Sicherheit in Zeiten des Spin

Das BKA wird zur elektronischen Gedankenpolizei

> Nicht erst mit dem Gemeinsame-Dateien-Gesetz (vgl. RHZ 1/2007) hat die Politik in der BRD den Weg zu einem de facto als Geheime Bundespolizei operierenden „Sicherheits“-Sumpf eingeschlagen. So können die Regelungen des neuen BKA-Gesetzes allenfalls überraschen, weil sie in Zeiten von allerlei wüsten Skandalen im Repressionsbereich allzu mutig vorgetragen wurden. Und so lohnt sich vielleicht auch ein kurzer Blick auf den Prozess, in dem aus diversen Ent- und Einwürfen schließlich ein Gesetz wurde. Er zeigt prototypisch, wie Bürgerrechtsabbau mit der Demonstration der Funktionfähigkeit der Demokratie einhergehen kann.

„Spin“ bezeichnet eine geschickte, an kommerzielle PR-Strategien angelehnte Öffentlichkeitsarbeit, mit der allerlei Fürchterlichkeiten so gedreht werden, dass sie am Ende als positiv für die „Gemeinschaft“ rezipiert werden. Im angesichts der reibungslosen Umsetzung eines gigantischen Programms von Überwachung und Sozialabbau als Mutterland des Spins geltenden Vereinigten Königreich heißen die BeraterInnen, die sich sowas ausdenken, spin doctors oder etwas elaborierter *spinmeisters*. Solche Meister gibts nun auch woanders, und der öffentliche Diskurs um das BKA-Gesetz könnte ein Schulbeispiel sein.

Der Prozess

Mit geradezu umwerfender Ehrlichkeit hat das der Berliner Innensenator Eberhard Körting am 28.11.2008 im Deutschlandfunk auf den Punkt gebracht: „Ich glaube, man ist gut beraten, in der Akzeptanz gegenüber den Bürgern bei diesem höchst umstrittenen Gesetz (Hirsch hat den Computer als ausgelagertes Gehirn bezeichnet oder Ähnliches) die Akzeptanz dadurch zu erhöhen, dass man wirklich ganz behutsam vorgeht. Dazu gehört eben der Richtervorbehalt. Dem Bundeskriminalamt wird nichts weggenommen, wenn ein Richtervorbehalt erst mal da ist.“

So viel zu einem der Punkte, die im Hin und Her zwischen Bundestag und Bundesrat debattiert wurden. Und tatsächlich, in der RH organisierten Menschen muss kaum erklärt werden, dass auch Gerichte mit Beschlüssen zu Durchsuchung, Gewahrsamnahme, DNA-Analyse und so fort gerade im Politbereich großzügig umgehen. Dabei hat Körting die pikante Regelung, das die ach so umstrittenen Entscheidungen dem „Amtsgericht [...], in dessen Bezirk das Bundeskriminalamt seinen Sitz hat“, zuschreibt, noch vornehm übergangen. Dass das BKA also immer die gleichen Richter befragt, lässt, man kennt sich, die ohnehin geringe Hoffnung auf eine kritische Prüfung weiter schrumpfen.

Es wurde hier also ein sachlich weitgehend irrelevantes Thema öffentlich zum Lackmustest für die Demokratie stilisiert, und in der Tat, die Demokratie besteht (in dem Fall durch Intervention des Bundesrates, ansonsten häufig durch Einspruch aus Karlsruhe). Diese Nummer ist inzwischen zu einem von zwei Standardmustern beim Abbau von Bürger- und Menschenrechten geworden[1] , denn hinter den großen öffentlichen Themen segeln die wirklichen Hämmer unbemerkt.

Durch beschönigende Metaphern können sie gleich noch eine Tarnkappe bekommen. Der „genetische Fingerabdruck“ etwa liefert drastisch mehr Spuren (richtige und falsche) als ein Fingerabdruck, und der Begriff „Onlinedurchsuchung“ tarnt geschickt, dass es hier um geheimpolizeiliche Mittel geht. „Fingerabdruck“ und „Durchsuchung“ suggerieren eine Fortschreibung des Bestehenden, wo in Wirklichkeit neue Dimensionen autoritären Durchgriffs eröffnet werden.

