Bürgerrechte & Polizei

Cilip 97
Nr. 3/2010

Private und staatliche Ermittlungen: Ein Fall für zwei?

Inhalt

Private und staatliche Ermittlungen: Ein Fall für zwei?

Redaktionsmitteilung

Der private Sicherheitssektor strebt nach Anerkennung. Er will Teil jener „neuen Sicherheitsarchitektur" sein, über die seit 2001 in den verschiedensten Variationen diskutiert wird. Mögliche Felder einer engeren Zusammenarbeit zwischen Staat und Privaten reichten vom Personen- und Objektschutz über die Sicherung von Großveranstaltungen bis hin zur Überwachung von Abschiebegefängnissen und öffentlichen Verkehrsmitteln, hieß es im Jahre 2008 in einer Studie des Deutschen Industrie- und Handelskammertages.

Diese Liste lässt sich verlängern und sie bezieht sich längst nicht nur auf jene Wachschutz-, Streifen- und Kontrolltätigkeiten, bei denen die privaten Sicherheitsdienste öffentlich in Erscheinung treten. Als Partner „auf gleicher Augenhöhe" mit der Polizei anerkannt werden wollen auch die Vereinigungen für die Sicherheit der Wirtschaft und erst recht die Sicherheitsabteilungen von Großkonzernen, jene „Global Players", mit denen das Bundeskriminalamt 2006 eine Initiative startete. Sie sind international präsent, sie verfügen über eigene Informationen und haben dem BKA scheinbar einiges zu bieten – auch wenn der Maßstab ihrer Tätigkeit nicht das Recht, sondern das Firmeninteresse ist.

Ob es um solche „Firmenkripos" geht, die interne Ermittlungen nach eigenen Regeln und mit eigener Zielsetzung führen, um firmenexterne Detekteien und Sicherheitsberater, um kommerzielle Anbieter von „Intelligence" – die private Strafverfolgung ist immer ein „Fall für zwei". Sie kann ohne ihre Beziehung zu den staatlichen Sicherheitsapparaten nicht diskutiert werden.

***

Spätestens seit den Umbrüchen in Nordafrika gilt das Internet als Treibriemen der Befreiung. Das weltweite Netz ist aber auch der Rahmen für neue Formen polizeilicher und geheimdienstlicher Kontrolle. Mit diesem Thema wird sich die kommende Ausgabe von Bürgerrechte & Polizei/ CILIP befassen.
(Heiner Busch)

Private und staatliche Kriminalisten

Konvergenzen, Kooperationen, Gefahren

von Norbert Pütter

Telekom, Deutsche Bahn, Lidl ... – so könnte eine Liste jener namhafter deutscher Unternehmen beginnen, deren Sicherheitsanstrengungen in den letzten Jahren für Skandale gesorgt haben. Nach der öffentlichen Aufregung und der juristischen Bewältigung ist es wieder ruhig geworden um die im Verborgenen wirkenden privaten Sicherheitsexperten. Kein Grund zur Entwarnung.

Seit die inneren Sicherheitsdebatten vom „neuen Sicherheitsbegriff" überwölbt werden, schwinden vertraute Grenzziehungen. Diese aufzulösen, war und ist dessen strategischer Sinn. Das betrifft mit der behaupteten Verflechtung von innerer und äußerer Sicherheit die Trennung zwischen militärischen und polizeilichen Aufgaben. Die Entgrenzung erstreckt sich aber auch auf die Verbindung von wirtschaftlichen und staatlichen Interessen und damit auf das Verhältnis zwischen „privater" und öffentlicher Sicherheitswahrung. So wie in der Polizei-Militär-Frage Tendenzen der Entdifferenzierung – also der Zusammenarbeit und Vermischung vormals getrennter Aufgaben und Tätigkeiten – unübersehbar sind, so hat „Sicherheit" für Unternehmen einen solchen Stellenwert eingenommen, dass ihnen die Kombination aus „Werksschutz" und staatlicher Polizei nicht mehr auszureichen scheint.

Je nach Branche und Firmengröße unterschiedlich ausgeprägt, ergeben sich die alten (jetzt aber verschärft wahrgenommenen) und neuen unternehmerischen Sicherheitsrisiken in vier Bereichen: Der erste betrifft die Beschäftigten. ArbeitnehmerInnen sind ein traditionelles Sicherheitsproblem. Unternehmen waren schon immer darum besorgt, den Diebstahl von Arbeitsmaterial und Werkzeug oder den Ladendiebstahl durch das Verkaufspersonal zu verhindern. Aber je aufwändiger die Produktion, je ausgefallener die Produkte, je teurer Neuentwicklungen und je härter die Konkurrenz ist, desto wichtiger wird nicht allein das

physische Betriebskapital, sondern das Know how, das Expertenwissen der Beschäftigten. Deren Loyalität und Verschwiegenheit zu sichern, ist eine direkte Folge gewandelter ökonomischer Bedingungen.

Die zweite Quelle unternehmerischer Sicherheitsrisiken sind die Konkurrenten am Markt. Sei es über das Einkaufen personengebundener Informationen („head hunting"), sei es über Praktiken der Korruption, der illegalen Informationsbeschaffung durch private Spionage oder der legalen durch inszenierte Kooperations- oder Übernahmeverhandlungen[1] – vor der Ausspähung durch die Konkurrenz sind Betriebsgeheimnisse jeder Art bedroht: von den Produktionsverfahren und Geschäftsbeziehungen bis zu strategischen Unternehmensentscheidungen.

Drittens gehen Risiken für Unternehmen von den KundInnen aus. Die „Schufa" ist das klassische Instrument, mit dem Unternehmen sich vor zahlungsunfähigen KundInnen zu schützen suchen. Seit längeren unterhalten Versicherungen und Kreditkartenfirmen eigene Ermittlungsabteilungen, um Betrugsfälle aufzudecken. Zumindest für den Bereich des Kunstdiebstahls gibt es immer wieder Berichte, die auf „operative Tätigkeiten" verweisen: Durch den Rückkauf des Diebesgutes soll der Schaden für die Versicherung verringert werden. In dem Maße, wie komplizierte Anlageformen zur Kapitalvermehrung Verbreitung finden, wie die Finanzwirtschaft ein von der so genannten Realwirtschaft getrenntes Eigenleben führt und Finanzgeschäfte global abgewickelt werden, steigen die Risiken, dass die Systeme mit illegalen Methoden ausgeraubt werden.

Viertens wächst mit der Globalisierung auch die Bedeutung der physischen Sicherheit von MitarbeiterInnen und Produktionsanlagen. Weltweites Engagement setzt voraus, dass Unternehmen auch über jene sozio-politischen Risiken informiert sind, die ihnen in anderen Ländern und Kontinenten drohen – seien es Bürgerkriege oder ethnische Konflikte, sei es die demografische oder ökologische Entwicklung. Auch hier gibt es immer wieder Berichte über Sicherheitsdienstleistungen, die sich auf mehr als nur Informationssammlung und -aufbereitung erstrecken – etwa wenn Firmen versuchen, entführte Mitarbeiter von den Entführern freizukaufen.

