1. Überwachen und Strafen

- Der autoritäre Staat
- Verschwörungen
- Beispiele
- Wer, warum und wogegen?

2. Der autoritäre Staat

Das Jahrzehnt nach 1995 war geprägt duch eine atemberaubende Selbstermächtigung des Staates. Ein paar Stichwörter:

Lauschangriff, endlose Präventivbefugnisse der Polizeien, faktische Abschaffung von Art. 16 GG, Otto-Katalog, ausufernde Telefonüberwachung, DNA-Datenbank samt Massenerfassungen, eskalierende Geheimhaltung, Schleierfahndung, Zusammenarbeit der Polizeien, Sicherungsverwahrung, Polizeiverordnungen, Internetsperren, Militarisierung nach innen und außen, biometrische Erfassung der Bevölkerung, Staatstrojaner, Aufrüstung der Geheimdienste, internationaler Datenaustausch, üble Versammlungsgesetze, Rütteln am Folterverbot...

Seit der zweiten Hälfte der Nullerjahre ist das Tempo zumindest in der BRD etwas gemäßigter geworden, teils auch, weil die „Zivilgesellschaft“ ein wenig wacher geworden ist (z.B. Freiheit statt Angst). An der Grunddiagnose ändert sich dadurch nicht viel: Der Staat wird immer autoritärer.

Bei all dem werden Kontrolltechnologien immer wichtiger.

3. Verschwörungen

Vorab: „Sie“ ist nicht ein geschlossener Block. Es handelt sich um wechselnde Koalitionen von

- BKA, Landespolizeien
- Bundesinnenminister, Länderminister
- diverse Industrien (Telekoms, IT, Content, Waffen, Überwachtungstechnologie)
- Geheimdienste
- Militär
- Andere Teile von Obrigkeiten

In jedem Einzelfall ist zu klären, wer da was warum betreibt. Im Rahmen dieses Rundumschlags kann ich das natürlich nur ansatzweise, und sobald Technologie ins Spiel kommt, wird das noch komplizierter, weil die „Entscheider“ meist reichlich unzutreffende Vorstellungen vom Gegenstand ihrer Entscheidung haben.

Beispiele für Interessenkonflikte: Kryptografie, VDS, „Anti-Terror“-Datei.

Insbesondere *gibt* es noch einen Rechtsstaat, und weite Teile von „Ihnen“ möchten den auch auf jeden Fall behalten (vgl. unten). Das weiß insbesondere das Verfassungsgericht (niedrigere Instanzen zwar tendenziell weniger, aber doch auch), das etliche der erwähnten Projekte und Maßnahmen kassierte oder jedenfalls deutlich einschränkte.

Die Widersprüche innerhalb der der PlanerInnen des autoritären Staats sind unsere Chance, politisch einzugreifen. Demgegenüber sind technische Maßnahmen zwar unter Umständen wirksam, aber keine Dauerlösung, da sie (a) unsere Arbeit schwerer machen, (b) meist erhebliche Sachkenntnis verlangen, wenn sie effektiv sein sollen und (c) häufig auch durch gesetzliche Regularien ausgehebelt werden können (z.B, Krypto-Verbot in Frankreich, Angriffe auf TOR-Server).

Die autoritäre Formierung ist ein politisches Problem und muss in erster Linie politisch bekämpft werden.

4. Beispiel Staatstrojaner

Die Ermächtigung der Obrigkeit, in Rechner der Untertanen einzubrechen.

Wahlweise um Verschlüsselung zu umgehen („Quellen-TKÜ“) oder um Daten vom Rechner zu ziehen („Onlinedurchsuchung“). In autoritären Kreisen wird um die Unterscheidung großes Gewese gemacht, da die Anlassstraftaten sich leicht unterscheiden. Im Politbereich mit dem Universalkampfmittel 129ff ist das aber von vorneherein nur Barock, und ohnehin ist die Ermächtigung zu derartigen klandestinen Operationen selbst das Problem, und rechtstechnische Einschränkungen ändern am zugrundeliegenden Konzept nichts.

Staat installiert Schnüffelsoftware bei Zollkontrolle, Wohnungseinbruch, durch Ausnutzen geheimgehaltener Sicherheitslücken.