Ergebnis ist, dass der Sicherheitssumpf trotz der Einsprüche im Wesentlichen kriegt, was er will. Querulan-

tInnen wie BürgerrechtlerInnen sind mit Klagen und Co eine Weile beschäftigt, und die BürgerInnen selbst sehen beim vermeintlichen Sieg gegen die Zumutung, wie schön demokratisch hier alles ist. Gefühlte Demokratie bei gleichzeitiger Einführung „präventiver“ Kompetenzen, d.h. der Formierung einer Polizei, die Menschen verfolgt, weil sie falsch denken. Have your cake and eat it, too.

Das soll nicht heißen, dass all die Prozesse, Einsprüche und Diskurse sinnlos sind oder gar den Gegenseiten in die Hand spielen, denn immerhin werden Teile der Angriffe ja zurückgenommen oder, etwa beim Lauschangriff, ein paar Hürden aufgebaut, die die Nutzung der „Instrumente“ nur bei wilder Entschlossenheit attraktiv erscheinen lassen. Dennoch wird mit ihnen, womöglich zur Gewinnung von Akzeptanz, kalkuliert, und solange die Gegenseiten keine bösen Fehler in ihren Kalkulationen macht, werden sie alleine unzureichend sein, um das jahrzehntealte Projekt des technokratischen Sonnenstaates auch nur aufzuhalten, geschweige denn umzukehren.

Das Gesetz

Die OG Hamburg hat in RHZ 04/08 das BKA-Gesetz insgesamt diskutiert und eingeordnet[2] . Hier soll es etwas genauer um die unmittelbar datenschutzbezogenen Klopfer gehen. Sie sind größtenteils in den neuen Unterparagraphen des § 20 beschrieben. Das Alphabet reicht kaum für die Aufzählung, erst beim x waren BKA und Regierung glücklich. Beeindruckend ist das nicht zuletzt, da im bisher geltenden BKAG dieser Paragraph keine 250 Zeichen lang ist.

Schon in § 20b gehts zur Sache, denn das BKA darf im Prinzip unbegrenzt „weiche“ Daten (wie „x war am y am Ort z“, „x ist heterosexuell“, „x programmiert in Java“) speichern, und zwar wenn es glaubt, dass eine Person „die Person eine Straftat gemäß § 4a Abs. 1 Satz 2 begehen *will*“ oder jemand „nicht nur flüchtig oder in zufälligem Kontakt in doit{Verbindung}“ mit so einer Person steht (Hervorhebungen d.V.). Mit anderen Worten ist mit diesem Gesetz gegen eine Speicherung beim BKA mit rechtsstaatlichen Mitteln nichts mehr zu tun[3] , denn § 4a ist das übliche Gummigewäsch zu internationalem Terrorismus, auf dessen Basis auch Mitarbeit in der RH inkriminierbar ist. Nicht ganz zufällig wurde dies weitgehend aus dem Gemeinsame Dateien-Gesetz (vgl. RHZ 1/2007) abgeschrieben.

Damit das BKA auch reichlich saftige Daten zum Speichern bekommt, erlaubt § 20g Observation, heimliche Überwachung mit Kamera und Mikrofon außerhalb von Wohnungen, V-Leute, verdeckte Ermittler und „sonstige besondere [...] technische Mittel“, worunter Peilsender, GPS-Geräte oder präparierte Mobiltelefone ebenso zu verstehen sind wie, da keine Einschränkungen gemacht werden, beliebige Gadgets aus der Werkstatt von Ian Flemings Q. Bei all dem braucht es nicht mal mehr das Gericht, das für Kameras und Mikros in Wohnungen noch verlangt wird (gähn); wenn das BKA meint, die Zielperson würde in anderen Wohnungen spannende Dinge treiben, darf es auch diese verwanzen. Tröstlich ist nur, dass nach den Erfahrungen mit dem großen Lauschangriff zunächst kaum mit BKA-Kameras auf dem WG-Klo zu rechnen ist, denn noch hat das BKA nicht die Personalstärke, die es dafür bräuchte.

