KFG kontrovers

Der Gegensatz von Freiheit und Sicherheit

Seit den Terroranschlägen vom 11. September 2001 wird (nicht nur) in Deutschland heftig die Frage diskutiert, wie weit die Sicherheitsbehörden in ihrem Kampf gegen Terrorismus und Kriminalität gehen sollten. Als natürliches Gegengewicht zu unbeschränkten Befugnissen stehen die garantierte individuelle Freiheit sowie das Recht auf Privatsphäre der Bürger.

Technischer Fortschritt macht es möglich, dass Sicherheitsbehörden per Videoüberwachung Plätze observieren, per Online-Durchsuchung, oft auch „Staatstrojaner“ genannt, Handys und PCs kontrollieren und durch Vorratsdatenspeicherungen alle möglichen Verbindungsdaten auf unbestimmte Zeit archivieren. Doch wie viel Sicherheit verträgt ein freies, demokratisches Land?

Warum der Staat uns überwachen muss

Ein Kommentar von Alexander Frei

In allen westlichen Demokratien kann in den letzten Jahren ein beunruhigender Trend beobachtet werden: Die Häufigkeit von Terroranschlägen ist exponentiell angestiegen. Die Anschläge 2015 in Paris, 2016 in Nizza und Berlin oder 2017 in Manchester haben weltweit für Entsetzen gesorgt. Erinnerungen und Bilder dieser Gräueltaten sind in all unseren Köpfen präsent, besonders bei Massenveranstaltungen wie den aktuell eröffnenden Weihnachtsmärkten. Laut einer Umfrage des Forschungsinstituts *statista* glauben 80 % der Deutschen, dass es in nächster Zeit Terroranschläge in Deutschland geben wird. Doch lediglich 52 % geben an, ihrer Meinung nach werde genug zum Schutz gegen Terroranschläge getan.

Fast 48 % der deutschen Bevölkerung sind also der Meinung, die Staatsgewalt müsse mehr tun, um sie vor der Terrorgefahr zu schützen. Jedoch sind es meist genau diese Menschen, die sich mit großer Vehemenz gegen neue, effektivere Sicherheitsgesetze wehren. Vorhaben wie die Vorratsdatenspeicherung und die Online-Durchsuchung (von Kritikern mehr oder weniger liebevoll „Staatstrojaner“ getauft), die dem Staat die Speicherung und Echtzeit-Auswertung von Verbindungsdaten ermöglichen, werden rigoros abgelehnt, obwohl sie eine effiziente und schnelle Aufklärung, wenn nicht sogar Prävention von Gräueltaten ermöglichen. Es ist wie bei Allem: Nach einem Anschlag schwirrt das Internet voller Mitleidsbekundungen, voller Aufrufe zu „thoughts and prayers“. Doch wenn es um konkrete Maßnahmen geht, die ebendiese Menschen auch nur ein bisschen betreffen, will niemand etwas davon hören. Es ist eine Sache, nach einem Anschlag auf Twitter seine Solidarität zu bekunden. Es ist eine andere zu versuchen, ein weiteres solches Ereignis tatsächlich zu verhindern.

Die Polizei und die Sicherheitsbehörden versuchen dies. Doch die Kriminalität ist längst im 21. Jahrhundert angekommen, während die Befugnisse der Polizei noch im 20. Jahrhundert feststecken. Mit dem Internet hat sich eine ganz neue Welt eröffnet. Ein rechtsfreier Raum, so scheint es. Und nicht nur im Darknet, einem verschlüsselten Teil des Internets, wo beispielsweise im Minutentakt Drogen und Waffen verkauft werden, sind Kriminelle aktiv. Der Terrorist von heute koordiniert seinen Anschlag ganz bequem über WhatsApp oder den Playstation-Chat. In Deutschland fehlen den Behörden zu oft die Möglichkeiten oder Befugnisse, um solche Datensätze schon vor oder sogar nach einer schweren Straftat auszuwerten. Bei der Aufklärung der Anschläge auf die Redaktion der Pariser Satirezeitschrift „Charlie Hebdo“ spielten circa 500 Telefonate, die die Lebensgefährtinnen zweier der Angreifer geführt hatten, eine wichtige Rolle. In Deutschland wäre die Auswertung dieser wegen der Aussetzung der Vorratsdatenspeicherung nicht möglich gewesen.

