Dauerhafter Friede

Der Überwachungsstaat schlägt zurück

> In jedem genügend reichhaltigen system also auch in diesem Sumpf hier, lassen sich Sätze formulieren, die innerhalb des Systems weder beweis- noch widerlegbar sind.
>
> Diese Sätze nimm in die Hand und zieh!
>
> —Hans Magnus Enzensberger, Hommage à Gödel

> Eine weiße Fahne auf dem Cover des Programmhefts, darin ein Artikel „We lost the war. Welcome to the world of tomorrow“: Die ComputermenschenrechtlerInnen vom CCC übten sich zu ihrem Kongress im Dezember 2005 („Private Investigations“) in Defätismus. Der totale Überwachungsstaat sei längst Realität, und wir könnten nur noch sehen, wie wir Nischen von Restfreiheit erhalten.

Das Szenario, das dort entworfen wurde, war in etwa, dass die mit dem postsozialistischen Kapitalismus einhergehende Desintegration der intra- und internationalen Gesellschaftsverhältnisse aus Sicht der Herrschenden nur mit einem gewaltigen Repressions- und Überwachungsapparat beherrschbar bleibt und dieser Apparat deshalb prioritär aufgebaut werden muss und aufgebaut wird. Die Folie von Nineeleven und folgende, also die des islamistischen Terrorismus, ist dabei auswechselbar -- was Angst macht, taugt, und je nach Bedarf halten auch mal andere Megaschurken als Gründe für den Ausbau des Apparats her, zur Not Mörder von Modeschöpfern.

Dieser Analyse ist aus linker Sicht kaum zu widersprechen. Der Schluss jedoch, Kampf gegen diese Entwicklungen sei längst vergeblich, erscheint doch etwas vorschnell -- wer kämpft, kann verlieren, dürfte das leicht romantisierende Mantra der Stunde sein, wer nicht kämpft, hat schon verloren.

Vorratsdatenspeicherung und Biometrie

Unter den vielen aktuell betriebenen Projekten zum Ausbau des Überwachungsapparats stehen derzeit in der BRD zwei weit heraus: Einerseits ist das die Vorratsdatenspeicherung, die Telekommunikationsunternehmen verpflichten wird, sämtliche Verbindungsdaten (wer hat wann mit wem kommuniziert) für mindestens ein halbes Jahr, wahrscheinlich aber gleich mal zwei Jahre, zu speichern. Auf EU-Ebene ist die entsprechende Gesetzgebung bereits verabschiedet, die Umsetzung in nationales Recht steht unmittelbar bevor.

Dies bedeutet nichts weniger als den staatlichen Zugriff auf die gewaltigste Datensammlung, die zur Aufdeckung von „Strukturen“ denkbar ist. Wer weiß, mit wem ihr telefoniert habt, wo euer Mobiltelefon wann war, wer auch weiß, mit wem eure GesprächspartnerInnen Mails ausgetauscht haben, wer dann diese Daten mit (realen und vermeintlichen) Erkenntnissen von Polizei und Verfassungsschutz von geeigneten und gar nicht mal übermäßig komplizierten Computerprogrammen kombinieren lässt, kann, wenn er es für nötig hält, recht schnell fast beliebig definierte Gruppen identifizieren und angreifen. Dass derartige Datensammlungen teilweise -- etwa beim US-Geheimdienst NSA -- wenigstens bruchstückhaft bereits bestehen, ändert an der Dramatik der Entwicklung in der EU nichts, da einerseits die repressiven Befugnisse der US-Dienste hierzulande recht beschränkt sind, sie im Regelfall ihre „Erkenntnisse“ kaum weitergeben werden und auch eher nicht die Arbeit ihrer Kollegen aus der BRD machen werden, andererseits die z.B. zu Abrechnungszwecken vorgehaltenen Daten für die Staatsgewalt nicht so einfach zugänglich sind und sie außerdem vom Datenschutzgesetz kontrolliert werden, also recht schnell gelöscht werden müssen.

