et dona ferentes

Schlechte Argumente des bürgerlichen Datenschutzes

> Seit Enthüllungen, nach denen auch höchste Repräsentant_innen unseres Staates nicht immun gegen Bespitzelung sind, gibt es kaum noch eine Rettung vor Bekenntnissen zu Datenschutz, Vertraulichkeit und Privatsphäre, meist nicht viele Atemzüge entfernt von genauso flammenden Bekenntnissen zu flächendeckenden Bewegungs- und Kommunikationsprofilen, DNA-Abgleichen, Gewalttäterdatenbanken, Videoüberwachung und Rasterfahndung. Wie das zusammengeht und warum argumentative Figuren, die sowas erlauben, nichts für uns sind, das wollen wir in diesem Artikel untersuchen.

Die Familie von Glaubenslehren, die auch Bürger_innen ein gewisses Recht auf Geheimhaltung zubilligt, Näheres jedoch „durch ein Bundesgesetz“ geregelt sehen will – was nach dem Vorbild vieler grundgesetzlicher Rechte „eingeschränkt“ heißt –, bezeichnen wir hier kollektiv als „bürgerlichen Datenschutz“. Er speist sich aus zwei widersprüchlichen Wurzeln: Zum einen einem Staatsbegriff, in dem es „ein Volk“ gibt und dieses einen Willen hat, der sich wiederum in den Organen des Staates reflektiert. Diese Sekularreligion führt, konsequent umgesetzt, praktisch sofort zu finsterster Unterdrückung und Blutbädern. Daher traten seit Beginn dieser Sorte Staat dazu Menschenrechte, also fundamentale Garantien für alle Individuen gegenüber dem Kollektiv, also bei uns dem Staat.

Klar geht diese Logik – Individuen brauchen Schutz gegenüber der Manifestation ihres gemeinsamen Willens – nicht ganz zusammen, aber so kleine Widersprüche muss mensch aushalten als gute_r Staatsbürger_in. Und das ist auch schon der Knackpunkt: Im bürgerlichen Datenschutz wird unterstellt, der Staat sei im Prinzip gut, auf magische Weise komme es aber manchmal zu Exzessen, auf die der Staat hingewiesen werden muss, damit er sie in Ordnung bringen kann.

magis amica veritas

Um demgegenüber zu einer vernünftigen Interpretation des unbegrenzten staatlichen Informationshungers zu kommen, braucht es offenbar eine etwas widerspruchsärmere Grundlage. Schon wegen der strömungsübergreifenden Natur der Roten Hilfe wollen wir uns auf keine spezifische Staatstheorie festlegen, doch allen ernstzunehmenden gemeinsam ist sicher das Modell einer vielstufigen Herrschaft. Der Begriff darf ruhig recht allgemein gefasst werden: Die Lehrer_in herrscht über den Schüler_in, der Polizist_in über die Ladendieb_in, die Kanzler_in über jedenfalls ziemlich viele der anderen.

Das reicht bereits, um die Rolle des Datenschutzes zu definieren. Wer nämlich in der Hierarchie oben steht, möchte nach unten alles durchblicken („Transparenz“). Hauptantrieb dabei ist der permanente Verdacht der Herrschaft, die Untertanen würden sich zu Ungehorsam und Rebellion verschwören, recht unabhängig vom aktuellen Stand der Umsturzpläne. Auf der anderen Seite ist Machtausübung fast aussichtslos, wenn Entscheidungsprozesse und -prinzipien tatsächlich transparent sind, weshalb Herrschaft großes Interesse hat, von unten nicht durchschaubar („opak“ mit dem schönen Substantiv „Opazität“ ist der akzeptierte Gegenbegriff zu „transparent“) zu sein – daher ja auch die zahlreichen Regeln zur Geheimhaltung, Sicherheitsüberprüfungen für den Apparat und die Verbissenheit im Kampf gegen Lecks.

