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

David Leeuwestein

Die wundersame Kreativität der GesetzgeberInnen

Haben Sie sich schon einmal gefragt, was der Staat eigentlich alles über Sie weiß? Welche verschiedenen Behörden Daten über Sie erheben, verknüpfen und analysieren? Waren sie schon mal verärgert oder verunsichert darüber, dass Sie nicht mehr wissen, welchen digitalen Fingerabdruck sie bei einer Verkehrskontrolle hinterlassen, einer Flugreise, einem Website-Aufruf?

Vermeintliche SicherheitspolitikerInnen erlassen immer mehr Gesetze, um unser digitales und analoges Leben bestmöglich zu überwachen. Polizeigesetze, Vorratsdatenspeicherung und Staatstrojaner bilden nur die Spitze des Eisbergs. Schon längst ist es für Einzelne unmöglich geworden, zu überblicken wie genau sie oder er von wem unter welchen Umständen überwacht werden darf.

Das hat das Bundesverfassungsgericht bereits vor Jahren als Problem erkannt. In seinem Urteil zur Vorratsdatenspeicherung 2010 hielt das Gericht fest, dass eine Vorratsdatenspeicherung zwar nicht per se verfassungswidrig sei, die Überwachung im Kontext bereits bestehender Überwachungsgesetze jedoch ein für die Demokratie gefährliches Maß erreiche. Aus diesem Urteil entstand der Begriff der Überwachungs-Gesamtrechnung.

Wir von Digitalcourage sind überzeugt, dass das für eine Demokratie verträgliche Maß an Überwachung schon lange überschritten ist. Um das zu belegen, pflegen wir schon seit Längerem eine Materialsammlung *(https://digitalcourage.de/ueberwachungsgesamtrechnung)* für eine Überwachungs-Gesamtrechnung, in der wir möglichst alle entstehenden und verabschiedeten Überwachungsgesetze erfassen. Als Absolvent eines Freiwilligen Sozialen Jahres bei Digitalcourage gehörte es zu meinem Aufgabenbereich, diese Übersicht aktuell zu halten.

Kein gutes Jahr

Schon die Gesetze, die in diesem einen Jahr dazugekommen sind, schaden unserer Demokratie empfindlich. Das sind unter Anderem:

- Das *Zensusvorbereitungsgesetz,* das zur Folge hatte, dass sensible Informationen wie Name, Geschlechtsidentität, Familienstand oder Religionszugehörigkeit von allen BundesbürgerInnen im Rahmen eines Testlaufs für den Zensus 21 im Statistischen Bundesamt zentral zusammengeführt wurden – ohne sie vorher zu anonymisieren oder pseudonymisieren. Das Gesetz sieht eine maximale Aufbewahrungsfrist von bis zu zwei Jahren vor.

- Das *Neunte Gesetz zur Änderung des Straßenverkehrsgesetzes,* das Autofahrer mit Überwachung für den Dieselskandal straft, anstatt die Autokonzerne in die Verantwortung zu nehmen.

- Das *European Travel Information and Authorisation System (ETIAS),* welches vorschreibt, dass alle Menschen, die aus Nicht-EU-Staaten einreisen möchten, sofern sie kein Visum benötigen, eine Reisegenehmigung (ETIAS Genehmigung) einholen müssen. Die erhobenen Daten wie Alter, Geschlecht, Nationalität, Gesundheitszustand und vorherige Reisen sollen durch einen Algorithmus auf Risikoindikatoren untersucht und gegen diverse Datenbanken abgeglichen werden.

- Die Ausweitung der EU-weiten Fahndungsdatenbank *SIS II,* die vorgibt, dass bei allen Treffern, die im Zusammenhang mit Terrorismus stehen, ab Ende 2019 die Behörde Europol informiert werden muss. Zusätzlich können nun auch Ermittlungsanfragen gestellt werden. Diese legen Fragen oder Informationen fest, auf deren Grundlage die betroffene Person bei einer Polizeikontrolle befragt wird. Zudem wird der Eintrag von „Rückführentscheidungen abgelehnter AsylantragstellerInnen“ verpflichtend.