Läuft die Vorratsdatenspeicherung, haben Dissiden-

tInnen nur zwei Möglichkeiten, um ihren Gefahren auszuweichen: Auf Telekommunikation weitgehend verzichten und auf diese Weise politisch fast handlungsunfähig werden, oder so viel Arbeit auf die Tarnung der Kommunikation verschwenden, dass das Ergebnis vom ersten Szenario kaum zu unterscheiden wäre. Beides bedeutet letztlich, dem Staat die Möglichkeit zur fast instantanen Unterdrückung wirksamer Opposition in die Hand zu geben. Vermutlich muss er noch nicht mal regelmäßig physische Repression anwenden, ein paar Exempel dürften für eine ausreichend paranoide Grundstimmung sorgen.

Das zweite spektakuläre Großprojekt ist die flächendeckende Erhebung und zentrale Speicherung biometrischer Daten, zunächst Fotos, demnächst Fingerabdrücke, wahrscheinlich früher oder später auch genetische „Fingerabdrücke“. Getarnt ist das derzeit noch als „fälschungssichere Ausweisdokumente“, inklusive der Versicherung, die erhobenen Daten würden niemals der „Verbrechensbekämpfung“ dienen. Doch zeigt alle Erfahrung mit ähnlichen Technologien, dass die nächste Sicherheitshysterie alle vorgeblichen Vorsätze in schlechte Luft auflösen wird; analoges gilt übrigens für Versicherung, auf den im Zuge der Vorratsdatenspeicherung erhobenen Daten würde kein Data Mining, also eben keine globale und systematische Analye etwa von Kommunikationsprofilen durchgeführt. Nach Fällen wie Toll Collect, das schon nach ein paar Monaten eben doch zum bundesweiten Kfz-Kennzeichenscanner mutierte, oder auch der inzwischen grenzenlosen Erfassung von DNS-Daten im UK, der nach anfänglichen Beteuerungen, es gehe nur um Schwerkriminalität längst auch Kinder und auch nach Polizeimaßstäben Unschuldige unterworfen werden, sind entsprechende Regelungen während der Einführungsphase nur noch in die Kiste „erhebet die Herzen“ zu sortieren.

Im Effekt wird der Staat mit dem biometrischen Personalausweis alle legal auf seinem Territorium lebenden Menschen ED-behandelt haben. Jede Sorte Anonymität bei politischer Betätigung ist damit vorbei, und wie das Absammeln von Zigarettenkippen nach einer Demo in Gorleben zeigt, wartet die Staatsgewalt nur darauf, komplette Personendateien von DissidentInnen zu haben -- im Augenblick fehlt ihr dazu in der Regel der Name zu den Finger- oder Genspuren. Nicht mehr lange, wenn erstmal die technischen Anlaufschwierigkeiten überwunden sind und Gesetzeslage den „Notwendigkeiten der Verbrechensbekämpfung“ angepasst ist.

Haben wir verloren?

Wären die Bekenntnisse zu Demokratie und Meinungsfreiheit, die die Herrschenden dann und wann gern absondern, auch nur einen Pfifferling wert, sollte in Berlin die Heilung von gespaltener Persönlichkeit ein boomendes Geschäft sein, während die grundgesetztreue Öffentlichkeit auf den Barrikaden stehen müsste. Sie tut es nicht, von einigen bedrängten DatenschützerInnen und bizarren Geeks mit ungewaschenen Haaren abgesehen.

Was noch schlimmer ist: Die radikale Linke, die, sobald sie wieder eine gewisse gesellschaftliche Relevanz bekommt, mit Sicherheit die durch Vorratsdatenspeicherung und flächendeckende ED-Behandlung mögliche neue Dimension von Repression am härtesten zu spüren bekommen wird, kriegt ebenfalls nur in Ausnahmefällen mehr als gedämpftes Interesse zusammen. Diese Wurstigkeit ist auch bedrückend, weil das Menschenrechtsthema bei all seiner bürgerlichen Drögerie durchaus das Zeug hätte, analog zum Volkszählungsboykott der 80er Jahre linke Themen in den breiteren Diskurs zu bringen.