Nimmt man diese vier Aspekte zusammen, so zeigt sich sehr schnell, dass „Sicherheit" zu einer grundlegenden unternehmerischen Voraussetzung in den fortgeschrittenen Ökonomien geworden ist. Die Verletzbarkeit der wirtschaftlichen Akteure hat derart zugenommen,

1 Wolf, N.: Sicherheitskooperation als weltweite Zweckbündnisse aus Sicht der Wirtschaft, in: www.bka.de/kriminalwissenschaften/herbsttagung/2005/rede_wolf_lang.pdf, S. 6

dass sie „Sicherheit“ nicht länger dem Staat alleine überlassen wollen. Um das „Unternehmensziel Sicherheit“ zu erreichen, müsse sie – so der Sicherheitschef von Siemens – „ganzheitlich als ‚integrale betriebliche Gefahrenabwehr‘“ realisiert werden.[2]

Korporative Sicherheit

Rechtlich und in der öffentlichen Diskussion wird herkömmlich zwischen privater und öffentlicher Sicherheit unterschieden. Dabei soll „öffentlich“ den staatlichen Zuständigkeitsbereich markieren, „privat“ den Rest nicht-staatlicher Verhältnisse. Eine solche Unterscheidung, die die Sicherheit einer betrogenen Ehefrau in derselben Kategorie behandelt, wie die Sicherheit eines forschenden Arzneimittelkonzerns, unterschlägt die enorme gesellschaftliche und politische Bedeutung kapitalistischer („privater“) Ökonomie. Die Folgen privatisierter Sicherheitsarbeit sind deshalb dort am größten, wo sie eine unmittelbare Verbindung mit wirtschaftlicher Macht eingehen, indem Unternehmen ihre Sicherheit selbst in die Hand nehmen.

Hinsichtlich der Organisation dieser „korporativen Sicherheit“ lassen sich zwei Formen unterscheiden:[3] Als „inhouse security“ werden jene Unternehmensabteilungen bezeichnet, die sich mit der Sicherheit der Firma oder des Konzerns beschäftigen. Große Unternehmen verfügen über eigene, meist nah an der zentralen Leitung angesiedelte Sicherheitsabteilungen, die sich in den letzten zwei Jahrzehnten aus dem traditionellen Werksschutz entwickelten. Ihr Aufgabenbereich geht aber je nach Unternehmen weit über die physische Sicherung des Betriebseigentums hinaus. Mitunter werden sie als „ein Art von Firmenkripo“ beschrieben.[4] Über die Zahl der Sicherheitsabteilungen, ihre personelle Größe, die Rekrutierung ihres Personals und ihr Tätigkeitsprofil gibt es nur wenige Informationen; sie werden meist bei „Skandalen“ öffentlich.

Neben den Sicherheitsabteilungen existiert der Markt der „contract security“, also jene privaten Sicherheitsanbieter, die auf vertraglicher Basis Aufträge (für die Unternehmen) übernehmen. Offenkundig treten dabei häufig die Sicherheitsabteilungen als Auftraggeber in Erscheinung,

2 ebd.

3 s. Nalla, M.K.: Police: Private Police and Industrial Security, http://law.jrank.org/pages/1691/Police-Private-Police-Industrial-Security.html

4 Jaeger, R.R.: Problematik privater Ermittlungsorganisationen in Unternehmen, in: der kriminalist 2008, H. 1, S. 19-24 (19)

so dass „corporate security“ durch das Zusammenwirken von eigenem Sicherheitspersonal und eingekauften Dienstleistungen gewährleistet werden soll (s. Kasten). In welchem Ausmaß private Sicherheitsfirmen zur „Konzernsicherheit“ beitragen, ist unbekannt. Für die USA ergab eine Untersuchung, dass Ermittlungstätigkeiten nur fünf Prozent des Umsatzes der Sicherheitsdienste ausmachten.[5] Auch in Deutschland liegt der Schwerpunkt privater Sicherheitsanbieter im Werks- und Objektschutz. 2009 wurden 36 Prozent der Beschäftigten in den Bereichen Objekt- und Werksschutz, 20 Prozent im Empfangsdienst und neun Prozent an Flughäfen eingesetzt.[6] „Ermittlungstätigkeiten“ sind offenkundig so unbedeutend, dass sie in dieser Auflistung des Bundesverban-

Die Telekom-Äffäre

Exemplarisch für das Zusammenwirken zwischen den Sicherheitsabteilungen in Unternehmen und externen „Sicherheitsfirmen“ steht die Überwachung von MitarbeiterInnen und Journalisten durch die Telekom, die 2008 bekannt wurde. Schon seit Anfang des Jahrzehnts war die Konzernleitung auf die Suche nach „undichten Stellen“ gegangen, über die interne Informationen an die Presse gelangten: Die Firma „Control Risk“ wurde mit Ermittlungen beauftragt; als deren Auswertung nicht ausreichte, wurde die auf Observationen spezialisierte Detektei „Desa Investigation & Risk Protection“ eingeschaltet. 2002 wurden diese Ermittlungen eingestellt.

2008 wurde bekannt, dass die Telekom in den Jahren 2005 und 2006 mehrere Dutzend Aufsichtsräte, Gewerkschafter und Journalisten hatte ausspähen lassen. Mit den Ermittlungen war die Berliner Detektei „Network“ beauftragt worden. Die Überwachungen waren aufgeflogen, nachdem deren Geschäftsführer die Zahlung ausstehender Rechnungen angemahnt hatte. Der verantwortliche Telekom-Mitarbeiter wurde im November 2010 zu dreieinhalb Jahren Haft verurteilt.

des Deutscher Wach- und Sicherheitsunternehmen nicht auftauchen. Für das Jahr 2009 gaben die Mitglieder des Bundesverbandes Deutscher Detektive an, dass 53 Prozent ihrer Aufträge aus dem Bereich „Wirtschaft, Industrie, Handwerk“ kamen; davon entfielen 53 Prozent auf In-

5 Mit 34 bzw. 30 Prozent entfielen die größten Umsatzposten auf Wachdienste und Alarmzentralen, s. The Security Industry and Private Policing, in: www.lib.uwo.ca/programs/generalbusiness/pp.html.

6 www.bdws.de/cms/index.php?option=com_content&task=view&id=28&Itemid=57&limit=1&limitstart=6 (10.1.2011)

dustrie, Handel und produzierendes/verarbeitendes Gewerbe, 30 Prozent auf Dienstleistungen, Handwerk und Baugewerbe und zehn Prozent auf Versicherungen. Knapp die Hälfte aller Aufträge aus der Wirtschaft betrafen „Mitarbeiterkriminalität“.[7]

Logik korporativer Sicherheitswahrung

Für private Sicherheitsleistungen gilt: Wer zahlt, bestimmt. „Policing for profit“ bedeutet, dass diejenigen, die die nötigen Mittel haben, sich ihre Sicherheit kaufen können. Bei der Diskussion um private Wachdienste im öffentlichen Raum oder zum Schutz des Eigentums sind die sozialen Folgen dieser Art der Privatisierung offensichtlich: Sie schafft unterschiedliche Sicherheiten für Reiche und Arme.[8] Für die private Aufrechterhaltung korporativer Sicherheit ist ein weiterer Aspekt von Bedeutung: Der private Auftraggeber bestimmt den Anlass von „Ermittlungen“, und er entscheidet darüber, wie deren Ergebnisse verwendet werden sollen. Untersuchungen von Polizei und Staatsanwaltschaft im Rahmen des Strafverfahrens sind in Deutschland an das Vorliegen „zureichender tatsächlicher Anhaltspunkte“ für eine Straftat gebunden (§ 152 Abs. 2 Strafprozessordnung). Ein Unternehmen, das MitarbeiterInnen der Spionage oder des Diebstahls verdächtigt, ist an diese Schwelle nicht gebunden. Zwar ist die Handlungsfreiheit privater ErmittlerInnen keineswegs unbegrenzt, aber die Grauzonen des Erlaubten sind allein deshalb größer, weil am Ende kein Strafprozess stehen muss, dessen Erfolg durch unzulässige Ermittlungsmethoden gefährdet würde. Denn der Auftraggeber entscheidet, was mit den durch die Sicherheitsabteilung oder beauftragte Fremdfirmen beschafften Informationen geschieht.

