iPhone zu ergattern. Und viele nahmen erhebliche Risiken in Kauf, als sie den neuen Tesla-Mittelklassewagen allein auf Basis einer allgemeinen Ankündigung verbindlich bestellten, der nicht nur elektrisch betrieben wird, sondern auch „autonom“ fahren soll.

Trotzdem haben viele derjenigen, die bereitwillig (fast) jede technische Neuerung mitmachen, ein mulmiges Gefühl. Und das zurecht!

Dass wir bei der Nutzung des Internets Spuren hinterlassen, ist inzwischen fast eine Binsenweisheit. Es hat sich auch herumgesprochen, dass das Smartphone in unserer Hosen- oder Handtasche mehr über uns preisgibt, als vor Jahren ein Privatdetektiv oder Polizist in mühsamer Recherche herausfinden konnte. Und dass die mit Technik vollgestopften modernen Autos riesige Datenmengen erzeugen, verwundert niemanden. Schließlich ist nicht zu übersehen, dass viele Menschen in Social Networks ziemlich viel über sich preisgeben.

Auch und gerade deshalb müssen wir uns fragen, warum es uns - und ich meine hier sowohl die professionellen Datenschützer als auch den Rest der Datenschutz-Community - nicht gelungen ist, Datenschutz und informationelle Selbstbestimmung sehr viel weiter oben in der öffentlichen Diskussion zu verankern. Vielleicht haben wir uns zu sehr um das Klein-Klein gekümmert und dabei die wirklich großen Dinge aus dem Auge verloren.

Welche Folgen es haben kann, dass Überwachungstechnologien immer stärker in unseren Alltag sickern, lässt sich gerade in der Türkei beobachten: Dort wurden Tausende Beamte und Richter entlassen, allein weil sie auf ihren Smartphones bestimmte Apps installiert hatten. Besonders verdächtig waren diejenigen, die verschlüsselte Massengerdienste nutzten.

Vor zwei Monaten wurden in Istanbul mehrere Menschenrechtsaktivisten verhaftet, allein weil sie sich in einem Seminar mit Techniken vertraut machten, mit denen sich die Kommunikation gegen Überwachung schützen lässt. Die Seminarteilnehmer, darunter mehrere Mitglieder von Amnesty International, sind weiterhin in Haft. Die türkischen Behörden werfen dem deutschen Menschenrechtler Peter Steudtner und den anderen Seminarteilnehmern vor, Terrorismus zu unterstützen. Dass es in der Türkei, die sich mit großer Geschwindigkeit in einen autoritären Staat verwandelt, sehr gute Gründe dafür gibt, sich gegen staatliche Überwachung zu schützen, muss ich hier niemandem erklären.

Aber wie sieht es bei uns aus? Mancher wird einwenden: „Anders als die heutige Türkei ist Deutschland doch ein Rechtsstaat.“ Das stimmt zwar, doch auch bei uns wird die staatliche Überwachung immer weiter hochgefahren. In den letzten Jahren hat der Bundestag mehr sogenannte „Sicherheitsgesetze“ beschlossen als nach dem 11. September 2001, von der Vorratsdatenspeicherung für Telekommunikationsdaten bis zum Staatstrojaner, von der Ausweitung der Videoüberwachung im öffentlichen Raum bis zur Schaffung eines umfassenden polizeilichen Datenpools ohne besondere Zweckbindungsregeln, die bisher den Zugriff auf besonders sensible Daten beschränken.

Alle diese Gesetze wurden beschlossen, ohne dass die Wirksamkeit der vielen zuvor eingeführten Gesetzesverschärfungen überprüft und nachgewiesen wurde. Und fast noch schlimmer: Der öffentliche Aufschrei blieb aus, die Kritik daran beschränkte sich auf die üblichen Verdächtigen.

Dabei gehen die Überwachungsphantasien weiter. Denken wir etwa an automatisierte Gesichtserkennung bei Videoüberwachungssystemen, die derzeit an einem großen Berliner Bahnhof getestet wird. Wenn

Bundesinnenminister de Maizière behauptet, die neue Technik solle nur zur Identifikation von bekannten Straftätern oder möglichen Terroristen eingesetzt werden, so beruhigt mich das nicht.

Auch bei anderen Überwachungstechniken, etwa bei der Kontodatenabfrage, war der Kampf gegen Terrorismus und Schwerkriminalität der Türöffner für eine Infrastruktur, die heute millionenfach von allen möglichen Behörden genutzt wird, vom Jobcenter bis zum Finanzamt, vom Gerichtsvollzieher bis zur Bafög-Stelle. Und dass sich mit der Gesichtserkennung in Echtzeit auch nur ein terroristischer Anschlag hätte verhindern lassen, glauben im Ernst nicht einmal die Befürworter der neuen Technologie. Und trotzdem stellt kaum jemand die Frage, wie es in den letzten Monaten in London zu mehreren Terroranschlägen kommen konnte, trotz umfassender Videoüberwachung, ausufernder Vorratsdatenspeicherung und Vorbeugehaft. Könnte es vielleicht der falsche Weg sein, einseitig auf immer mehr Technik und immer mehr Überwachung zu setzen, statt sich viel stärker mit den Ursachen von Terror und Kriminalität auseinanderzusetzen? Wären die Demokratien nicht gut beraten, mit mehr Gelassenheit zu

reagieren und die Ermittler ihre Arbeit machen zu lassen, statt nach jedem Vorfall neue Gesetze zu fordern?