Hätten wir bereits verloren, blieben, wenn überhaupt, die oben diskutierten Auswege -- Verzicht auf Technologie oder technologiebasierte Abwehr der Überwachung --, und sie führen nur weiter in die Marginalisierung. Es gibt aber fast sicher (noch) eine Alternative: Widerstand gegen den Generalangriff.

Was braucht es dazu? Zunächst ein Brechen der Trägheit und des Ignorierens. Gerade als Antirepressionsorganisation ist es an uns, die Thematik hinaus in linke Zusammenhänge zu tragen. Ist dort ausreichend Bewusstsein für den Ernst der Lage vorhanden, sind Veranstaltungen zur überbordenden Überwachung nicht mehr leer, Bündnisdemos gegen Vorratsdatenspeicherung nicht mehr programmierte Rohrkrepierer, direkte Aktionen zum ePass keine one-person-shows mehr.

Überwachung und Repression sind selten wirklich populäre Themen, zumal viele Menschen ein Gefühl der Aussichtslosigkeit des Kampfes lähmt und die Gefahren häufig abstrakt erscheinen, bevor die Fallen zuschnappen. Bei der Hi-Tech-Repressionswelle kommt erschwerend die Technologielastigkeit hinzu,

doch hilft auf der anderen Seite, dass ePass und Vorratsdatenspeicherung beileibe nicht isolierte Vorstöße sind -- praktisch alle Strömungen, die sich innerhalb der Roten Hilfe finden, dürften in der einen oder anderen Weise ganz direkt Bekanntschaft mit den elektronischen Freunden und Helfern gemacht haben.

Ein paar dieser Anknüpfungspunkte sollen im Folgenden diskutiert werden. Sie sind nur eine kleine Auswahl -- ein halbwegs vollständiger Überblick über die gegenwärtigen Entwicklungen hätte diese Zeitung problemlos gefüllt. Vielleicht geben sie aber die eine oder andere Idee, wie fortschrittlichen Menschen das Ausmaß des Problems näher gebracht werden kann.

Flüchtlinge und MigrantInnen

Vor allem Flüchtlinge und vorerst weniger Linke sind im Fokus des Schengen-Informationssystem (SIS), einer monströsen Datenkrake mit Kopf in Straßburg und Tentakeln überall in Schengenland. Datensätze für eine knappe Millionen Menschen finden sich dort, weil irgendwer beschlossen hat, sie dürften nicht in die EU einreisen. Rechtsmittel sind nach Lage der Dinge kaum möglich, denn wer unter den Menschen, die in die Festung Europa zu kommen versuchen, könnte ernsthaft einen Prozess von außerhalb der EU gegen EU-Polizeibehörden führen, wo auch wir selbst in solchen Prozessen meist chancenlos sind.

Abgefragt wird SIS überall: an den Grenzen, an Flughäfen, an Bahnhöfen. In Österreich hat die Polizei in Zügen offenbar Abzüge von SIS auf Notebooks „mobil“ dabei. Meldet ein Programm „Person gefunden“, läuft das Abschieberegime unmittelbar aus dem Zugabteil heraus an.

Seit Jahren in Planung und vermutlich dann doch demnächst mal fertig ist SIS II, der, wie aus EU-„Sicherheits“kreisen gejubelt wird, neue und vielfach leistungsfähigere Nachfolger von SIS, dessen erklärtes Ziel unter anderem ist, biometrische Daten recherchierbar zu machen.

Was, wenn nun die dank Massen-ED-Behandlung vollständig vorhandene Biometrie der EU-Legalen in SIS landen würde? Da Visa zunehmend biometrische Merkmale tragen, würde dann bei der Personenkontrolle nicht mehr geprüft, ob jemand in SIS als abzuschieben erfasst ist („erlaubt ist, was nicht verboten ist“), es wird geprüft, ob jemand eigentlich legal in Schengenland ist („was nicht erlaubt ist, ist verboten“).

Dieses Szenario wird nicht heute oder morgen kommen. Beim derzeitigen Tempo der Orwellisierung ist es aber für 2015 durchaus vorstellbar. Wenn niemand etwas dagegen tut.