Da es Unternehmen – anders als der staatlichen Strafverfolgung – nicht darum geht, die Rechtsordnung aufrechtzuerhalten, sondern ihre eigenen Interessen zu wahren, d.h. etwa auf das öffentliche Image, die Position am Markt, den Börsenwert etc. zu achten, ist die öffentliche Anzeige nur eine von vielen Möglichkeiten. Für Unternehmen stehen Schadensbegrenzung und Wiedergutmachung im Vordergrund. Eine international vergleichende Untersuchung konnte nicht nur erhebliche

7 www.bdd.de/Download_Oeffentlicher_Bereich/DatenundFakten2009.pdf. Im BDD sind allerdings nur 10 Prozent aller in Deutschland registrierten Detekteien organisiert.

8 z.B. Beste, H.; Voß, M.: Privatisierung staatlicher Sozialkontrolle durch kommerzielle Sicherheitsunternehmen?, in: Sack, F. u.a. (Hg.): Privatisierung staatlicher Kontrolle: Befunde, Konzepte, Tendenzen, Baden-Baden 1995, S. 219-233

Unterschiede in der Sanktionspraxis gegenüber Beschäftigten etwa zwischen Asien und Europa feststellen, sondern lieferte auch Hinweise darauf, dass die Unternehmen weniger scharf reagieren, je höher die verdächtigte Person in der Hierarchie steht.[9] Einen Mitarbeiter etwa wegen des Verrats von Betriebsgeheimnissen anzuzeigen, würde – neben dem Imageschaden – vermutlich auch dazu führen, dass der Betroffene den entstandenen Schaden nicht wird ausgleichen können, weil er keine adäquate Beschäftigung finden wird, die ihm eine materielle Wiedergutmachung erlaubte. Aus Unternehmenssicht ist es deshalb günstiger, unter Zusage einer Entschädigung auf eine Anzeige zu verzichten und das Arbeitsverhältnis in gegenseitigem Einvernehmen zu lösen.[10]

Einzig das Unternehmen profitiert von dieser Art der „Verfahrenserledigung". Für den Betroffenen werden alle rechtsstaatlichen Sicherungen außer Kraft gesetzt; zwar kann er sich theoretisch der Kündigung widersetzen und es auf einen Prozess ankommen lassen. Aber praktisch böte selbst ein gewonnenes Strafverfahren keine Basis für eine weitere Arbeitsbeziehung. Für die Allgemeinheit bedeutete eine „private" Lösung, die Schutzfunktion des Strafrechts auszuhebeln. Denn sollten die Vorwürfe zutreffen, würde ein entdeckter Delinquent auf den Arbeitsmarkt – gegebenenfalls für Führungskräfte – entlassen. Schließlich wird auf diesem Wege das gesamte Strafverfolgungssystem für private Kalküle funktionalisiert. Es dient als Drohung, um den Beschuldigten zum „freiwilligen" Einlenken zu bewegen. Strafverfolgung kann dann nur bei jenem Rest von Gesetzesübertretungen tätig werden, der ihm von den Privaten überantwortet wird. Rechtsschutz und die Allgemeingültigkeit strafrechtlicher Normen gehen auf diesem Wege verloren.

Kooperationen

Es war schon immer falsch, aus den Unterschieden zwischen privaten und staatlichen Sicherheitsproduzenten einen Widerspruch zwischen beiden zu konstruieren. Durchaus folgen beide unterschiedlichen Handlungslogiken: Die Grade der Geheimhaltung, der öffentlichen Kontrollierbarkeit und der rechtlichen Einbindung sind verschieden, und es gibt auch eine beschränkte Konkurrenz – etwa im Hinblick auf die Ar-

9 Bussmann, K.-D.; Werle, M.M.: Addressing Crime in Companies, in: British Journal of Criminology 2006, No. 6, pp. 1128-1144 (1139 f.)

10 s. Maier, B.: Verbrechensaufklärung durch Privatdetektive, in: Kriminalistik 2001, H. 10, S. 670-672 (670)

beitsbedingungen oder die öffentlichen Mittel, die zur Verteilung stehen. Aber diese Differenzen stehen neben vielen Gemeinsamkeiten, die die Basis unterschiedlichster Kooperationen bilden. Die Bedeutung korporativer Sicherheitsproduktion erschließt sich deshalb nur dann, wenn ihr Verhältnis zu den staatlichen Apparaten mitbetrachtet wird.

Vier Ebenen privat-öffentlicher Zusammenarbeit lassen sich in Fragen der Sicherheit unterscheiden: Deren erste, die gemeinsame strategische Ausrichtung besteht zunächst darin, dass private wie öffentliche Instanzen darauf ausgerichtet sind, Sicherheitsprobleme zu diagnostizieren, die aus den Handlungen von Personen resultieren (können). Zudem sind beide am Ziel der Prävention orientiert. Gemeinsam wird eine risiko-orientierte Perspektive verfolgt.[11] Man möchte Schaden verhindern oder eingetretenen Schaden möglichst klein halten. Weil die Risiken frühzeitig entdeckt werden sollen, sind staatliche wie private Instanzen an der Sammlung von Informationen interessiert – von möglichst vielen Informationen aus unterschiedlichen Quellen, die zusammengefügt neue Informationen ergeben sollen. Unter dem Ansatz der „vorbeugenden Verbrechensbekämpfung" gibt sich die polizeiliche Strategie schon lange nicht mehr damit zufrieden, darauf zu warten, dass die Schwellen der Strafprozessordnung erreicht werden. Auch wenn allem Anschein nach die Kompetenzen des Polizeirechts in wirtschaftskriminalistischen Ermittlungen nur eine untergeordnete Rolle spielen, so teilen private wie öffentliche Ermittler die präventive Orientierung. Die Gewinnung von Informationen ist daher auf besondere Methoden angewiesen. Auch wenn beiden Seiten diese Methoden nicht im gleichen Maße zur Verfügung stehen (s.u.), so setzen sie beide auf die Kombination aus offener und verdeckter Datenerhebung.

Die zweite Ebene, die persönliche Verbindung, ist aus der Diskussion um private Sicherheitsdienste als „old boys network" hinlänglich bekannt.[12] Ursprünglich – darauf bezieht sich das „old" – ging es hier darum, dass Polizisten nach der Pensionierung eine zweite und einträgliche Karriere im privaten Sicherheitsbereich begannen. Mittlerweile stellt das Abwandern in die freie Wirtschaft einen durchaus häufiger anzutreffenden Laufbahnwechsel dar (s. Kasten auf S. 10). Die Basis dieses Netz-

11 O'Reilly, C.; Ellison, G.: ‚Eye Spy Private High', in: British Journal of Criminology 2006, No. 4, pp. 641-660 (649)

12 Hoogenboom, B.: Grey Policing: A Theoretical Framework, in: Policing & Society 1991, No. 1, pp. 17-30 (26)

Karrieren jenseits des Staatsdienstes

Eine kleine Liste bekannter ehemaliger Polizisten und Strafverfolger lässt erahnen, wie weit die personellen Verflechtungen zwischen staatlicher und privater Sicherheitselite mittlerweile gediehen sind:

Buchert, Rainer: Ombudsmann gegen Korruption von namhaften Unternehmen, vorher: Kriminaldirektor im Bundeskriminalamt (BKA), Präsident des Landeskriminalamts (LKA) Sachsen-Anhalt, Polizeipräsident in Offenbach
Hellenbroich, Herbert: in den 1990er Jahren Vorstandsvorsitzender der Industrie- und Handelsschutz GmbH (IHS), vorher Präsident des Bundesamtes für Verfassungsschutz (BfV) und des Bundesnachrichtendienstes
Hoffmann, Wolfhardt: Sicherheitsberater von IHS, vorher: Polizeipräsident Frankfurt am Main
Langendörfer, Dieter: Sicherheitschef VW-Konzern, vorher: Kriminaloberrat im LKA Hamburg
Menk, Thomas: bis Juni 2010 Leiter Konzernsicherheit DaimlerChrysler, vorher: beschäftigt im Bundesinnenministerium (BMI) und im BfV
Neubeck, Gerd: ab 2009 Nachfolger von J. Puls als Chef der Konzernsicherheit der Deutschen Bahn, vorher: Polizei-Vizepräsident in Berlin
Puls, Jens: bis 2009 Leiter Konzernsicherheit Deutsche Bahn AG, vorher: Kriminaldirektor Kripo Frankfurt am Main
Rupprecht, Reinhard: Berater des ASW (Arbeitskreis für Sicherheit in der Wirtschaft) und der Telekom nach dem Überwachungsskandal, vorher: Abteilungsleiter im BMI, BKA-Vizepräsident
Sack, Dieter K.: bis 2008 Direktor von Corporate Security BASF, seitdem freiberuflicher Consultant im Bereich Security Management, vorher BKA
Schaupensteiner, Wolfgang: 2007-2009 „Chief Compliance Officer" der Deutschen Bahn, 2009: Gründung eines eigenen Unternehmens „Corporate Risk & Compliance Consulting", vorher Oberstaatsanwalt (Korruptionsbekämpfung) in Frankfurt am Main
Steininger, Harald: 1999-2002: Head of Corporate Security der Deutschen Bank, danach bis 2007 Sicherheitschef der Telekom, vorher: Polizei in Hessen, Bundeskriminalamt
Tidiks, Thomas: Chief Security Officer der Henkel-Gruppe, vorher 13 Jahre Polizist

Quelle u.a.: Dieter Schenk: BKA. Polizeihilfe für Folterregime, Bonn 2008, S. 285-287

werks sind die gemeinsame berufliche Sozialisation, eine gewisse Gleichförmigkeit in der Denkungsart und den Kategorien der Wahrnehmung, die Kenntnis des Gegenübers aus der Binnenperspektive sowie auch die persönliche Bekanntschaft. Auf dieser Ebene vielfacher Ge-

meinsamkeiten, so die Vermutung, lassen sich viele Dinge problemloser und jenseits bürokratisch-rechtlicher Regulierungen schneller erledigen.

Die dritte Ebene der Kooperation bezieht sich auf die direkten Formen arbeitsteiliger Zusammenarbeit. Für diesen Aspekt sind die unterschiedlichen rechtlichen und institutionellen Bedingungen beider Seiten ausschlaggebend. Die öffentliche Polizei ist durch das Polizei- und Strafprozessrecht in ihrem Handlungsrepertoire – so ausgeleiert die Rechtsnormen mittlerweile auch sein mögen – begrenzt; gleichzeitig hat sie faktisch kaum Möglichkeiten, Verdachtschöpfung in den internen Bereichen von Unternehmen zu betreiben. Das ist umgekehrt das Feld, zu dem die privaten Ermittler, ermächtigt durch das Unternehmen, direkten Zugang haben. Sie sind nicht behindert durch fehlende Ermittlungsbefugnisse, sondern durch die Persönlichkeitsrechte der Betroffenen, durch Datenschutz- und Arbeitsrecht oder durch zivilrechtliche Bestimmungen. Angesichts dieser Konstellation wird gerne auf die durch öffentlich-private Kooperationen noch keineswegs ausgeschöpften „Synergien in der Ermittlungsarbeit" hingewiesen.[13]

Dass die Privaten in diesen Konstellationen die „dirty work" übernähmen, ist bereits in den 1980er Jahren vermutet worden; dabei könne es sich sowohl um Tätigkeiten handeln, die nur der staatlichen Polizei untersagt seien, wie um solche, die generell illegal seien.[14] In der Selbstdarstellung eines privaten Anbieters werden nicht nur die „hohen ethischen Standards" erwähnt, denen man sich verpflichtet fühle. Es wird zugleich darauf hingewiesen, dass man Informationen auch durch „Undercover agents, technische Einsatzmittel etc." gewinne.[15] In welchem Ausmaß derartige Arbeitsteilungen in Deutschland stattfinden, ist unbekannt. Der tabellarischen Übersicht des Bundesverbandes Deutscher Detektive für 2009 ist zu entnehmen, dass sieben Prozent der Auftraggeber aus den Bereichen „Körperschaften des öffentlichen Rechts, Behörden, Sonstige" stammten.[16] Die bekannteste Public-Private Partnership dieser Art war der Fall Werner Mauss (s. Kasten auf S. 12). Aus der jüngeren Vergangenheit

13 Wörner, R.: Kooperationsformen von Versicherungen und Polizei als wirksames Mittel gegen Versicherungsbetrug in der Schadensversicherung, in: der kriminalist 2006, H. 6, S. 253-258 (253)

14 s. Marx, G.T.: The Interweaving of Public and Private Police in Undercover Work, in: Shearing, C.D.; Stenning, Ph.C. (eds.): Private Policing, Newbury Park 1987, pp. 172-193

15 Nowotny, V.; Flormann, W.: Control Risks: Kontrolle ist machbar – auch in Krisensituationen, in: der kriminalist 2000, H. 4, S. 165-167 (166)

16 www.bdd.de/Download_Oeffentlicher_Bereich/DatenundFakten2009.pdf

gibt es wenig Bekanntes: etwa dass kommunale Ordnungsbehörden Detektive beauftragten, um illegale Müllentsorger zu identifizieren,[17] oder dass eine Ermittlungsfirma „auf Empfehlung einer deutschen Strafverfolgungsbehörde in der Ukraine eine kriminelle Struktur" aufdecken konnte.[18]

Die vierte Beziehung zwischen der öffentlichen Polizei und den privaten Ermittlern besteht im Informationsaustausch. Sowohl die Sicherheitsdienste als auch die Polizeiführungen sehen in der Weitergabe und gegenseitigen Nutzung von Informationen das wichtigste Element der Zusammenarbeit.[19] Dabei kann es sich um einzelfallbezogene Nachrich-

Werner Mauss

Nach eigenen Angaben (www.werner-mauss.de) war der Privatdetektiv an der Festnahme von „ca. 2.000" Personen beteiligt. Seit Ende der 60er Jahre war Mauss vom Bundeskriminalamt und verschiedenen Länderpolizeien als „ziviler Mitarbeiter" (Mauss' Selbstbeschreibung) eingesetzt worden; korrekter müsste man sagen als eine Mischung aus V-Mann und verdecktem Ermittler. Sein einträgliches Hauptgeschäft bestand in Aufträgen von Versicherungen, zur Aufdeckung von Versicherungsbetrug oder Wiederbeschaffung von Hehlerware. Mauss arbeitete gleichzeitig für die Polizei, erhielt Einblick in Ermittlungsunterlagen, konnte Haftanstalten besuchen, Scheingeschäfte abwickeln und sich mit falschen Identitäten bewegen. Im Zusammenhang mit dem niedersächsischen Polizeiskandal Anfang der 80er Jahre wurde Mauss einer größeren Öffentlichkeit bekannt. Später war er in Südamerika tätig und – hauptsächlich in Kolumbien – an der Freilassung westlicher Geiseln beteiligt.

ten handeln. In einigen deutschen Großstädten ist etwa die Beteiligung privater Sicherheitsdienste an polizeilichen Fahndungen seit mehreren Jahren vertraglich geregelt.[20] Der Informationsaustausch ist darüber hin-

17 Brauser-Jung, G.: Das überwachungsbedürftige Sicherheitsgewerbe des § 38 I Nr. 2 und 5 GewO – zum rechtlichen Rahmen des Detektivgewerbes und des Gebäudesicherungseinrichtungsgewerbes, in: Stober, R.; Olschok, H. (Hg.): Handbuch des Sicherheitsgewerberechts, München 2004, S. 207-221 (219)

18 Nowotny; Flormann a.a.O. (Fn. 15), S. 166

19 exemplarisch: Kötter, F.P.: Wie private Dienstleister die Polizei unterstützen können, in: Polizei – heute 2007, H. 3, S. 107-109; Ziercke, J.: Kooperationsfelder Polizei – Private Sicherheit, in: Die Polizei 2004, H. 11, S. 331 f.