Demgegenüber möchten sich auf jeder Stufe die Untertanen ungern von oben zugucken lassen – ob heimlich Abschreiben in der Schule oder Abrüstungsmaßnahmen in Heimwerker_innenmanier, je weniger die Obrigkeit merkt, desto größer sind die Handlungsspielräume. Umgekehrt würden die Untertanen aber gerne wissen, wie sie bespitzelt werden und welche Kriege sie demnächst ausfechten sollen, sie haben also ein großes Interesse an einer möglichst transparenten Obrigkeit.

Mithin ist radikaler Datenschutz die Forderung nach

maximaler Transparenz von unten nach oben und maximaler Opazität von oben nach unten. In der Tat gestehen auch bürgerliche Theoretiker_innen ein, das sei eine Bedingung für „Freiheit“, was im Übrigen auch erklärt, wie sie darauf kommen, „Sicherheit“ sei ein Gegenbegriff dazu: Da der Staat für sie eine Art Emanation des Volkes ist, ist Sicherheit des Volkes die Sicherheit des Staates, also der Herrschaft, und verlangt darum im Gegenteil Opazität nach oben und Transparenz nach unten. Zumindest soweit hat ihre Denke Stringenz.

Nun aber zu den Argumentfiguren dieser Leute; in den Figuren könnt ihr X jeweils durch eines der zahlreichen aktuellen Staatsprojekte zur Durchleuchtung der Untertanen ersetzen: Vorratsdatenspeicherung, Biometrie, Antiterrordateien oder was immer.

(1) cui bono?

Die Figur: „X wirkt nicht“.

Feststellungen dieser Art sind erstaunlich oft wahr. So gibt es beispielsweise einen großen Korpus von Studien, nach denen der einzig nachweisbare Nutzen von Videoüberwachung eine Reduktion im Autodiebstahl auf Parkplätzen ist – und der zudem wohl eher aus dem Extralicht für die Kameras resultiert. Wer in Politgrüppchen unterwegs ist, wird wohl auch schon gefeixt haben über fehlerhafte, ja völlig abwegige Vorstellungen, die Staatsorgane trotz all ihrer Datenbanken, Ausweise und Spitzel entwickeln. Und noch bevor Nacktscanner an Flughäfen in aller Welt ausgerollt wurden, war in einer Fernsehshow zu bewundern, wie trotzdem allerlei entführungstaugliches Material an Bord zu schmuggeln wäre.

So verpuffen selbst atemberaubende Menschenrechtsverletzungen häufig fast wirkungslos, vielleicht wegen Intrigen im Apparat, vielleicht, weil Hierarchien in individuelle Inkompetenz treiben, oft, weil die Versprechen (oder eher Drohungen) von vorneherein maßlos aufgeblasen waren. Dennoch greift das mit dem „nicht wirken“ zu kurz: Der Kram wirkt in aller Regel nicht *wie vorgeblich gewünscht*.

Denn selbst wenn Videoüberwachung nicht Kriminalität reduziert, hat natürlich das Bewusstsein, dass die Obrigkeit jede Handlung potenziell sieht und, noch mehr, mit Aufzeichnung auch jederzeit in die Vergangenheit blicken kann, drastische Konsequenzen für kleine Regelüberschreitungen – sagen wir, Plakatieren oder vielleicht auch das Außerbetriebsetzen von Überwachungseinrichtungen –, die in der politischen Praxis jenseits staatsaffirmativer Rituale unverzichtbar sind.

Potenziell katastrophal schädlich wird die Figur aber, weil daraus abgeleitete Argumente zusammenbrechen, wenn die Obrigkeit die Wirkung nachweist oder jedenfalls behauptet. Vorratsdatenspeicherung oder Folter sind eben auch dann inakzeptable Unterdrückungsinstrumente, wenn sie zur Aburteilung von zwei Dschihadisten oder zweitausend Raubkopierern führen.