JobberInnen

Natürlich macht die Repressionswalze keinen Halt vor der „sozialen Frage“ -- im Gegenteil. Im Bereich der Bekämpfung von vermeintlichem „Missbrauch“ des Arbeitslosengeld II probiert sich die Bundesagentur in Data Mining-Techniken und lässt sich Rechte zum Durchgriff auf staatliche wie private Datenbestände geben, wie sie früher allenfalls zu Rasterfahndungsaktionen denkbar schienen.

Schon die klar optimistisch geschätzten „Erträge“ -- ein paar hundert Millionen Euro -- sind Peanuts im Vergleich zu den Gesamtkosten des ALG II-Projekts und vor allem im Vergleich zum Ausmaß des damit verbundenen Eingriffs in die Grundrechte. Es geht ja auch gegen potenzielle UnruhestifterInnen, die im oben zitierten Szenario die eigentliche Zielgruppe des Überwachungsapparats sind.

Andererseits liefert ein Vergleich zum simultan stattfindenden Diskurs über eine Beschränkung der automatisierten Kontenabfrage staatlicher Bedarfsträger („wir können das nicht so machen, weil sonst alle ihre Konten in die Schweiz verlegen“), eine wesentliche Einsicht in das Wesen von Bürgerrechten im Allgemeinen und das Datenschutzrecht im Speziellen: Sie werden nicht aus Großmut oder Menschenfreundlichkeit gewährt, sondern weil der Kapitalismus mit ihnen viel besser funktioniert, sei es, weil Eigentum zuverlässig vor staatlicher Willkür oder Begehrlichkeiten anderer BürgerInnen geschützt ist, sei es, wie hier, weil die kleinen Dinger, die man als Subjekt wirtschaftlichen Handelns nebenbei dreht, nicht selten eines funktionierenden Bankgeheimnisses bedürfen.

Schlecht für die gläsernen Erwerbslosen, dass sie nicht nur als politisch unzuverlässig einzustufen sind, sondern eben auch lediglich als Reservearmee für den Standort relevant sind. Der Wert ihrer Bürgerrechte ist mithin kaum größer als der Inhalt ihrer Geldbeutel, der wiederum bei den ALG-II-Sätzen sehr überschaubar ist. Es sei denn, und hier kommt der für die

Organisation wirksamen Widerstands entscheidende Punkt, schon der Angriff auf ihre Rechte würde den sozialen Frieden, zu dessen Verteidigung er ja letztlich vorgetragen wird, gefährden oder wenigstens zu gefährden scheinen. So ärgerlich das sein mag, diese Sorte Standortfaktor ist gegenwärtig einer unserer wirksamsten Hebel.

In der Grauzone

Wenn der soziale Friede mal wirklich gefährdet ist, ist es „der Bundesregierung [...] gestattet, eine Stelle zur Sammlung und Verbreitung von Auskünften über umstürzlerische, gegen die Bundesregierung gerichtete Tätigkeiten einzurichten. Diese Stelle soll keine Polizeibefugnisse haben." Das ist aus dem alliierten Polizeibrief Nr. 2 vom 14.4.1949 und war damals natürlich als „sonst nicht" gemeint. Die Ziele von Bundespolizei und BKA haben sich seit damals wohl nicht wesentlich geändert, das mit den Polizeibefugnissen hat seine Aktualität dagegen ebenso eingebüßt wie das implizite „sonst nicht".

Noch davor, 1946, hatte der Alliierte Kontrollrat in seinem Gesetz Nummer 31 „[a]lle deutschen Polizeibüros und -agenturen, die die Überwachung oder Kontrolle der politischen Betätigung von Personen zum Zweck haben" aufgelöst und ihre Wiedereinführung verboten. Nachdem sich der deutsche Staat weitestgehend vom Artikel 139 des Grundgesetzes, „der Befreiung... vom Nationalsozialismus und Militarismus" befreit hat, befreit er sich nun auch endgültig von diesem alliierten Gebot der Trennung von Polizei und Geheimdienst, im Zeichen der „Sicherheit", natürlich.