Ozapftis: „Weiter privat über Liebe“, Digitask, Nachladen, Scheunentore.

Das Wort „Durchsuchung“ ist hier dreistes Neusprech. Der Staatstrojaner ist weit übler als die ohnehin schon stark destruktiven Hausdurchsuchungen, weil bei letzteren die Opfer immerhin wissen, wenn es sie erwischt. Die riesige panoptische Wirkung des Staatstrojaners kommt hingegen davon, dass jedes komische Verhalten des Rechners sofort Angst, Schrecken und in der Folge nicht selten Selbstzensur folgt. Das ist Foucaults panoptisches Prinzip in Reinkultur, da real der Staatstrojaner (von den Polizeien) über ein paar Jahre hinweg nur in einigen Dutzend Fällen eingesetzt wurde.

5. Beispiel Vorratsdatenspeicherung

Telekoms speichern, wer wann mit wem von wo wie lange telefoniert oder gemailt hat. VDS verpflichtet sie, die Daten 6 bis 24 Monate vorzuhalten, ohne VDS tun sie das zwischen 7 und ca. 100 Tagen.

Polizei darf diese Daten für Personen oder „örtlich und zeitlich hinreichend genau bestimmt“ (Funkzellenabfrage) bestellen. Z.B. zu Dresden 2011: ca. 2 Mio Verbindungen, fast 100000 Anschlussinhaber_innen.

Die VDS als Zwangsregelung geht auf eine EU-Richtlinie zurück, die unter maßgeblicher Beteiligung deutscher Sicherheitsfanatiker durchgedrückt wurde und inzwischen vom EuGH kassiert wurde. Während der Planungsphase wollten die Behörden ursprünglich „alle“ Verbindungen, auch die erfolglosen, speichern lassen, was speziell im Internetbereich völlig wahnsinnig wäre (DNS-Abfragen, ICMP-Nachrichten...). Allein der Plan illustriert, dass die Obrigkeit oft nur sehr nebulöse Vorstellungen hat, wovon sie redet. Auf Druck der Telekoms wurde die Richtline auf das zusammengestutzt, was sie jetzt ist.

Zwei Propagandafiguren, die bei der VDS eine große Rolle spielten, deren komplette Wertlosigkeit aber das Beispiel Dresden gut illustriert: Richtervorbehalt; Einschränkung auf „erhebliche“ oder mittels TK begangene Straftaten.

Wieder: Panoptikum – alle wissen, dass der Staat sofort rauskriegen kann wo sie waren und mit wem sie geredet haben.

6. Beispiel Data Mining

„Rasterfahndung auf Steroiden“ – der Versuch, Strukturen in großen Datenmengen zu erkennen. Man sammelt alles, was man an Daten bekommen kann: Polizeidaten, Kommunikations- und Bewegungsprofile, Kontodaten, Konsumdaten usf.

- Supervised Data Mining: Man nimmt bekannte Zecken, lässt den Rechner Merkmale identifizieren, mit denen man nach neuen Zecken sucht.
- Unsupervised Data Mining: Der Rechner guckt aufs Geratewohl, was es an Struktur in den Daten gibt – danach können Menschen überlegen, ob Teile dieser Struktur zeckig aussehen.

Methoden aus diesem Bereich können auch anderen Zwecken dienen – beispielsweise der Aufdeckung der Verwendung mehrerer Identitäten, das Säubern von Datenbeständen von bewusst oder versehentlich falsch erhobenen Daten usf. Das Ausleuchten von Strukturen ist aber wohl das, was die Staatsgwalt gegenwärtig am aufrgendsten findet.

Gegenwärtig auf staatlicher Seite erst in Ansätzen entwickelt (Hartz IV!), vor allem vom Datenschutzrecht behindert – aber alle investieren eifrig.

7. Beispiel Datenbanken

Geführt von Diensten (NADIS), BKA (INPOL), LKAen, verstärkt auch europäische Stellen (SIS); dazu AZR, BZR, ZEVIS, Meldeämter usf, weitere Unterfütterung durch Banken, Renten-, ggf. Krankenversicherung usf.

Sollten Datenschutzprinzipien unterliegen: Finalitätsprinzip, Datensparsamkeit, Fristbindung.