20 Bernhard, H.: Möglichkeit und Grenzen der Zusammenarbeit von Behörden/Polizeien mit privaten Sicherheitsdiensten – aus Sicht der Polizei, in: Stober, R. (Hg.): Jahrbuch des Sicherheitsgewerberechts 1999/2000, Hamburg 2000, S. 23-34; Schmidt, S.: Das ex-

aus in einzelnen Deliktsbereichen institutionalisiert; für Deutschland ist die Datenbank „UNI-WAGNIS“, in der die Versicherungen auffällige Schadensfälle erfassen, ein Beispiel für eine private Datensammlung, auf deren Bestände die Polizei – mittelbar – zugreifen kann.[21]
In anderen Feldern sind die intensivierten Informationsbeziehungen eine Folge gewandelter Sicherheitslagen oder -politik. Dazu einige Beispiele:

- Im Hinblick auf den Schutz von Betriebsgeheimnissen gibt es rechtlich weiterhin eine Zweiteilung: Handelt es sich um die unbefugte Weitergabe an Private, dann liegt die Abwehr dieser „Konkurrenzausspähung“ oder „Industriespionage“ bei den Unternehmen selbst. Erfolgt die Ausforschung im Auftrag eines Staates („Wirtschaftsspionage“), dann fällt deren Aufdeckung in Deutschland in die Zuständigkeit des Verfassungsschutzes, die Ahndung in die des Strafverfolgungssystems.[22] Angesichts der jüngeren Entwicklungen wird diese Unterscheidung mehr denn je hinfällig. In einer globalisierten Ökonomie, in der zugleich mit den Unternehmen sich Nationalstaaten in der Konkurrenz um Standortvorteile, technologischen Fortschritt und Wachstumsraten befinden, treten fremder Staat und fremdes Unternehmen als kaum unterscheidbare (verdeckte) Akteure auf. Die Abwehr von Wirtschaftsspionage, so der Staatssekretär im Bundesinnenministerium, bilde „einen wichtigen Aufgabenschwerpunkt“ für das Bundesamt für Verfassungsschutz, dessen Kapazitäten in diesem Bereich verstärkt worden seien. Gemeinsam mit den Landesämtern unterstütze man die Unternehmen beim „Informationsschutz“ und könne dabei „umfassende Vertraulichkeit zusichern“.[23] Zwar liegt es in der Natur der Sache, dass die Öffentlichkeit nichts über die Informationen selbst erfährt. Dass auch nichts über die Verfahren, die Beteiligten, die Menge und die Routinen des Datenverkehrs bekannt ist, deutet auf erhebliche demokratische und bürgerrechtliche Defizite hin.
- Seit den 1990er Jahren wird der Bekämpfung der Geldwäsche international hohe Priorität eingeräumt. Banken und Geldinstituten sind Identifizierungs-, Registrierungs- und Meldeverpflichtungen auferlegt worden. Die Banken selbst sind von der Strafandrohung betroffen, indem sie sich der Beihilfe schuldig machen können. Das heißt nach dem Willen

---

pandierende private Sicherheitsgewerbe – droht der Verlust des staatlichen Gewaltmonopols im öffentlichen Raum?, Berlin 2004

21 Wörner a.a.O. (Fn. 13)

22 Strümpfel, J.: Werkzeuge der Industriespionage, in: www.dfn-cert.de/dokumente/workshop/2007/dfncert-ws2007-f9.pdf

23 Fritsche, K.-D.: Sicherheit für Bürger und Unternehmen, in: Innenpolitik 2010, H. 6, S. 4-7 (6)

des Gesetzgebers sollen Banken und Strafverfolgung zusammenarbeiten; demzufolge haben beide gemeinsame Kriterien für verdächtige Transaktionen entwickelt.[24] Eine jüngere Untersuchung stellt für Frankreich fest, dass der Informationsaustausch zwischen Geldinstituten und Strafverfolgungsbehörden zur Routine geworden sei und zur Entwicklung gemeinsamer Erkenntnissen geführt habe.[25]

Ein zweiter Bereich, der sicherheitspolitisch aufgeladen wurde, ist die „Kritische Infrastruktur". Durch die Privatisierungspolitik der vergangenen Jahrzehnte handelt es sich bei diesen Sparten mittlerweile meist um privatwirtschaftlich verfasste Strukturen: Energie- und Wasserversorgung, Verkehr, Kommunikation etc. Aber auch die Versorgung mit Lebensmitteln wird zur „Kritischen Infrastruktur" gezählt. Die Reichweite des Begriffs ist unbestimmt. Diese Bereiche sind angesichts des Gefahrenpotentials (Atomkraftwerke, chemische Industrie), angesichts ihrer Verletzlichkeit (Trinkwasserversorgung, Digitalisierung) und angesichts der terroristischen Bedrohung zu einem wichtigen Feld der Zusammenarbeit von (privaten) Betreibern und staatlichen Sicherheitsapparaten geworden. Gefahrenabwehr als staatliche Aufgabe und Selbstschutz der Unternehmen sind nahezu identisch. Ein reger Informationsaustausch, fallbezogener wie strategischer Art, liegt nahe. Auch die Ausweitung der Sicherheitsüberprüfungen auf den „vorbeugenden Sabotageschutz" erlaubt Unternehmen, ihre in „lebens- oder verteidigungswichtigen Einrichtungen" Beschäftigten von Polizei und Verfassungsschutz überprüfen zu lassen.[26] Damit ist der Austausch von personenbezogenen Daten auf eine rechtliche Grundlage gestellt.

- Was die Digitalisierung technisch ermöglicht bzw. erleichtert, wurde und wird durch die Politik des Anti-Terrorismus zu realisieren versucht: eine systematische und umfassende Verknüpfung privater und öffentlicher Informationsbestände. Dabei werden zum einen private Informationssammlungen erst staatlich vorgeschrieben: Das gilt nicht nur für den Bereich der Geldwäsche, sondern z.B. auch für die „Vorratsdatenspeicherung" im Bereich der Telekommunikation. Der Staat ver-

24 s. etwa die Formulierung von „Anhaltspunkten" durch das Bundeskriminalamt und den Zentralen Kreditausschuss, einem Zusammenschluss der 5 Spitzenverbände der deutschen Kreditwirtschaft, abgedruckt in: Körner, H.H.; Dach, E.: Geldwäsche, München 1994, S. 162 f.