Da werden, gegebenenfalls im Ausland, gemeinsame Zentren von Diensten und BKA gebildet, Datensammmlungen geteilt, heiße Drähte geschaltet. Die Entwicklung der letzten Jahre spricht eine deutliche Sprache: Wir befinden uns auf dem Weg in einen Staat proaktiver Kriminalpolitik und grenzenloser, durch Sicherheitsfanatismus geschürter Überwachung. Sein Ende ist unschwer abzusehen. Wenn bei Ermittlungen frei zwischen der praktisch keiner rechtlichen Kontrolle unterworfenen Geheimdienstarbeit und jederzeit mit breiter repressiver Macht ausgestatteten Polizeitätigkeit (gegen die zwar eingestandenermaßen auch fast nie erfolgreich justiziell vorzugehen ist, deren Entscheidungen aber glücklicherweise oft genug vor Gericht keinen Bestand haben) hin und her gewechselt werden kann, wird sich unsere Arbeit recht schnell von der Rechts- zur Fluchthilfe entwickeln müssen.

Datenbanken

Schon lange, bevor es soweit ist, hat die enge Zusammenarbeit spürbare Konsequenzen, und zwar beispielsweise, weil die Polizei zunehmend Daten bei den Diensten „parken" wird. Der entscheidende Vorteil ist, dass diese jedenfalls auf Bundesebene und in vielen Ländern de facto keiner Auskunftspflicht unterliegen und daher im Groben alle Regelungen, was wie lang gespeichert werden darf, unterlaufen können.

Auswirkungen dieser Datensammlungen spüren beileibe nicht nur KifferInnen, die bei jeder (bis vor nicht allzu langer Zeit übrigens auch illegalen) „verdachtsunabhängigen Kontrolle" ordentlich gefilzt werden. Da bekommen Linke „Gefährderanschreiben", Serienbriefe aus den Datenbanken der politischen Polizei, die den guten Rat geben, lieber nicht zu einer Demo zu fahren, da werden öffentlich Beschäftigte in den Keller versetzt, weil in irgendeiner Datenbank steht, sie seien mal in einer Autonomen Gruppe gewesen, da werden Platzverweise und Gewahrsamnahmen nach einem kurzen Funkgespräch mit den Zentrale und ohne weiteren Grund ausgesprochen. Und auch wenn das gegenwärtige Berufsverbotsverfahren gegen ein Mitglied der Roten Hilfe soweit bekannt wohl noch auf Papierakten und Schlapphüte aus Fleisch und Blut zurückzuführen ist: Es ist längst nicht mehr die Technik oder die Personalkapazität, die flächendeckende Kontrolle der FDGO-Konformität für BewerberInnen oberhalb des SpargelstecherInnenniveaus verhindert, sondern lediglich Mangel an politischer Notwendigkeit und vielleicht auch eine Prise ökonomischer Zwang.

Solange also die geheime Bundespolizei noch eine Dystopie ist und immerhin noch Einblick in große Teile der staatlichen Datenhaltung möglich sind, sollte zur Datenhygiene politischer AktivistInnen (und, wenn immer möglich, auch anderer) in jedem Fall gehören, regelmäßig bei der Polizei anzufragen, was sie an Daten gespeichert hat -- die Datenschutzgruppe der Roten Hilfe Heidelberg hat dazu einen bequemen Auskunftsgenerator erstellt (vgl. URL unten). Allein durch das Auskunftsersuchen kommt es häufig zur Bereinigung (noch) rechtswidriger Datenhaltung. Um hier aktiv zu werden, reicht ein Weg zum Briefkasten.

Allerdings: Sobald die Vorratsdatenspeicherung greift, existiert von allen Menschen mit Telefon oder Netzanschluss ein Datensatz, gegen den alles, was Polizei und Verfassungsschutz selbst von den fiesesten Anarchos derzeit so haben, komplett irrelevant wird. Fast in Echtzeit lassen sich damit weit präzisere Erkenntnisse gewinnen, als es Scharen verdeckter ErmittlerInnen und PersonenkontrolleurInnen in Jahren mühevoller Arbeit könnten.