Argumentativ sollte bei solchen Gelegenheiten („aber du kannst doch all die Vergewaltiger nicht laufen lassen“) angemerkt werden, dass bei den wirklich konsensfähig schlimmen Verbrechen die Aufklärungsquoten gewiss nicht durch Eingriffsbefugnisse der Polizei, sondern durch deren Interessenlage beschränkt sind. Mensch erinnere sich nur an die 745 „unaufgeklärten“ Mordfälle, die sich die deutsche Polizei im Dezember 2013 wieder vornahm, nachdem sie im Nachgang der NSU-Affäre einfach mal einen „Kriterienkatalog“ (also: Nix Data Mining) zur Identifikation von Nazimorden durchgegangen war. Solche Punkte sind wichtig als Illustration, dass der Apparat Teil des Problems ist und seine Aufrüstung gewiss nicht die Lösung.

Also: Im radikalen Datenschutz gilt es, der Obrigkeit die Instrumente zur Unterdrückung zu verweigern, selbst wenn sie damit *auch* mal Dinge tun kann, die wir nützlich finden.

(2) nulla poena

Die Figur: „X trifft vor allem Unschuldige“.

Ganz fraglos gehört zu den besonders verstörenden Aspekten des neoautoritären Umbaus der fast schon selbstzerstörerische Übergriff auf eigentlich loyale Subjekte, in diesem Sinne also Unschuldige. Vernünftigerweise meldet der bürgerliche Datenschutz Einspruch an, wenn der Staat, sagen wir, Millionen Auslandsüberweisungen untersucht und speichert oder die dietätischen Präferenzen aller Flugpassagiere mit ihren Kreditkarten korreliert. Klar geraten all die Überweiser und Flieger „unter Generalverdacht“. Noch dramatischer ist die Lage bei flächendeckender Erfassung von Gesichtern und Fingerabdrücken – die erkennungsdienstliche Behandlung „Schwerkrimineller“ von gestern ist, von ein paar technischen Details abgesehen, Standard für alle Untertanen heute.

Der wohlmeinende Einspruch erstreckt sich auch auf die Einführung einer neuen Klasse, nämlich der der amtlich potenziell Schuldigen. Dabei allerdings kleinlautet der bürgerliche Protest üblicherweise zu einem

„also gut, wenn ihr es in Einzelfällen denn mal müsst“. Diese Einzelfälle sind Menschen, bei denen es für die Eröffnung eines Gerichtsverfahrens oder gar eine Verurteilung vorne und hinten nicht reicht, die aber dennoch in Polizeidatenbanken landen, weil „kriminologische Erfahrung“ oder vergleichbarer Hokuspokus künfige Verbrechen „erwarten lassen.“ Die Unentschlossenheit beim Protest gegen diesen grassierenden Wahnsinn ist um so weniger verständlich, als solche Speicherungen jedenfalls gelegentlich schon zu massiven Nachteilen (z.B. ständige schikanöse Kontrollen, Ausreisebeschränkungen, Benachteiligung im Job, Ausforschung des sozialen Umfelds) führen, von Menschen, die auf opportunitätgesteuerten Terrorlisten landen mal ganz zu schweigen.

Radikaler Datenschutz sollte sich aber nicht mit einer Kritik der Willkürlichkeit aufhalten; dieser Kram wird nicht besser, wenn die Obrigkeit ihre Gesetze so anpasst, dass allerlei Verhalten dann eben doch justiziabel wird – im Gegenteil, wenn mensch an die Definition von Gedankenverbrechen im Rahmen von 129a oder auch der Gesetzgebung gegen „Hassprediger“ denkt.

Nein, der Punkt ist, dass wir schuldig *sind* und genau *deswegen* der Staat keine Listen und Dossiers über uns anlegen soll. Linke Politik, egal welcher Strömung, hat immer mit Emanzipation zu tun, also mit Schwächung der Hierarchie. Ob nach Gesetz oder nicht, aus Sicht der Obrigkeit *muss* das Schuld sein, auch wenn es konkret vielleicht nicht gleich nicht um Aufstand und Revolution geht, sondern nur um etwas mehr Freiheit, Gleichheit und Solidarität.