Wikimedia Commons/psyomjesus

Die Gewährleistung von Sicherheit ist eine der Kernaufgaben eines Staates. Sie ist einer der Hauptgründe, warum sich Individuen in Gesellschaften zusammengefunden haben. Allerdings wird seit eh und je darüber gestritten, wie weit der Staat in die Freiheit seiner Bürger eingreifen darf, um ihre Sicherheit zu gewährleisten.
Schon der britische Staatstheoretiker John Locke war der Meinung, das Individuum müsse einen Teil seiner Freiheit aufgeben, um in einer politischen Gesellschaft leben zu können. Dieser Aussage kann sicherlich fast jeder (mit Ausnahme der Anarchisten) zustimmen. Denn die eigene Freiheit kann nur so weit gehen, bis sie die Freiheit eines Anderen einschränkt. Dieser Gedanke ist uralt und wurde in seiner bekanntesten Formulierung in der „Erklärung der Menschen- und Bürgerrechte“ (Déclaration des Droits de l'Homme et du Citoyen) vom 26. August 1789, die im Rahmen der französischen Revolution von der neuen französischen Nationalversammlung verfasst wurde, niedergeschrieben.

Doch in der Diskussion, wie weit der staatliche Eingriff gehen dürfen soll, wird eines gerne übersehen: Sicherheit ist eine Voraussetzung, damit Freiheit überhaupt existieren kann. Dies stellte schon der preußische Politiker Wilhelm von Humboldt mit seinem berühmten Zitat: „Ohne Sicherheit ist keine Freiheit“ fest. Der ehemalige Innenminister und bayerische Ministerpräsident Dr. Günther Beckstein kommentiert diese Aussage in einem Diskussionsbeitrag für die Bundeszentrale für politische Bildung so: „Dieser Antagonismus [zwischen Sicherheit und Freiheit] aber ist ein großer Irrtum. Sicherheit und Freiheit sind alles andere als Gegensätze. […] Ohne Sicherheit ist alle Freiheit nichts, weil sie ein Leben in Angst bedeuten würde. Nur wer in Sicherheit lebt, kann sich frei entfalten und bestmöglich entwickeln.“

Auch sollte genau überlegt werden, wie groß das vermeintliche Opfer der aufgegebenen Freiheit tatsächlich ausfällt. Gespeicherte Daten würden ja nur bei besonderen Verdachtsfällen nach richterlicher Anordnung von Behörden kontrolliert werden, nicht permanent. Wer nichts zu verbergen hat, wird auch nicht kontrolliert; die diffuse Angst vor totaler Überwachung, wie sie George Orwell beschreibt, bleibt somit ein unsachliches Schreckgespenst von linksliberalen Meinungsmachern.

Keinesfalls soll in diesem Kommentar für totale Überwachung plädiert werden. Totalitarismus ist eine große Gefahr für die Demokratie und die starke Überwachung aller Bürger führt zwingend zu ihm. Doch in Maßnahmen wie der Vorratsdatenspeicherung schon eine Gefahr für den Rechtsstaat zu sehen, ist übertrieben, wie auch der SPIEGEL-Kolumnist Jan Fleischauer in

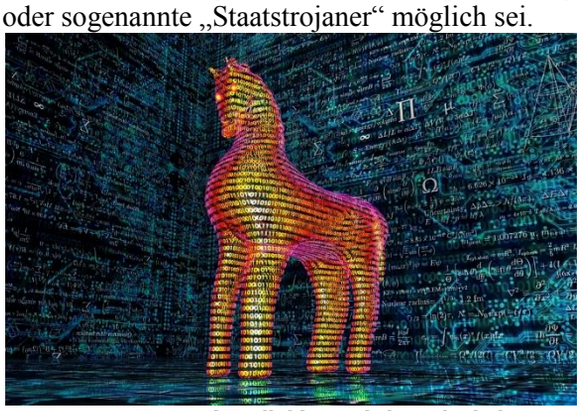
seinem lesenswerten Kommentar „Speichert endlich, wer mit wem telefoniert“ meint: „[Z]wischen totaler Kontrolle und dem Aufbewahren von ein paar Datensätzen, über deren Freigabe ein Richter wacht, liegen Welten.“

Es ist also definitiv sinnvoll, längst verpönte Maßnahmen wie die Vorratsdatenspeicherung oder den „Staatstrojaner“ noch einmal neu zu evaluieren. Denn eins ist klar: Diese Maßnahmen können Leben retten.