25 Favarel-Garrigues, G.; Godefroy, Th.; Lascoumes, P.: Sentinels in the Banking Industry, in: British Journal of Criminology 2008, No. 1, pp. 1-19 (18) („and led to the development of joint intelligence ‚production'")

26 § 1 Abs. 4 Sicherheitsüberprüfungsgesetz, eingefügt im Januar 2002

pflichtet die Unternehmen zur Erhebung und zur Speicherung von Daten, die sie (in diesem Umfang etc.) aus eigenen Motiven nicht erheben würden. Zum anderen wird der staatliche Zugriff auf privat vorhandene Informationsbestände gesucht. Dass staatliche Sicherheitsbehörden die Zusammenarbeit mit Google oder den Betreibern „sozialer Netzwerke" suchen, ist logische Folge der Strategie informationeller Vernetzung. In dem Maße, wie die privaten Datenbestände wachsen, nehmen die Informationen zu, auf die staatliche Sicherheitsapparate mittelbaren Zugriff erhalten können – sei es „reaktiv" im Ermittlungsverfahren oder „präventiv" im Hinblick auf Lagebilderstellung, Gefährdungsprognosen und Verdachtschöpfung. Auch hier muss darauf hingewiesen werden, dass es sich nicht um einseitige Informationsbeziehungen handelt, sondern dass – in einigen Feldern (Gefährdungsanalysen, modus operandi) die Informationen von den Sicherheitsbehörden zu den Privaten gehen.

Grauzonen, mehrfach verschachtelt

Vor knapp zwei Jahrzehnten hat Bob Hoogenboom den Komplex polizeilich-privater Ermittlungen als „grey policing" bezeichnet. Der zunehmenden Bedeutung des Informationsaustauschs und der „Auswertung von Informationen" folgend, hat er vor wenigen Jahren auf die Herausbildung von „grey intelligence" hingewiesen.[27] Seine Anregungen sind international auf wenig, in Deutschland auf fast keine Resonanz gestoßen. Über jene Zone zwischen Unternehmens- und öffentlicher Sicherheit, zwischen privaten und staatlichen Ermittlungen, zwischen Schadensbegrenzung und Strafverfolgung, zwischen unternehmerischen und staatlichen Sicherheitsinteressen ist – jenseits der anfangs erwähnten Ereignisse – zuverlässig nur bekannt, dass es sie gibt und dass ihre Bedeutung vermutlich wächst.[28] Angesichts dieses Nichtwissens kann abschließend nur auf die drei wichtigsten Probleme hinwiesen werden:

Erstens bedeutet „Sicherheit" aus der Perspektive von Unternehmen, dass ihre Interessen gegenüber Beschäftigten, Kunden, Konkurrenten, fremden Staaten, Terroristen oder Saboteuren geschützt werden. In

27 Hoogenboom a.a.O. (Fn. 12); s.a. ders.: Die Verflechtung zwischen staatlicher und privater Polizei. Zur Entstehung von „grey policing" in den Niederlanden, in: Brusten, M. (Hg.): Polizei-Politik, Kriminologisches Journal 4. Beiheft, Weinheim 1992, S. 197-208; ders.: Grey Intelligence, in: Crime, Law and Social Change 2006, No. 4-5, pp. 373-381

28 Ein Antrag von Mitgliedern der CILIP-Redaktion, für Deutschland eine erste empirische Bestandsaufnahme zu erstellen, wurde von der Forschungsförderungs-Einrichtung abgelehnt.

dem Maße, wie die Unternehmen die Aufdeckung, Abwehr und Sanktionierung mit professionalisierten Abteilungen selbst in die Hand nehmen, sinkt der rechtsstaatliche Schutz für alle Beteiligten, und zugleich wachsen die Überschneidungen, mögliche Konkurrenzen, aber auch Formen der Kooperation mit staatlichen Polizeien (und Geheimdiensten). Durch die Einschaltung privater Ermittlungsdienste entsteht zweitens ein Markt verdeckter Ausforschungs- und Überwachungsmethoden, die von verschiedenen Akteuren in wandelnden Interessenkonstellationen zu unterschiedlichen Zwecken genutzt werden können.

Wechselnd, so kann drittens vermutet werden, sind die Dominanzverhältnisse zwischen den Beteiligten: Während bei betriebsinternen Delikten die staatliche Strafandrohung für die Unternehmen nur die zweitbeste Lösung darstellt, existieren in anderen Bereichen (Terrorabwehr, Wirtschaftsspionage, Geldwäsche und mitunter Korruption) gleichgerichtete Interessenlagen, so dass die privaten und privat erlangten Informationen ein reiches Reservoire für staatliche Ermittlungen darstellen.

In diesem Geflecht bleiben Transparenz und Kontrollierbarkeit offenkundig auf der Strecke.

Saubere Geschäfte

Korruptionsbekämpfung und Datenaffäre bei der Bahn

von Albrecht Maurer

Anfang Juni 2008 begann in Parlament und Öffentlichkeit eine Auseinandersetzung um die inneren Zustände der Deutschen Bahn AG. Was als Datenaffäre gehandelt wurde, war nur möglich durch den systematischen Missbrauch von Kontroll- und Aufsichtsrechten durch die für die Korruptionsbekämpfung zuständigen Organe des Konzerns und ihre externen Helfer.

„Was dem Staat der Terrorverdacht, ist etlichen Unternehmen mittlerweile der Korruptionsverdacht", schrieb Hans Leyendecker im Juni 2009 in der „Süddeutschen" anlässlich der Datenaffäre bei der Bahn. „Mit enormer Energie gehen Sicherheitsabteilungen großer Konzerne gegen vermutete oder behauptete Kriminalität vor, die sie der Einfachheit halber ‚Korruption' nennen … Selbst das Aufspüren von möglichen Verstößen wurde intern damit begründet, dass man so die Korruption bekämpfen wolle."[1]

Die Affäre bei der Deutschen Bahn AG (DB AG) förderte einen kaum vorstellbaren Umgang des Unternehmens mit den Daten der eigenen aber auch denen fremder Belegschaften und Geschäftspartner zutage. Unter dem damaligen Bahnchef Hartmut Mehdorn hatte der Konzern seine Beschäftigten „systematisch einer Rasterfahndung" unterzogen.[2] Seit Ende der 90er Jahre hatte es – ohne Kenntnis des Betriebsrates und des betrieblichen Datenschutzbeauftragten – mehrere Wellen von „Screenings" gegeben. Bei der größten derartigen Aktion waren in den Jahren 2002/2003 die Daten von 170.000 MitarbeiterInnen mit denen von 80.000 Partnerfirmen abgeglichen worden, um mögliche Betrügerei-

1 Süddeutsche Zeitung v. 12.6.2009
2 Stern v. 2.4.2009

en aufzudecken. Zur Aufklärung möglicher Verstöße ließ der Bahn-Konzern MitarbeiterInnen auch von „externen Dienstleistern", im Klartext: privaten Ermittlerfirmen, ausforschen. Projekte trugen Phantasienamen wie „Babylon", „Eichhörnchen", „Rubens" oder „Kabeljau".