Wir haben also etwas zu verbergen, und drum muss unser Argument sein, dass im Interesse der Entwickelbarkeit der Gesellschaft die Mittel der Obrigkeit, uns auszuforschen und in der Folge mit oder ohne Gesetz zu unterdrücken, so schwach gehalten werden wie wir das eben durchsetzen können.

(3) quis custodiet?

Die Figur: „X darf auf keinen Fall für Y verwendet werden.“

Es ist zum Haareausraufen, wie sehr sich der bürgerliche Datenschutz nach eigentlich jeder Niederlage auf die Schultern klopft, da am Ende doch alles gerettet ist: Die Fingerabdrücke werden nur im Pass gespeichert und nicht zur Strafverfolgung verwendet, die Personalausweisbilder nur bei der Gemeinde und nicht... halt, die werden jetzt doch schon zur Strafverfolgung verwendet, aber *am Anfang*, da war alles gut, die Bilder von den Mautkameras, den Ampelkameras, der große Lauschangriff nur für ganz schreckliche, Verbindungsdaten wie Inhalte, Staatstrojaner nicht im Kernbereich und DNA-Daten, klar, nur die ganz Bösen, Gerichtsvorbehalt und SWIFT-Daten kontrolliert Europol, eh schon keine Aufzeichnung... eine Kakophonie, die nicht mehr reflektiert als die Salamitaktik von oben.

Keine Frage: Es ist immer gut, wenn obrigkeitliches Handeln beschränkt wird. Nur: Eine skandalöse Erweiterung herrschaftlicher Befugnisse im Nachhinein als Beschränkung zu verkaufen ist nichts als Beihilfe zur Propaganda der Obrigkeit. Dazu kommt, dass die Beschränkungen im Nachhinein entweder ignoriert werden (etwa, was die Voraussetzungen zur Speicherung in Polizeidatenbanken angeht, solange niemand hinguckt), sie irgendwann aufgehoben werden (etwa bei Telekommunikationsverbindungsdaten oder der Aufzeichnung von Videosignalen), oder weil gleich Schlupflöcher in die Gesetze geschrieben werden. Ein schlagendes Beispiel für letztere Taktik ist die DNA-Analyse, vor der an sich ein Gericht das Vorliegen der halbwegs strikten Voraussetzungen feststellen müsste. 90% der Daten in der einschlägigen BKA-Datenbank sind aber ohne gerichtliches Nicken eingespeist worden. Möglich ist dieses Wunder, weil bei „freiwilliger“ Entnahme einfach so analysiert werden darf. Keine Frage, 90% der Untertanen lieben ihre Obrigkeit freiwillig.

Aber auch, wo es keine derartigen Freiwilligkeitsklauseln gibt, zeigt sich fast durchweg, dass Kontrolle nicht funktioniert. Wenn ein Gericht in Kenntnis des Versammlungsrechts und der Beschränkungen zur Nutzung von Verbindungsdaten die Funkzellenabfragen in Dresden *(nicht, wie peinlicherweise gedruckt, Leipzig – Hrsg.)* genehmigt – es landeten nicht nur Millionen von Verbindungen, sondern auch noch irrsinnige 40000 den Anschlüssen zugeordnete Personen in Polizeicomputern –, ist wirklich fraglich, was denn abgelehnt würde. Noch frivoler ist die Situation, wenn, wie bei den internationalen Überweisungen, ausgerechnet ein Geheimpolizei-Moloch wie Europol mit der Prüfung der Rechtmäßigkeit von Datenübertragungen beauftragt wird.