Die Schattenseite der Digitalisierung

Ein Kommentar von Marlena Bender

In unserer Informationsgesellschaft sind Daten schon lange keine unbedeutenden Aneinanderreihungen von Nullen und Einsen mehr. Denn wer sie besitzt, hat automatisch auch die Macht darüber – und über uns. Diese Erkenntnis hatte, neben den großen amerikanischen Monopolfirmen wie Google und Facebook, nun auch der deutsche Staat, um sie für die Strafprävention und -verfolgung zu nutzen. Begründet wird dies damit, dass man den Straftätern von heute einem Schritt voraus sein müsse, was nur durch Überwachungsmethoden wie Gesichtserkennung, Vorratsdatenspeicherung oder sogenannte „Staatstrojaner“ möglich sei.



Hier und Titelbild: istockphoto/the-lightwriter

Selbstverständlich wäre es naiv zu leugnen, dass es zur Wahrung der Sicherheit und des Rechtstaates absolut essenziell ist, dass Staatsgewalten wie die Polizei über die bestmöglichen Mittel zur Ausübung ihrer Aufgaben verfügen müssen. Zumal nach richterlichem Beschluss und genauer Abwägung der Rechtslage. Doch müssen wir, als Bürger, wirklich unsere Freiheit und Privatsphäre für ein subjektives Gefühl der Sicherheit riskieren?

Oft wird die staatliche Überwachung von Befürwortern mit der Wahrung der allgemeinen Sicherheit gerechtfertigt, da dies ja bekanntlich eine der Kernaufgaben des deutschen Staates sei. Besonders nach Terroranschlägen wächst der – oft aktionistische – Wunsch nach mehr Sicherheit. Trotz der Angst vieler Menschen sollte darauf geachtet werden, dass solche Probleme nicht für falsche Zwecke instrumentalisiert oder in irgendeiner Weise überdramatisiert werden. Subjektives Sicherheitsgefühl und objektive Sicherheitslage klaffen hier oft auseinander.

Ob die Überwachung überhaupt in dem Maße hilfreich ist, wie es von Befürwortern prophezeit wird, ist fraglich. Besonders gut lässt sich das am Beispiel Frankreichs veranschaulichen. Dort herrscht seit 2015 der Ausnahmezustand: Hausdurchsuchungen werden ohne richterliche Anordnung durchgeführt, zahlreiche Demonstrationen werden verboten und für den Staat ist es wesentlich einfacher, die Bürger zu überwachen, als in Deutschland. Trotzdem ereigneten sich mehrere gewaltsame Terroranschläge mit ungefähr 250 Toten in vier Jahren.

Ginge es nach Bundesinnenminister Horst Seehofer (CSU), würde demnächst auch Gesichtserkennungssoftware an öffentlichen Plätzen eingesetzt werden. Mitte Oktober zog er stolz ein Fazit nach einer Testphase am Berliner Bahnhof Südkreuz, wo ein solches System mehr als 80 Prozent der gescannten Gesichter auch erkannte. In nur 0,1 Prozent der Fälle sei ein Mensch von der Software verwechselt worden. Das klingt doch gut, oder?
ABER: Wie bei dem gesamten Thema liegt das Problem bei den zu Unrecht Verdächtigten. Bei ca. 11,9 Millionen Bahnreisenden pro Tag und nach aktuellem Stand etwa 600 deutschen Gefährdern, von denen, sagen wir, 100 pro Tag mit der Bahn fahren, entstünde folgende Rechnung: Laut Horst Seehofer würden 80 Gefährder (80 %) erkannt werden und von den 11,9 Millionen anderen Menschen täglich nochmals 11.900 (0,1 %) fälschlicherweise für gesuchte Personen gehalten werden. Folglich läge die Wahrscheinlichkeit, dass bei einem Alarm auch ein echter Gefährder erkannt wird, bei 80/11.980, also 0,7 Prozent. Anders formuliert: Etwa 99,3 Prozent der „erkannten“ Personen wären unschuldig und würden zu Unrecht einen Polizeieinsatz auslösen. Nach unserer Rechnung über 350.000 Mal im Monat.