Voyeure mit Pensionsberechtigung

Zu den Daten, die ohne wirtschaftsfeindliche Gesetzesänderungen von der Polizei allenfalls in extremen Ausnahmefällen gespeichert werden können, gehören auch die Datenfluten aus den mittlerweile reichlich im öffentlichen Raum vorhandenen Kameras. Hier muss insbesondere der Innenstadt- und Zentrenbewegung ein Lob ausgesprochen werden, weil sie diesen Teil der Verdatung der Gesellschaft recht aktiv thematisiert hat.

Wenn es um das Erzeugen einer Sensibilität für den Durchmarsch der Überwacher geht, ist ein klarer Vorteil des Zugangs über Videoüberwachung die besondere Eignung dieses Felds für direkte oder jedenfalls öffentlichkeitswirksame Aktionen -- erwähnt seien hier nur die Surveillance Camera Players aus New York, die den ÜberwacherInnen amusante kleine Theaterstückchen vorspielen. Und Menschen, denen das zu harmlos ist, brauchen auch nicht viel Fantasie, um kernigere Handlungsmöglichkeiten zu finden.

Darüber hinaus lässt sich an den Kameras auch recht klar demonstrieren, was die neue Qualität der Hi-Tech-Überwachung ist: Verwendung und Empfänger der Daten sind völlig offen. Niemand kann wissen, ob die Aufnahmen von einer Demo 2003 oder dem Treffen mit Anna und Arthur in der Karl-Marx-Straße 2004 nicht plötzlich 2007 wieder in einem Verfahren auftauchen. Möglich wird das erst durch die Fähigkeit von Rechnern, enorme Datenmengen zu speichern und zu verknüpfen, bei Verbindungsdaten ebenso wie bei entsprechend verarbeiteten Videobildern. Die potenziell große Schar derer, die beim Nasebohren zusieht oder über die eine oder andere Eigenschaft von PassantInnen feixt, die den gesellschaftlichen Idealen vielleicht nicht oder gerade besonders gut entspricht, ist dabei nur noch lästige Randerscheinung.

Wie weit diese Schar erweiterbar ist, wird derzeit in einigen Gemeinden in England erprobt. Dort werden Überwachungskameras über das Internet für alle BürgerInnen zugänglich gemacht, quasi als Fortsetzung von Ansätzen aus den USA, Informationen über vermeintliche ehemalige Verbrecher in Echtzeit zu verbreiten. Aber wie gesagt: Im Vergleich zu gut programmierten Rechnern der nahen Zukunft ist der Blockwart nur eine lästige Randerscheinung.

Angesichts der raschen Fortschritte im Bereich der image registration, also der Identifikation von beispielsweise Personen auf Bildern, fällt es nicht schwer, von Kameras auf die Generalerfassung biometrischer Daten zu kommen. Denn erst mit diesen Daten werden aus Pixeln Namen und aus Namen Staatsfeinde, so sie mit den falschen Menschen telefoniert haben. Oder ihr Mobiltelefon zur falschen Zeit in der falschen Funkzelle war. Genau solche Verknüpfungsmöglichkeiten hat der Computer dem Blockwart voraus.

Nochmal: Was tun?

Freiheit stirbt mit Sicherheit, und mit ihr auch immer mehr die Möglichkeit, Unterdrückung abzuschütteln. Als Linke müssen wir um unsere Freiräume und also gegen die rasende Produktion von Sicherheitsmaßnahmen kämpfen. Da diese im Augenblick am stärksten dadurch bedroht werden, dass die verschiedensten staatlichen und privaten Stellen immer mehr Technologie gegen die nicht ganz umsonst unter Generalverdacht stehenden Bürger- und KundInnen in Stellung bringen, folgt daraus insbesondere auch: Know Your Enemy, the Enemy Knows You, auch und gerade wenn der Feind zum unmittelbar verständlichen Stahl etwas schwerer verständliche Software samt Silizium in sein Arsenal aufgenommen hat.