Nein, radikalem Datenschutz kann es nie um die Einschränkung der Nutzung von Daten gehen, Daten dürfen schlicht gar nicht erhoben und schon gar nicht gespeichert werden. Abgesehen von der eben disku-

tierten langfristigen Aussichtslosigkeit obrigkeitlicher Selbstbeschränkung war nämlich jedenfalls historisch noch jede Obrigkeit so opak, dass das schlichte Vorhandensein von Daten bereits für die einschüchternde Wirkung sorgt („das machen die doch bestimmt. . . “). Die gegenwärtigen Obrigkeiten sind es in jedem Fall.

(4) amantes, amentes

Die Figur: „X erlaubt Einblicke in den Kernbereich der persönlichen Lebensgestaltung.“

Diese Figur könnte als Variante von (3) gelesen werden: „Obrigkeitlicher Durchgriff muss beschränkt werden“ – oder vielleicht auch von (2): „Im Herzen der Menschen ist die Unschuld daheim“. In der Tat aber illustriert kaum ein Begriffspaar den Niedergang bürgerlichen Datenschutzes besser als der zwischen der „informationellen Selbstbestimmung“ des Volkszählungsurteils in den frühen 80ern und dem des „Kernbereichs“ aus dem Urteil zum großen Lauschangriff Mitte der Nullerjahre – leitet ersteres aus den Menschenrechten die Förderung politischer Partizipation ab und ist so für radikalen Datenschutz zumindest anschlussfähig, rekurriert letzteres auf neblige Konzepte von „Persönlichkeit“, vielleicht gar „Schamgrenzen“.

An diesem Typ Argument ist wirklich alles schief. Erstens ist ja schon nicht einzusehen, warum es irgendeiner Menschenwürde helfen soll, wenn der Bulle den Beziehungsstress in der fiesen Polit-WG zwar mitschneidet und feixt, ihn danach aber immerhin wieder löschen muss. Zweitens war wohl niemand überrascht, als z.B. beim Staatstrojaner rauskam, dass noch nicht mal die technischen Voraussetzungen für diese Löschung vorhanden waren, von der tatsächlichen Durchführung ganz zu schweigen.

Vor allem aber: Letztlich kann es aufgeklärten Menschen eigentlich wurst sein, wer ihnen beim Stuhlgang oder beim Sex zusieht, um mal zwei Felder zu nennen, die das Bundesverfassungsgericht wohl klar seinem Kernbereich zuordnen würde; deswegen nämlich gibts keine Hausdurchsuchung, keinen Knast oder andere Repressalien. Die gibt es aber durchaus als Folge der Ausforschung von politischen Aktivitäten. Und drum gehts radikalem Datenschutz nicht um den Kernbereich der *persönlichen* Lebensgestaltung. Sondern um die ganze beschissene Bäckerei, vom Umtopfen bis zur Umsturzplanung.

ceterum censeo

Eine schöne Kritik bürgerlicher Überwachungskritik, vor allem des Youtube-Hits „Überwachungsstaat – was ist das?“ hat das Seminar für angewandte Unsicherheit auf http://unsicherheit.tk/359 ins Netz gebracht; wir können den Text nur warm empfehlen.

All das soll übrigens nicht heißen, dass die bürgerlichen Datenschützer_innen unsere Feinde wären – wobei wir den Eindruck nicht verhehlen wollen, dass die Ämter der Datenschutzbeauftragten in den letzten Jahren fast durchweg mit Sockenpuppen des sicherheits-industriellen Komplexes besetzt wurden und daher immer weniger als Verbündete in Frage kommen. Es soll aber sehr wohl heißen, dass Datenschutz nichts ist, das wir Sabine Leutheusser-Schnarrenberger oder Thilo Weichert überlassen können, und übrigens auch nicht dem CCC.

Datenschutzgruppe der Roten Hilfe Heidelberg

Kontakt und Artikel-Archiv: http://datenschmutz.de

PGP Fingerprint: a3d8 4454 2e04 6860 0a38 a35e d1ea ecce f2bd 132a