Krachiger ist § 20i, die Ausschreibung zur polizeilichen Beobachtung. Landespolizeien machen sowas (besser auch „verdeckte Registrierung“ genannt) schon ausgiebig, gerne auch in SIS auf europäischer Ebene. Idee ist, unschuldige Menschen quasi zur Fahndung auszuschreiben. Weil die Polizei aber wg. Unschuld noch nichts hat, um die Opfer verhaften zu können, werden einfach bei jedem Antreffen alle möglichen Daten (wann, wo, wie, und, besonders perfide, mit wem) in die Datenbank eingefüttert. So entstehen mit etwas Glück umfangreiche Bewegungs- und Sozialprofile, potenziell EU-weit. Die Landespolizeien nutzen das im Gegensatz zu direkter Wohnraumüberwachung ausgiebig. Aus Bayern waren 2006 rund 2000 Personen zur Beobachtung ausgeschrieben, in SIS standen 1000 Beobachtungen aus der BRD. Das BKA darf das jetzt auch, und zwar ohne jede sachliche Begründung (die „Gesamtwürdigung der Person“ reicht). Erst nach einem Jahr muss mal wer außerhalb des BKA draufgucken (und dann auch nur das befreundete Gericht).

So geht es weiter: § 20j erlaubt dem BKA, von „öffentlichen oder nichtöffentlichen Stellen“ (außer den Geheimdiensten) fast beliebige Daten zu verlangen („Namen, Anschrift, Tag und Ort der Geburt sowie auf andere im Einzelfall festzulegende Merkmale“) -- das ist die Rasterfahndung, die hier schon dann erlaubt ist, „wenn konkrete Vorbereitungshandlungen die Annahme rechtfertigen,“ ein Anschlag stehe bevor. Diese Formulierung orientiert sich am Rezept, das Karlsruhe 2006 für die Umschiffung des Grund-

gesetzes in diesem Bereich angegeben hat. Wie „konkret“ irgendwas da sein muss, wurde ja schön durch die Mega-Aktion wegen der Luftnummer eines geplanten Attentats auf eine El Al-Maschine am Frankfurter Flughafen im November 2006 vorgeführt. Dennoch rechnet die Regierung bei „gegenwärtiger Sicherheitslage“ nur mit einer Rasterfahndung alle vier Jahre.

§20 k ist, was im Spintalk „Onlinedurchsuchung“ genannt wird, im Titel des Paragraphen aber richtiger „Verdeckter Eingriff in informationstechnische Systeme“ heißt. Die Fantasie nämlich, dass BKA-Leute in der Art des Whizkids aus Independence Day (der einen „Virus“ in die Computer der fiesen Außerirdischen pflanzt) von ihren Wiesbadener Rechnern beliebig in die Kisten der Bösen cracken, war im Bereich der paranoid-technophoben Ziehrkes und Schäubles möglicherweise verbreitet, doch angesichts des real damit verbundenen Aufwands, der jedenfalls im Bereich einer Wohnraumüberwachung liegt, wohl nie im Zentrum der Begierde derer, die nachher was damit machen sollen. Es geht einfach darum, beschlagnahmte, bei Hausbesuchen der Behörde oder Klobesuchen des/der EigentümerIn vorgefundene Rechner oder Mobiltelefone präparieren zu dürfen, bei Providern anzuklopfen und mit ihrer Hilfe „Fangschaltungen“ in dort laufende Foren- oder Serversoftware implantieren zu dürfen usf.

Es folgen Befugnisse zum Angriff auf die Telekommunikation in Form von Abhören (§ 20l), Zugriff auf Verkehrsdaten (also im Groben die Daten aus der Vorratsdatenspeicherung, § 20m) sowie spezielle Daten mobiler Geräte (§ 20n, das sind IMSI-Catcher und Co) -- im Groben deckt sich der Entwurf hier mit den reaktionärsten unter den Landespolizeigesetzen. Zusammen mit der Grundbefugnis der Gedankenpolizei kann das BKA jetzt also abhören und orten, wen es will. Insofern ist davon auszugehen, dass die gegenwärtig eher im Promillebereich liegende Beteiligung des BKA am Abhörzirkus der hiesigen Behörden künftig kräftig ausgebaut werden wird.