Überwachung ist nicht nur eine Frage, die wir im Verhältnis zwischen Bürger und Staat diskutieren müssen. Sie stellt sich auch im nicht-staatlichen Bereich.

Wenn wir uns mangels menschlicher Gesprächspartner mit „Alexa“, „Cortana“ oder „Siri“ unterhalten, den angeblich mit künstlicher Intelligenz ausgestatteten Sprachassistentinnen großer IT-Konzerne, installieren wir damit freiwillig Überwachungstechnologie in unsere Wohnungen. Wir geben damit den „unantastbaren Kernbereich der privaten Lebensgestaltung“ auf, den das Bundesverfassungsgericht vor vielen Jahren postuliert hat. Wir machen uns mit der Installation von mit Mikrofonen ausgestatteten Lautsprecherboxen freiwillig zu Opfern großer Lauschangriffe, wenn wir bereitwillig die Selbst-Verwanzung unserer Privaträume vornehmen.

Nicht nur hier überschneiden sich technologische Entwicklungen, kommerzielle Interessen an möglichst umfassenden Kundenprofilen und staatliche Überwachungs-Begehrlichkeiten - und alles nur, um uns ein noch angenehmeres Nutzungserlebnis zu

verschaffen und unser Leben komfortabler zu gestalten, wie uns die Werbung weiß machen will.

Da ist er wieder, der erhobene Zeigefinger des Datenschutzes! Wäre die Welt nicht schöner, wenn wir gemäß dem Motto handelten: „Digitalisierung first, Bedenken second“, den eine Partei plakatiert, die sich gerade um den Wiedereinzug in den Bundestag bemüht? Ich habe da meine Zweifel! Das Wort „Bedenken“ kommt von „Denken“ - und das dürfen wir auch künftig nicht Maschinen überlassen.

Vielleicht müssen wir Datenschützer uns damit abfinden, als Bedenkenträger angegriffen zu werden. Aber wir dürfen uns nicht darauf beschränken, zu sagen, was nicht sein darf. Gefragt sind praktikable Vorschläge, wie sich sinnvolle Ziele unter Beachtung unserer Werte, der Grund- und Menschenrechte realisieren lassen. „Datenschutz durch Technik“ muss das rechtliche Konzept der informationellen Selbstbestimmung ergänzen. Das muss ich eigentlich hier in Schleswig-Holstein niemandem erklären. Aber der technologische Datenschutz ist im Big Data Zeitalter vor neue Herausforderungen gestellt, gerade weil seine bisherigen Konzepte der Anonymisierung und Pseudonymisierung

angesichts der riesigen Datenmassen und der immer effektiveren Auswertungsmethoden an ihre Grenzen stoßen.

Die Frage stellt sich, wie wir modernste Techniken einsetzen können, um unsere Privatsphäre und unser Selbstbestimmungsrecht zu schützen. Metadaten könnten z.B. so verfremdet werden, dass sie einen personalisierten Rückschluss auf das individuelle Verhalten ausschließen, ohne den angestrebten Erkenntnisgewinn zu beeinträchtigen.

Block Chain ist nicht per se eine Big Brother-Technologie, sie kann auch auch zur Gewährleistung der Integrität und Vertraulichkeit der Daten und zur Sicherstellung der Betroffenenrechte eingesetzt werden.

Künstliche Intelligenz kann nicht nur dazu verwendet werden, unser Verhalten immer umfassender auszuforschen und zu steuern, sondern auch, um uns vor Gefahren der Ausforschung, Überwachung und Manipulation besser zu schützen.

Wenn wir über das Informationelle Selbstbestimmungsrecht im 21. Jahrhundert

nachdenken, müssen wir uns klar machen, dass es auch beim Umgang mit Informationen um politische Entscheidungen geht. Es gibt sie, die Stellschrauben, die bewegt werden können. Wir müssen uns nicht mit Fehlentwicklungen abfinden. In diesem Bundestagswahlkampf wird um die Zukunft der Verbrennungstechnologie beim Auto gestritten. Wir brauchen eine vergleichbar intensive Diskussion über die Gestaltung der Informationstechnologie.

Zugleich müssen wir Datenschützer uns davor hüten, als Besserwisser aufzutreten, die die Menschen vor sich selbst schützen. Im Mittelpunkt muss Aufklärung stehen. Und es geht um die Gewährleistung von Wahlfreiheit. Formale, umfassende Einwilligungserklärungen, auf die wir bei immer mehr Internetdiensten stoßen, bewirken genau das Gegenteil.