Möglich war das Ganze nur durch den nahezu unbegrenzten Zugang der Ermittlungsstellen des Konzerns zu Daten von Beschäftigten und Geschäftspartnern. Die Bespitzelung diente aber nicht nur der Korruptionsbekämpfung, sondern auch zur Identifizierung von internen KritikerInnen und deren journalistischen Kontaktleuten. Um den „Abfluss" betriebsinterner Informationen zu unterbinden, wurden von März 2005 bis Oktober 2008 täglich rund 145.000 E-Mails automatisch auf bestimmte Adressaten und eine Liste von Suchbegriffen hin kontrolliert, die in diesem Zeitraum insgesamt 45-mal bearbeitet und ergänzt wurde und am Ende rund 570 solcher „Hitwords" enthielt.[3]

Nachdem schon im Jahre 2008 immer mehr Details der Affäre in die Schlagzeilen geraten waren und der damalige Bahnvorstand aus naheliegenden Gründen nicht zu einer Aufklärung bereit war, gab der Aufsichtsrat des Konzerns im Februar 2009 zwei Untersuchungen in Auftrag: die eine bei dem Wirtschaftsprüfungsunternehmen KPMG und die andere bei den ehemaligen JustizministerInnen Gerhart Baum und Herta Däubler-Gmelin.[4] Ende März 2009 trat Hartmut Mehdorn endgültig zurück, sechs Wochen später wurde auch sein Chief Compliance Officer Wolfgang Schaupensteiner geschasst.[5] Am 13. Mai nahm der DB-Aufsichtsrat die Empfehlungen der beiden Gutachten an. Für die Bundesregierung war die Sache kurz darauf erledigt. Im Juni 2010 erklärte sie in der Antwort auf eine Anfrage der Linken im Bundestag, sie betrachte „die Datenaffäre als aufgearbeitet". Die staatsanwaltschaftlichen Untersuchungen dauerten zwar noch an, aber „der Vorstand der DB AG hat die notwendigen organisatorischen und personellen Konsequenzen aus den Feststellungen gezogen."[6]

Wie war ein solcher Skandal möglich in einem Unternehmen, das weltweit dafür gelobt worden war, die seit etwa 15 Jahren international immer dringender geforderten Anti-Korruptionsrichtlinien und -maß-

3 Stern v. 2.4.2009; Süddeutsche Zeitung v. 3.4.2009

4 KPMG AG: Die Sonderuntersuchung bei der DB AG, Berlin 13.5.2009; Däubler-Gmelin, H.; Baum, G.: Zusammenfassender Kurzbericht, Düsseldorf, Berlin 13.5.2009

5 Süddeutsche Zeitung v. 28.5.2009

6 BT-Drs. 17/2229 v. 18.6.2010

nahmen vorbildlich umgesetzt zu haben. Die Frage führt mitten in das Geflecht aus aktiven oder ehemaligen VertreterInnen staatlicher Sicherheitsbehörden, privaten Ermittlungsdiensten und den im Bahnkonzern unter dem Stichwort „Compliance“ eingerichteten Strukturen.

Die Entwicklung der DB-Compliance

Der Begriff „Compliance“ schwappte in den 90er Jahren aus dem US-Managementjargon nach Europa über und bezeichnet die Selbstverpflichtung von Unternehmen, „ein System einzurichten, welches gewährleistet, dass sich alle Mitarbeiter an die rechtlichen Rahmenbedingungen halten (to comply: befolgen, erfüllen). Das betraf (zunächst, A.M.) insbesondere Geldwäsche, Korruption und Insiderhandel ... Mittlerweile reicht das Einhalten formalrechtlicher Regelungen nicht mehr aus, um in der Öffentlichkeit einen glaubwürdigen Eindruck von Integrität zu präsentieren. Schritt für Schritt entwickeln Unternehmen darum zusätzlich Standesregeln und unternehmensspezifische Verhaltenskodizes (‚Codes of Conduct‘).“[7] Und nicht nur das: Sie bauen auch die entsprechenden internen Kontroll- und Ermittlungsstrukturen auf, um Verstöße gegen die rechtlichen und „ethischen“ Regeln aufzudecken bzw. zu verhindern.

Trotz einer Reihe von Korruptionsfällen beim Zusammenschluss von Bundesbahn (West) und Deutscher Bahn (Ost) gab es ein solches fest organisiertes Compliance Management bei der DB AG in den 90er Jahren noch nicht. Die Korruptionsbekämpfung erfolgte – wie es im KPMG-Bericht heißt – „einzelfallbezogen durch die Organisationseinheiten Recht, Konzernrevision und Konzernsicherheit“.[8] Der Bericht nimmt einen Vorstandsbeschluss vom 16. Februar 2001 als Ausgangspunkt für die Einrichtung eines eigenen Compliance-Bereichs im Konzern.[9] Die Ermittlungen wurden zwar weiterhin von der Konzernrevision oder der Konzernsicherheit geführt, ein neu geschaffener Lenkungskreis Compliance (LKC) „unter der Leitung der Organisationseinheit Recht“, diente aber nun als Koordinations- und gleichzeitig als Entscheidungsgremium

7 Geißler, C.: Was ist compliance management?, in: Harvard Business Manager 2004, H. 2, www.harvardbusinessmanager.de/heft/artikel/a-620695.html
8 KPMG a.a.O. (Fn. 4), S. 1
9 ebd., S. 73 ff.

für die an der Korruptionsbekämpfung beteiligten Gliederungen des Konzerns.

Leiter des LKC und gleichzeitig Chef der Abteilung „Ermittlung und besondere Aufgaben“ war ab 2001 Jens Puls, der zuvor siebzehn Jahre beim Bundeskriminalamt (BKA) gearbeitet hatte. Weitere Mitglieder waren die Leiter der Organisationseinheiten Revision, Recht und Sicherheit, die Chefs der Abteilungen „Konzernsicherheit Ermittlungen“ und „Arbeitsrecht und Baurecht“ sowie die beiden im Jahr zuvor als Ombudsleute bestellten Anwälte, die als Ansprechpartner unter anderem für das Personal dienen sowie Anzeigen und Verdachtshinweise auf Korruption und andere Regelverstöße entgegennehmen sollten. Der eine hatte bis 1999 in der Organisationseinheit Recht des Konzerns gearbeitet, der andere hatte eine Polizeikarriere hinter sich: Er war zunächst Mitarbeiter des BKA, danach Landeskriminaldirektor in Magdeburg und zuletzt Polizeipräsident in Offenbach gewesen.

Ab 2001 entstanden auch diverse Richtlinien, die schrittweise den Praktiken der mit der „Compliance“ befassten Organisationseinheiten des Konzerns eine interne Rechtsgrundlage geben sollten. Im Juni 2002 trat die Richtlinie 166.0101 – „Interne Revision: Ziele, Aufgaben, Kompetenzen, Verantwortung, Zusammenarbeit“ – in Kraft. Sie verlieh der Konzernrevision ein „uneingeschränktes Informationsrecht“. Deren PrüferInnen konnten danach alle für notwendig befundenen Informationen, auch IT-gestützte, einholen und die Unterlagen einsehen. „Der Konzernrevision wurde darüber hinaus die Befugnis erteilt, im Rahmen ihrer Aufgabenstellung Externe in ihre Prüfungen einzubinden.“[10] Die Richtlinie 135 0101 „Ermittlungen: Ziele, Aufgaben und Zuständigkeiten“ räumt den ErmittlerInnen des Konzerns zusätzlich die Befugnisse zur Einbindung externen Fachwissens und zur Durchführung von Befragungen ein. In der Fassung vom 1. Juni 2007 erhielten „die mit der Durchführung von Ermittlungen beauftragten Mitarbeiter/innen“ ferner ein „Zutrittsrecht zu allen Einrichtungen und Fahrzeugen des DB-Konzerns.“[11]

Konzernrevision und Konzernsicherheit erhielten zwar durch diese Richtlinien umfassende Befugnisse für die Ermittlungen, die der LKC anordnete. Kennzeichnend ist aber, dass konkretisierende Regelungen

10 ebd., S. 74

11 Konzernrichtlinie 135 0101 Organisation und Managementsysteme, S. 4

zum Beispiel für den Umgang mit verdächtigten MitarbeiterInnen oder Anweisungen, wie Verfahren durchzuführen seien, fehlten.[12]

Der kurze Dienstweg zu den Privaten

Die Befugnisse zur Nutzung externen Fachwissens und zur Einbeziehung Externer legitimierten notdürftig den Beizug privater Rechercheure und Ermittlungsfirmen, der bereits vor Erlass der Richtlinien zur Praxis der KorruptionsbekämpferInnen des Konzerns gehörte.