Klassisch: Auskunftsdatenbanken (operativ, dispositiv; z.B. diverse POLAS, DAD, KAN, AFIS usf.). Schwer im Kommen: Vorgangsverwaltungen, Fallbearbeitungen.

Auskunftsanspruch: Zur informationellen Selbstbestimmung gehört, dass BürgerInnen wissen, wer was über sie gespeichert hat.

8. Beispiel Anti-Terror-Datei

Gemeinsame Datei von Geheimdienst und Polizei.

„Erhobene“ Daten der beteiligten Behörden zu „Extremist_innen“ UnterstützerInnen, ihren Bekannten („Kontaktpersonen“) und „Sachen“, die damit zu tun haben.

Grunddaten: Daten zur Identifikation, „Fallgruppe“

„Erweiterte Grunddaten“: Kontonummern bis Ausbildungsgang, insbesondere auch Religion, „Volkszugehörigkeit“, Freitextfeld.

Schon das Wort „Erweiterte Grunddaten“ deutet darauf hin, dass hier ein Kompromiss vorliegt: Die Geheimdienste wollten allenfalls eine „Indexdatei“, in der höchstens drinsteht, *dass* sie etwas über wen wissen, aber nicht, *was*. Die Polizei wollte möglichst umfangreichen Zugriff auf das (vermutlich herbeifantasierte) „Wissen“ der Dienste. Das Ergebnis ist die vorliegende Kompromissformel, bei der auf die „Erweiterten Grunddaten“ außer im Eilfall nur mit Einwilligung der einstellenden Behörde zugegriffen werden darf.

Ursprünglich war die Datei auf ausländische Terrorist_innen beschränkt, nach NSU wurde dann auf „Rechtsextremisten“ erweitert, die Ausdehnung nach links ist nur eine Frage der Gelegenheit.

Zusätzlich: Verdeckte, beschränkte Speicherung.

Das GDG erlaubt weitere gemeinsame Dateien von Diensten und Polizeien ohne parlamentarische Beratung, d.h. unter Ausschluss der Öffentlichkeit.

9. Was passiert hier?

Modell 1: Obrigkeit und Untertanen. Die Interessen der Spieler sind leicht zu durchschauen: Herrschende wollen herrschen. Dazu brauchen sie Kontrolle, und dafür brauchen sie so viel Information über die Beherrschten wie möglich – sie wollen transparente Beherrschte. Dass dies dabei hilft, Bedrohungen ihres Status als Herrschende frühzeitig zu identifizieren und dann mit relativ wenig Aufwand zu eliminieren, ist ein angenehmer Nebeneffekt. Auf der anderen Seite ahnen die Herrschenden, dass die Beherrschten ihre Handlungen in der Regel nicht so toll finden – deswegen wollen sie lieber opak sein.

Umgekehrt wollen die Beherrschten nicht, dass ihr Leben in allen Einzelheiten durchleuchtet wird, schon, weil das z.B. erlaubt, UnruhestifterInnen zu identifizieren und mithin ihre Partizipationsmöglichkeiten reduziert – also wollen auch sie lieber opak sein, was sich mit dem Wunsch nach ihrer Transparenz von Seiten der Herrschenden schlecht verträgt.. Sie würden aber gerne wissen, was die Herrschenden für sie ausbrüten, wollen also transparente Herrschende.

Dieser fundamentale Interessengegensatz besteht so auch in der realen Gesellschaft. Da im Augenblick die Beherrschten schwach sind, sind die Herrschenden am Drücker und lassen sich eifrig Kontrollmechanismen einfallen.

Verschärft wird die Notwendigkeit zu stärkerer Aufklärung der Untertanen durch die Neuausrichtung von „governance“ seit den späten 70er Jahren. War seit der Bewältigung der Weltwirtschaftskrise 1929ff bis dahin ein Regime von Regierung durch Teilhabe (also hin zu mehr gesellschaftlicher Gleichheit) dominant gewesen, hat sich, beginnend mit dem Pinochet-Putsch und wohl gleichmäßig inspiriert durch fallende Profitraten und vollständige Entzauberung realsozialistischer Alternativen, zunehmend ein Regime wachsender Ungleichheit etabliert. Mehr Ungleichheit sorgt automatisch für mehr Bedarf nach sozialem Management und mithin mehr Möglichkeiten zu Repression und Durchleuchtung.