Wikimedia Commons/Dirk Ingo Franke

pixabay

Ein weiterer Ansatz ist, dass künstliche Intelligenz per Vorratsdatenspeicherung in der Lage ist, sich von jedem Bürger, der das Internet in irgendeiner Weise nutzt, eine Art persönliches Profil zu erstellen. Wie bereits Google, Facebook oder Amazon unser Kaufverhalten analysieren, um uns personalisierte Werbung zu senden, können auch Geheimdienste unsere Klicks, Likes und Suchanfragen analysieren. Dazu kommen noch Emailverkehr, WhatsApp-Chats, Instagram-Verbindungen oder Twitter-Follower. Doch was heißt all das für uns „uninteressante“ Durchschnittspersonen? Jeder Algorithmus macht auch Fehler, reißt Teile von Daten aus ihrem eigentlichen Kontext heraus und verdächtigt so möglicherweise Benutzer, die absolut unschuldig sind. Nur ist es diesmal nicht, wie bei dem Beispiel der Gesichtserkennung, mit einer kurzen Polizeikontrolle getan. Stattdessen würde jeder Winkel unserer Privatsphäre durchleuchtet und überwacht. „Staatstrojaner“ würden unsere Handys und Computer infizieren und sogar das Auslesen unserer Festplatten möglich machen. Auch wenn sich dabei herausstellen würde, dass wir unbescholtene Bürger wären; die Beschädigung unserer Privatsphäre wäre nicht mehr rückgängig zu machen.

Auch mag man sich gar nicht vorstellen, was mit diesen Daten in Zukunft passieren könnte, wenn unsere Demokratie nicht mehr so lupenrein wäre und ein Regime nicht mehr das Wohl der Bevölkerung als Ziel hätte. Das mag zunächst eher wie ein dystopischer Science-Fiction-Film klingen, allerdings ist dies bereits mehrfach Realität geworden. Leider sehen wir an zu vielen Beispielen auf der gegenwärtigen Landkarte, wie Menschenrechte von Staaten mit Füßen getreten, eigene Bevölkerungen unterdrückt und die digitalen Medien als Überwachungsinstrument eines totalitären Regimes missbraucht werden.

Apropos Menschenrechte: Eines der gesetzlich festgelegten Persönlichkeitsrechte ist das „Recht auf informationelle Selbstbestimmung“, welches das Recht des Einzelnen beschreibt, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Dazu kommt ebenfalls der gemäß Artikel 13 des Grundgesetzes festgelegte Schutz der Privatsphäre, welcher im Zusammenhang mit diesem Thema von großer Bedeutung ist.

Auch die abgedroschene Phrase, man habe als braver Bürger ja nichts zu verbergen, darf so nicht stehen bleiben. Ein Argument, das etwas unschlüssig erscheint, da wir im realen Leben außerhalb des Internets tagtäglich versuchen, diesen „Schutz der Privatsphäre“ aufrecht zu erhalten. Egal, ob ich meinen Brief in einem Umschlag verschicke, um dafür zu sorgen, dass er auf seinem Weg nicht von zehn Weiteren mitgelesen wird, oder ob ich abends meine Vorhänge zuziehe, damit nicht jeder Passant mir in mein Wohnzimmer schauen kann; das Bedürfnis zu entscheiden, welche Teile des eigenen Privatlebens an die Öffentlichkeit geraten und welche nicht, begegnet uns täglich. Warum sollten wir dieses Recht der Selbstbestimmung in der digitalen Welt plötzlich aufgeben? Was für einen Sinn hat ein solches Persönlichkeitsrecht denn noch, wenn es in diesem bedeutenden Teil unseres Alltags keine Gültigkeit mehr hat?

Die im Grundgesetz niedergelegten Persönlichkeitsrechte sind meiner persönlichen Auffassung nach eine der größten Errungenschaften unserer heutigen Demokratie, die man keinesfalls leichtfertig aufs Spiel setzen sollte. Auch Benjamin Franklin, Gründervater der USA, wusste schon: „Wer die Freiheit aufgibt, um Sicherheit zu gewinnen, wird am Ende beides verlieren.“