Weitere Tiefschläge erfolgen in § 20v, der dem BKA erlaubt, die mit all den schönen Methoden gewonnenen Daten weitgehend frei an „andere Polizeien des Bundes und der Länder sowie an sonstige öffentliche Stellen“ zu übermitteln. Restriktiver gehts zur Sache, wenn Daten an die Opfer der Maßnahmen übermittelt werden sollen. Wer nämlich observiert, ausgeschrieben oder abgehört würde, wer Trojaner auf die Platte bekommen hat oder in der Rasterfahndung hängen geblieben ist, soll nach § 20w benachrichtigt werden, *wenn* dem keine „schutzwürdige[n] Belange einer betroffenen Person“ (also etwa eines Beamten oder V-Menschen des BKA) entgegenstehen *oder* der Eingriff „nur unerheblich“ war und „anzunehmen ist“, dass es dem Opfer eh wurscht war. Das alles steht unter dem Vorbehalt, dass eine Gefährdung „des Zwecks der Maßnahme, des Bestandes des Staates, von Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, [... oder] auch der Möglichkeit der weiteren Verwendung des Verdeckten Ermittlers oder der Vertrauensperson“ ausgeschlossen ist.

Etwas weniger verschwurbelt heißt das: Die Benachrichtigung könnt ihr vergessen. Das weiß auch der Gesetzgeber und hat deshalb schon in der der StPO-Reform („Vorratsdatenspeicherung“, RHZ 2/07) verordnet, unterlassene Benachrichtigungen müssten gerichtlich überprüft werden; die Regelungen im BKAG sind im Wesentlichen parallel zu denen in der StPO, inklusive der Frist von fünf Jahren, nach der das Gericht endlich beschließen kann, es wolle mit der Frage nicht mehr behelligt werden („wenn die Voraussetzungen für die Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden“). Mit anderen Worten: Die Benachrichtigung könnt ihr *weitgehend* vergessen[4] . Und das ist schade, denn eine ernstzunehmende Benachrichtigungspflicht wär mal echt ein Pflästerlein für den Bestand der FDGO.

Bei den verbleibenden Unterparagraphen geht es um Skandale wie Platzverweise, Gewahrsamnahmen usf., die hier nicht Thema sind; interessant ist vielleicht noch, dass § 20t dem BKA das Betreten von Wohnungen, Geschäftsräumen usf weitgehend analog zur Bundespolizei erlaubt; relevant ist dies, weil sowas zusammen mit der Regelung, dass V-Leute mit Einverständnis des/der BewohnerIn in Wohnungen reindürfen, vermutlich ein populärerer Weg für Angriffe auf Rechner nach § 20k sein dürfte als der Elitehackerpolizist im abgedunkelten Keller von Meckesheim.

Fazit

Glaubt mensch der Regierung, wird sich das BKA als Folge dieses Gesetzes für mindestens fünf Millionen Euro neue High-Tech kaufen. Es wäre überraschend, wenn diese High-Tech nicht früher oder später mit

Mutmaßungen über euch beschäftigt würde, wenn eure Gedanken nicht ausreichend blankpoliert sind, selbst wenn sie sich kaum mit „internationaler Solidarität“ beschäftigen. Ob es beruhigend ist, dass ihr davon aller Wahrscheinlichkeit nach allenfalls indirekt erfahren werdet, müsst ihr selbst entscheiden.

Datenschutzgruppe der Roten Hilfe Heidelberg

http://www.datenschmutz.de

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

[1] Die zweite Methode kam in diesem Fall nicht in Frage, weil wichtige Protagonisten, in dem Fall der BND, der die Konkurrenz durch das BKA gar nicht leiden kann, nicht mit im Boot waren. Aber bei Nacht und Nebel abnicken (Modell Speicherung von Videoüberwachungsdaten im Bundestag letztes Jahr) kann auch gehen und ist weniger Arbeit. Das Risiko eines PR-Desasters ist aber auch größer...

[2] Den Artikel gibt es als Flugblatt unter http://pressback.blogsport.de/images/bka_rote_hilfe_hamburg.pdf

[3] Da zu befürchten steht, dass die EDV des BKA redundant und mit umfangreichen Backups angelegt ist und solche Daten ohnehin in alle möglichen anderen Systeme diffundieren, wirds auch mit anderen Mitteln schwierig.

[4] Uns ist allerdings seit Einführung der StPO-Reform schon eine Benachrichtigung bekannt geworden, die es davor wahrscheinlich nicht gegeben hätte. Wer das als Hoffnungsschimmer werten will, ist herzlich dazu eingeladen.