Warum aber beschränken sich die Machthaber dann doch wieder selbst?

Modell 2: Add Marktwirtschaft. Marktwirtschaft funktioniert mit einem Rechtsstaat viel besser – die Marktakteure haben Investitionssicherheit, die Geschäfte werden nach Marktregeln (und nicht z.B. nach Gewalt oder staatlicher Willkür) abgewickelt usf. – nicht zuletzt ist in typischen Geschäften ein Mindestmaß an Vertraulichkeit wichtig, nicht nur, da sie praktisch immer in einer Grauzone zur Korruption stattfinden.

Ein Marktteilnehmer will sich also auf das Recht verlassen können – das ist ein Grund, warum wir de facto kein Feindstrafrecht haben. Es gibt dabei noch allerlei weitere Komplikationen, weil es ja z.B. noch weitere Staaten gibt, deren man sich auch bedienen möchte, aber so detailliert muss es jetzt nicht sein. Es bleibt: Marktwirtschaft will einen Rechtsstaat, will opake MarktteilnehmerInnen, will keine Staatswillkür. Daher die Beschränkungen, die sich die Herrschenden auferlegen.

Dann wäre ja eigentlich alles in Butter, allenfalls müsste man die Marktfraktion unter den Herrschenden stärken. Das ist in etwa das, was Teile der FDP glauben. Leider ist es falsch.

Modell 3: Gewerkschaften, KommunistInnen, AnarchistInnen: Krisengewinnler. Es gibt Dinge, die die Marktfraktion noch weit mehr fürchtet als eine Willkürherrschaft. Dazu mögen Staaten gehören, die sich der Benutzung verweigern oder gar die Benutzung des eigenen Landes bedrohen, in erster Linie sind das aber Linke. Werden diese stärker, wird auch die Marktfraktion einer Ausweitung der Willkürherrschaft zu stimmen (Beispiele gibt es genug, der Faschismus ist beileibe nicht der einzige – ein Blick in die Geschichte der Gewerkschaften in den USA ist da z.B. sehr aufschlussreich). Daten, die dann bereits vorliegen, werden letztlich beliebig genutzt werden. Und das ist die Hauptgefahr: Uns werden die Daumenschrauben proportional zu unserer eigenen Stärke angezogen werden..

Ganz zu vermeiden ist das natürlich nie. Wenn allerdings der Paranoia der Herrschenden schon ohne wirklich konkrete (fortschrittliche) Umgestaltungsprozesse freier Lauf gelassen wird, wird es später entsprechend schlimmer.

Auch im Normalzustand müssen die Herrschenden sehen, wie sie den sozialen Frieden erhalten – und das bedeutet, dass mit einer ausreichend starken Bewegung all der Kram abgewendet

werden kann. Vorbild mag hier die Kampagne zum Volkszählungsboykott sein, die 1982ff viele der Datenschutzrechte, die wir heute noch haben, erkämpft hat.

10. Was tun?

Technische Lösungen für soziale Probleme = Scheiße

Die Auswirkungen des autoritären Staats kann man teilweise technisch mildern – die Vorratsdatenspeicherung lässt sich z.B. mit einigem Sachverstand und der Bereitschaft zum Verzicht auf Bandbreite durch TOR begegnen, Data Mining kann durch Vermeidung von Datenspuren und gezieltes Legen irritierender Spuren ausgehebelt werden –, letztlich kann der Staat durch Gesetze und sanften Terror die „Kosten“ dafür so in die Höhe treiben, dass uns die Konspiration mehr kostet als sie wert ist. Letztlich hilft nur eine politische Auseinandersetzung.

- Kampf der Politik der Angst
- Sicherheit negativ besetzen – stattdessen lieber konkret bennenen, was gemeint ist: Menschenwürde, Unverletzlichkeit (der Person, der Wohnung...), Schutz vor Armut usf Insbesondere: Es gibt kein „Grundrecht auf Sicherheit“, und das ist auch gut so.
- Das Übliche

http://www.datenschmutz.de