- Die *Verordnung zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern,* welche nahezu alle EU-BürgerInnen zur Abgabe von Fingerabdrücken zwingt. *(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R1157)*

- Das Zentralisierte System für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen vorliegen *(ECRIS-TCN),* in dem biometrische Daten (Fingerabdrücke und Passbild) sowie biographische Informationen über alle in der

EU verurteilten StraftäterInnen aus dem Ausland gespeichert werden sollen.

- Das *Urheberrechtsschutzgesetz,* welches Uploadfilter und ein EU-weites Leistungsschutzrecht eingeführt hat. Es ist wahrscheinlich, dass DiensteanbieterInnen auf fertige Lösungen von Konzernen wie Google zurückgreifen werden, um Uploadfilter zu implementieren. Das wird deren ohnehin schon bedrückende Machtstellung weiter ausbauen.

- Zudem wurden zahlreiche Landes-*Polizeigesetze* verschärft. In allen Fällen bedeutet die Verschärfung einen massiven Grundrechteabbau und eine Gefährdung des Rechtsstaats. (Übersicht unter: *https://digitalcourage.de/blog/2018/uebersicht-polizeigesetze*). In Nordrhein-Westfalen führte das Polizeigesetz etwa die Schleierfahndung, mehr Videoüberwachung und Staatstrojaner ein.

Dies sind jedoch nur die Gesetze, die schon verabschiedet wurden und höchstens noch durch Klagen aufgehalten werden können. Zahlreiche weitere Gesetze befinden sich entweder gerade im Verabschiedungsprozess oder sind noch in der Abstimmungsphase.

Die nächsten Jahre werden nicht besser

Zu den geplanten Gesetzesprojekten zählen aktuell etwa:

- Eine Neuauflage der *EU-weiten Vorratsdatenspeicherung:* Bis zu 487 verschiedene Datenkategorien sollen nach dem aktuellen Plan auf Vorrat und verdachtsunabhängig von allen EU-BürgerInnen gespeichert werden. Das diskutiert der EU-Rat zur Zeit. Dazu zählen Standortdaten, Verbindungsdaten u. v. m. Auch Diensteanbieter (OTTs) wie *WhatsApp* sollen von der neuen Vorratsdatenspeicherung erfasst werden.

- Das *Verfassungsschutzgesetz:* Auch Verfassungsschutz und Bundesnachrichtendienst sollen Staatstrojaner einsetzen dürfen. Zudem soll das Mindestalter für Personen, die vom Verfassungsschutz beobachtet werden dürfen, ersatzlos gestrichen werden.

- Der Entwurf eines *Strafrechts-Änderungsgesetzes* – Einführung einer eigenständigen Strafbarkeit für das Betreiben von internetbasierten Handelsplattformen für illegale Waren und Dienstleistungen *(Tor-Verbot):* Der Bundesrat will einen neuen Straftatbestand gegen Betreiber sogenannter *Darknet-Märkte* einführen. Im schlimmsten Fall wird das Betreiben von Tor-Servern illegal.

- Das EU-Vorhaben *TERREG:* Alle Onlinedienste sollen verpflichtet werden, gemeldete Nutzerkommentare innerhalb von einer Stunde offline zu nehmen. Außerdem werden die Diensteanbieter dazu verpflichtet, proaktiv mithilfe von Künstlichen Neuronalen Netzwerken, Hash-Tabellen und Uploadfiltern terroristische Inhalte zu filtern.

- Die geplante *Interoperabilität von EU-Datenbanken:* Fünf große Biometrie-Datenbanken sollen in einem „gemeinsamen Identitätsspeicher" zusammengelegt werden. Dies betrifft die StraftäterInnen-Datenbank ECRIS-TCN, das Visa Information System, das Flüchtlingsregister EURODAC, die Reisedatenbank ETIAS und das noch geplante Entry Exit System (EES). Zudem sollen die Strafverfolgungsbehörden eine Suchmaske erhalten, um alle diese Datenbanken in einem Zug abfragen zu können.