Wie oben gesagt: Wir als Antirepressionsorganisation sollten uns aufgerufen sehen, Problembewusstsein in die verschiedenen in der RH vertretenen Strömungen zu tragen und vielleicht sogar Bündnisse in Fragen des Widerstandes gegen Repression herzustellen. Der Widerstand rund um den Volkszählungsboykott hat vor 20 Jahren den repressiven Sonnenstaat tatsächlich verzögert, vielleicht sogar zurückgeworfen. Was damals an Bedrohung im Raum stand, ist indes allein wegen des Technologiefortschritts aus heutiger Sicht schon fast eine positive Utopie.

Zwischen London, Madrid und New York, zwischen Arena auf Schalke und Tarifa tösen die Forderungen nach dem Opfern der „grundgesetzmäßig geschützten“ Rechte. Statt Individualrechten wird das neue „Recht auf Sicherheit“ als vordergründiges und fast ausschließlisches Gemeinwohlinteresse propagiert, dazugedichtet. Datenschutz, „Rechtstaatlichkeit“ und „Freiheitsrechte“ werden denunziert als Luxus, den wir uns angesichts terroristischer Bedrohung nicht mehr leisten können. Dass die dabei angeführten Bedrohungen, terroristische zumal, verglichen mit Dutzenden anderer Gefährdungen (Nazis inklusive) praktisch insignifikant sind, spielt im Diskurs längst keine Rolle mehr -- was zum Ausbau des Überwachungsapparats nützliche Angst erzeugt, taugt.

Um so wichtiger ist es, jetzt Widerstand zu leisten. Die RH ist ein guter Platz, damit anzufangen -- aber dazu braucht es einfach auch mehr Menschen in den Aktivengruppen. Beteiligt euch, solange es noch geht. Die Faust in der Tasche war schon immer am falschen Platz, doch gerade jetzt könnte der Platz nicht falscher sein.

Vorstellen könnten wir folgende Initiativen der Ortsgruppen:

1) Die bereits angefangene Arbeit der Datenschutzgruppe der RH auf breitere Basis stellen. Wir sollten wissen, was es an Gesetzen, Erlassen und Verordnungen sowie an Vorhaben in der BRD und der EU zu dieser Thematik gibt; sammeln, auf dem neusten Stand halten, Betroffenen zur Verfügung stellen. Übrigens sind auch Einsichten in die Firmen, die die Überwachungshard- und software herstellen, nicht uninteressant und bringen manch Ansatzpunkt für konkrete Aktionen.

2) Veranstaltungen über die geschilderte Problematik organisieren, auch in Kooperation mit bürgerlichen Anti-Repressionsgruppen.

3) Fantasievoll Widerstand leisten: „Surveillance Camera Players“ auch bei uns, Boykott der kommerziellen RFID-Technologie und allen kommerziellen Datensammler, Boykott der neuen Pässe und künftiger Ausweise (oder massenhaft verbrennen...), wenn gar nichts anders geht, das z.B. bei der Patentproblematik durchaus effektive Lobbying probieren.

4) Die Möglichkeit von Verfassungsklagen oder EU-Klagen gegen die Überwachungsgesetze überprüfen und dann sich dafür Gruppen Klagegruppen organisieren.

5) Selbst Datenhygiene betreiben: Nicht unnötig Datenspuren hinterlassen („Don't protest and Payback“), Auskunftsersuchen stellen, Willkürentscheidungen der Polizei nicht einfach hinnehmen usf.

6) Die Politik der Angst nicht mitmachen -- im Vergleich zu den „Notwendigkeiten“ der Lohnarbeit, zum EU-Grenzregime und vielen weiteren Bedrohungen, zu denen der Repressionsapparat beiträgt, sind sämtliche Selling Points des Überwachungsstaates Popanze. Überwachung macht nichts besser. Aber vieles schlechter.

Datenschutzgruppe der Roten Hilfe Heidelberg

http://www.datenschmutz.de

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