Umso wichtiger ist es, dass wir uns mit dem Koppelgeschäft auseinandersetzen, das etlichen digitalen Plattformen zu Grunde liegt: Die Nutzer liefern ihre persönlichen Daten und dürfen dafür als Gegenleistung bestimmte Dienste vermeintlich kostenlos nutzen. Zugleich gewinnen diese Plattformen eine derartige Marktmacht, dass nicht nur den Nutzern,

sondern auch den eigentlichen Dienstleistern einseitig ihre Bedingungen diktieren können. Nicht nur das informationelle Selbstbestimmungsrecht, sondern auch die Chancen kleinerer und mittlerer Unternehmen in einem digitalen Umfeld können dabei unter die Räder kommen.

Um dem informationellen Selbstbestimmungsrecht Geltung zu verschaffen, brauchen wir signifikante Fortschritte auf verschiedenen Ebenen:

Wir brauchen *Empowerment*: Technische Systeme sind so zu gestalten, dass sie dem Einzelnen die Entscheidungsfreiheit über seine Daten ermöglichen. Von zentraler Bedeutung sind kryptographische Verfahren, die vertrauliche Informationen vor Überwachung und Registrierung schützen.

Bestrebungen, verschlüsselte Kommunikation zu verbieten und Informationstechnik mit Hintertüren für Geheimdienste und sonstige Stellen auszustatten, sind kontraproduktiv, denn sie schwächen die Informationssicherheit nicht nur dort, wo es um die Aufdeckung krimineller Aktivitäten geht, sondern generell. Bedeutsam sind auch Techniken, welche die

Betroffenen dabei unterstützen, ihre Präferenzen zum Schutz der Privatsphäre auszudrücken und durchzusetzen.

Notwendig ist auch mehr *Transparenz*: Angesichts immer größerer Datenmengen und algorithmischer Steuerung kann der Einzelne kaum noch erkennen, was mit seinen Daten geschieht. Obwohl die Folgen der Profilbildung gravierend sein können, hat der Betroffene kaum eine Chance zu erfahren, wie mit den ihn betreffenden Informationen umgegangen und welche Schlüsse daraus gezogen wurden.

Einen verbesserten Durchblick könnten rechtliche Verpflichtungen zur Offenlegung der bei der Verarbeitung und Bewertung verwendeten Algorithmen verschaffen. Algorithmentransparenz kann diskriminierende Praktiken aufdecken und zurückdrängen.

Mehr Transparenz - in Bezug auf staatliches und privatwirtschaftliches Handeln - befördert die dringend notwendige politische Debatte und sie erweitert den persönlichen Handlungsspielraum, etwa den Wechsel zu einem datenschutzfreundlichen Internetangebot.

Last but not least ist mehr *Öffentlichkeit* erforderlich: Solange der Umgang mit Daten und die Ausübung von Datenmacht ein Nischenthema bleiben, werden sich die gesellschaftlichen und rechtlichen Rahmenbedingungen beim Umgang mit persönlichen Informationen nicht wirklich verbessern. Nur wenn zweifelhafte Praktiken sichtbar gemacht und darüber frei diskutiert wird, haben Gegenmaßnahmen eine Chance.

Die Überwachung der Überwacher, mehr Transparenz bei Nachrichtendiensten und privatwirtschaftlichen Datenkraken sind zentrale Zukunftsthemen. Den Praktiken der autoritären Datenkontrolle und Zensur, die in vielen Teilen der Welt um sich greifen, müssen wir genauso eine Abfuhr erteilen wie der Konzentration von Datenmacht in staatlichen und privatwirtschaftlichen Händen. Das Datenschutzrecht muss deshalb flankiert werden durch das Verbraucher- und Wettbewerbsrecht und wirksamere Kontrollstrukturen bei der staatlichen Datensammlung.

Ein letztes Wort: Es wäre ein schwerer Fehler, die Gewährleistung des Rechts auf informationellen Selbstbestimmung allein dem Datenschutzrecht und den mit seiner Umsetzung beauftragten amtlichen

Datenschützern zu überlassen. Ähnlich wie beim Umweltschutz - der ja auch lange gebraucht hat, bis er gesellschaftlich akzeptiert wurde - geht es auch hier um Nachhaltigkeit: Zivilisatorische Werte und Prinzipien, Demokratie, Freiheit des Individuums, verbriefte Grund- und Menschenrechte lassen sich in der Informationsgesellschaft nur bewahren, wenn wir ihre Durchsetzung als persönliche, technologische und gesellschaftliche Aufgabe begreifen, die sich nicht auf eine Behörde oder einen Datenschutzbeauftragten delegieren lassen.

Wie sich die Informationsgesellschaft weiterentwickelt, wird nicht nur durch technische und wirtschaftliche Faktoren bestimmt, sondern auch von der Bereitschaft der Bürgerinnen und Bürger, darauf Einfluss zu nehmen.

Ich danke für Ihre Aufmerksamkeit!