- Der *Detektor für Mehrfachidentitäten:* Er soll die hinterlegten Fingerabdrücke und Gesichtsbilder in den fünf großen Biometrie-Datenbanken der EU (ECRIS-TCN, VIS, EURODAC, ETIAS und EES) durchsuchen und Menschen ausfindig machen, die unter verschiedenen Identitäten erfasst wurden. Das wird automatisch geschehen.

- Der *Eurotrojaner:* Medienberichten zufolge soll Europol mit einem „Eurotrojaner" getauften Staatstrojaner ausgestattet werden. Dieser soll sogar Zero-Day-Sicherheitslücken nutzen.

- Das EU-Vorhaben *Tensor:* Im Rahmen dieses Projekts forschen europäische Polizeibehörden und Rüstungsfirmen an Uploadfiltern, die auch unbekannte terroristische Inhalte erkennen und entfernen sollen. Die EU-Kommission hat dafür fünf Millionen Euro bereitgestellt.

- Der *Cloud-Act:* Polizei- und Justizbehörden sollen zukünftig leichter auf Cloud-Daten in den USA zugreifen. Umgekehrt könnten auch US-Behörden direkt bei europäischen Internetfirmen anklopfen.

- Das *zweite „Datenaustauschverbesserungsgesetz":* Das Mindestalter zur verpflichtenden Abnahme von Fingerabdrücken Geflüchteter soll von 14 auf sechs Jahre gesenkt werden. Zudem sollen lokale und Länderbehörden das Ausländerzentralregister mit eigenen Daten anreichen dürfen. Auch die Zugriffsbefugnisse für Behörden (insbesondere Sicherheitsbehörden) werden massiv ausgeweitet.

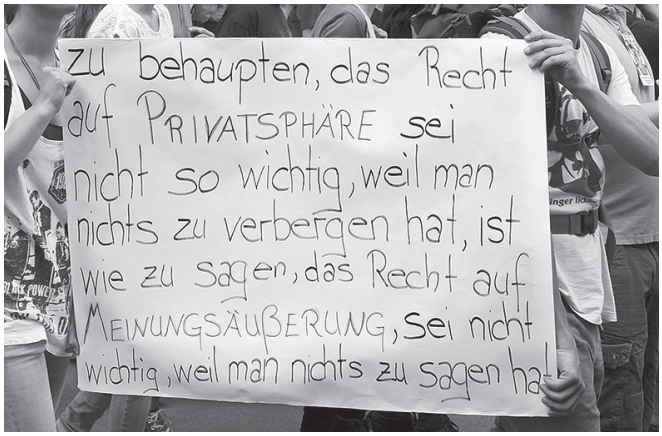
- Die *E-Evidence-Verordnung:* Betreiber von Internet-Diensten sollen Daten ihrer NutzerInnen künftig direkt und mitun-

David Leeuwestein

David Leeuwestein kommt aus einer Kleinstadt inmitten des digitalen Niemandslandes Brandenburg. Dennoch kam er früh mit den Themen Datenschutz, IT-Sicherheit und Hacking in Berührung. Sein Interesse für Politik lebte er zunächst in einer Lokalzeitung aus. Er unterstützte das Digitalcourage-Team 2018 und 2019 als Freiwilliger im FSJ.

ter innerhalb von sechs Stunden für Behörden aus allen EU-Ländern zugänglich machen. Andernfalls drohen Strafen von bis zu 2 % des Jahresumsatzes. Vorbild für das Gesetzesvorhaben ist der Cloud-Act in den USA.

Eine vollständige Übersicht unserer Sammlung finden Sie auf unserer Website: *https://digitalcourage.de/ueberwachungsgesamtrechnung/sammlung*. Wir freuen uns über Hinweise und Ergänzungen.



Das Recht auf Privatsphäre, Foto: Günther Gerstenberg

Wie die Erfahrung zeigt, werden Überwachungsgesetze gerne ergänzt und ausgebaut, jedoch fast nie zurückgenommen. Mittlerweile erreicht der Überwachungswahn ein Maß, das auch für eine kritische Öffentlichkeit nur noch schwer zu überblicken ist. Ohne die unermüdliche Arbeit von Journalistinnen, Politikern und Aktivistinnen wäre unsere Materialsammlung niemals zu ihrer jetzigen annähernden Vollständigkeit gelangt.

Doch nicht nur die Erfassung bekannter Überwachungsvorhaben ist eine immense Herausforderung, immer öfter liegt die Aufgabe auch darin, solche Vorhaben ausfindig zu machen.

Unserer Veröffentlichung interner Dokumente über eine Neuauflage der EU-weiten Vorratsdatenspeicherung ging etwa ein monatelanger Rechercheprozess voraus, in dem wir zahlreiche Dokumente von Behörden angefragt und ausgewertet haben. In der Vergangenheit waren diese Recherchen zudem immer von rechtlichen Auseinandersetzungen mit verschiedenen Behörden begleitet, da diese die Herausgabe entscheidender Dokumente verweigerten.

Auch vermeintliche Pro-Datenschutz-Gesetze entpuppen sich zunehmend als Kompetenzgeber für Datenkraken. So droht etwa die aktuell verhandelte E-Privacy-Verordnung zu einer Hintertür für eine private Vorratsdatenspeicherung zu werden: Diensteanbietern soll das Speichern möglichst attraktiv gemacht werden, sodass die freiwillig gespeicherten Daten lediglich noch nach bereits geltendem Recht angefragt werden müssen.

Was wir fordern

Dem bereits 2010 vom Bundesverfassungsgericht geforderten Prinzip der Überwachungs-Gesamtrechnung schenkt der Gesetzgeber dabei bis heute keine Beachtung. Somit fehlt der Öffentlichkeit ein entscheidendes Werkzeug, um neue Überwachungsgesetze bewerten zu können. Sie weiß schlicht nicht mehr, wie sie sich ins Gesamtmaß staatlicher Eingriffe einfügen. Besondere Risikogruppen wie AnwältInnen, Journalisten oder AktivistInnen fallen in dem Diskurs sowieso unter den Tisch.

Wir fordern daher, dass der Gesetzgeber sich endlich an die bereits seit 2010 bestehenden Vorgaben des Bundesverfassungsgerichts hält und bei jedem neuen Überwachungsgesetz

1. eine Auflistung aller bestehenden Überwachungsgesetze vorlegt, und

2. begründet, warum dieses neue Vorhaben dennoch zielführend, notwendig und verhältnismäßig ist.

Und wir fordern echte Sicherheitspolitik statt Überwachung: Investieren in Gesundheit, Bildung, Wohnraum und soziale Sicherheit. Es darf nicht sein, dass vermeintliche SicherheitspolitikerInnen mit euphemistischen Gesetzesnamen oder mit kurzfristigen Änderungsanträgen der Bevölkerung Überwachungsmaßnahmen unterschieben. Das für eine Demokratie kritische Maß an Überwachung ist schon lange erreicht.

Frank Herrmann

Denn sie wissen nicht, was sie tun. Oder doch?

Es liegt im Wesen der Überwachung, dass sie für sehr lange Zeit weit weg, ja unsichtbar bleibt, jedoch ganz plötzlich wahrgenommen wird, wenn sich eine persönliche Betroffenheit einstellt. Und es liegt im Wesen der Politik, vor allem der Regierungspolitik, dass für aktuelle Probleme meist die schnelle Aufmerksamkeit und kurzfristige Lösungsversprechen im Vordergrund stehen, denn die nächste Wahl steht immer irgendwo vor der Tür.

Nicht die besten Voraussetzungen für ein Parlament, im täglichen Politikbetrieb auch die noch nicht offensichtlichen Auswirkungen beschlossener Gesetze wahrzunehmen und bei der weiteren Gesetzgebung zu berücksichtigen. Doch genau das wäre die Aufgabe, zu der das Bundesverfassungsgericht den Gesetzgeber verpflichtet. Es verlangt von ihm den „Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen“[1], wenn er weitere Datenspeicherungspflichten plant, also die Betrachtung in einer Überwachungs-Gesamtrechnung. Aber wer soll diese aufstellen? Und wer hat überhaupt ein Interesse daran?