Mindestens sechs solcher Firmen haben im Laufe der Jahre Aufträge der Bahn erhalten, die meisten gingen an die Network Deutschland GmbH (NWD), mit der die Bereiche Konzernsicherheit und Revision spätestens seit 1998 zusammenarbeiteten und die danach auch zum wichtigsten „externen Dienstleister" des LKC wurde.[13] Der Kontakt zu NWD soll auf einem Seminar entstanden sein, erklärten Bahnvertreter gegenüber dem Berliner Datenschutzbeauftragten. Das kleine Unternehmen „mit vier bis sechs Mitarbeitern, die von der Ausbildung her Mathematiker oder Informatiker seien ... sei für die Deutsche Bahn AG insbesondere aufgrund seiner internationalen Kontakte interessant gewesen", heißt es im Gesprächsvermerk des Datenschutzbeauftragten.[14] Die Muttergesellschaft der NWD soll ihren Sitz in Großbritannien gehabt haben, in den beiden Untersuchungsberichten und den Unterlagen des Verkehrsausschusses findet sich nicht einmal deren Name. Der wurde auch auf Nachfrage von Abgeordneten weder im Verkehrsausschuss noch im Plenum des Bundestags bekannt gegeben.[15] Fakt ist allerdings, dass der Berliner Firmensitz der NWD sehr schnell nach dem Bekanntwerden der Telekom- und DB-Skandale „verwaist" war.[16]

---

12 KPMG a.a.O. (Fn. 4), S. 74

13 Ursprünglich hatte der spätere Chief Compliance Officer Schaupensteiner behauptet, NWD sei die einzige Firma gewesen, die entsprechende Aufträge erhalten hatte. Diese Version ließ sich ab Februar 2009 nicht mehr halten, s. Deutsche Bahn: Zwischenbericht – Überprüfung der Ordnungsmäßigkeit von Maßnahmen der Korruptionsbekämpfung in den Jahren 1998-2007, Berlin 2009 (dem BT-Verkehrsausschuss vorgelegt am 10.2.2009), S. 36

14 Berliner Beauftragter für Datenschutz und Informationsfreiheit: Gespräch mit der Deutschen Bahn AG über die Geschäftsbeziehungen des Unternehmens mit der Network Deutschland GmbH am 28. Oktober 2008, Vermerk v. 13.11.2008, S. 2 (www.netzpolitik.org/wp-upload/datenschutz_bei_der_bahn.pdf)

15 BT-PlProt. 16/204 v. 11.2.2009, S. 22058 f.

16 Hamburger Abendblatt v. 4.6.2008

Wie viele „Projekte“ der NWD zugeschanzt wurden, ist nicht definitiv klar. Bis 2007 sollen es insgesamt 43 mit einem Volumen von insgesamt 800.000 Euro gewesen sein.[17] Für ihren größten Einzelauftrag kassierte die NWD 128.000 Euro.[18] Die Vergabe erfolgte jeweils „ausschließlich mündlich“, was die Berliner DatenschützerInnen auch wegen der Höhe erstaunte. Die Aufträge seien nicht ausgeschrieben worden, weswegen es „entsprechend der Praxis der Deutschen Bahn AG“ nicht einmal ein „kaufmännisches Bestätigungsschreiben“ gegeben hat. Selbst bei „Großprojekten“, bei denen sich Vertreter der Bahn und der NWD zuvor zu einem Workshop getroffen hatten, machten sich nur Letztere Aufzeichnungen. Nur dann, wenn ein Projekt zu Verdachtsfällen führte, lieferte NWD ein Gutachten, in dem dann auch die Aufgabenbeschreibung und die Zielsetzung des Auftrags nachzulesen war. Gab es keinen Verdacht oder führten die Nachforschungen zur Entlastung der betroffenen MitarbeiterInnen, dann gab es auch keinen Bericht – angeblich aus Fürsorgepflicht gegenüber den Betroffenen.[19] Diese Fürsorge reichte aber nicht für eine Benachrichtigung des Betriebsrates oder des betrieblichen Datenschutzbeauftragten.

Die Bahn, vor allem die Konzernrevision, lieferte Daten an NWD, die dann jeweils weitere Informationen suchte. Bei Großprojekten waren über tausend Personen betroffen, bei den kleineren „insgesamt ca. 500“. MitarbeiterInnen, deren EhepartnerInnen, Lieferanten und sonstige Vertragspartner seien überprüft worden – „nicht jedoch Fahrgäste“. Die NWD war auch an dem Screening von 2002/2003 beteiligt und lieferte die Software für den Datenabgleich, der aber in Räumen des Konzerns stattgefunden habe. NWD besorgte unter dem Codewort „Babylon“ auch die weiteren Ermittlungen über Personen, die bei diesem Abgleich auf die „Positivliste“ gerieten. Anders als beim Telekom-Skandal habe NWD für den Bahnkonzern keine Telefon-, Bank- oder Steuerdaten ausgewertet, betonten die DB-Vertreter gegenüber dem Berliner Datenschutzbeauftragten.

Allerdings, so heißt es weiter in dem Gesprächsvermerk, „räumten die Vertreter der Deutschen Bahn AG auf Nachfrage ein, dass sie bezüglich der Umsetzung der Aufträge keine Vorgabe gemacht haben, ent-

17 BT-Verkehrsausschuss, Protokoll der 68. Sitzung v 25.6.2008
18 Deutsche Bahn a.a.O. (Fn. 13), S. 26
19 Berliner Beauftragter für Datenschutz a.a.O. (Fn. 14) S. 2 f.

scheidend war nur das Ergebnis. Insofern kann die Deutsche Bahn AG zumindest nicht ausschließen, dass die Network Deutschland GmbH auch Telefonverbindungen, Bank- und Steuerdaten ausgewertet hat. So ist ihr auch nicht bekannt, ob und wenn ja in welchen Fällen Unteraufträge verteilt wurden. Hierzu war die Network Deutschland GmbH jedenfalls unbeschränkt berechtigt."[20] Anders ausgedrückt: im Umgang mit der NWD verfuhr der Bahnkonzern nach dem Motto der drei Affen: nichts sehen, nichts hören und nichts sagen – vor allem aber: nichts niederschreiben.

Dieses Motto galt offenbar auch für die Aufträge, die nicht direkt, sondern über einen Anwalt an die Kölner Detektei Argen gingen, berichtete das „Handelsblatt" unter Berufung auf den Berliner Datenschutzbeauftragten.[21] Im Falle eines der Korruption verdächtigten Mitarbeiters habe diese Firma sehr wohl und offenbar „in großem Umfang" Kontodaten geliefert, mit denen aber die Anschuldigungen nicht nachgewiesen werden konnten. Solche Informationen, gegebenenfalls sogar Original-Kontoauszüge, zu besorgen, gehöre zur „Spezialität" der Detektei. Wie die Firma, die nur vier Angestellte habe, aber einen Jahresumsatz von vier Millionen Euro ausweise, an solche Daten herankomme, sei nicht bekannt. Die Argen GmbH sei ursprünglich der deutsche Ableger der britischen „Argen Information Services" gewesen, die 1968 von einem ehemaligen Mitarbeiter des britischen Inlandsgeheimdienstes MI 5 gegründet wurde und 2003 vom Konkurrenzunternehmen Capcon aufgekauft wurde. Auch dieses Unternehmen wirbt damit, dass Betrugsermittlungen und „forensic accounting" zu seinen Kerngeschäften gehöre.[22]

Kurz aber heftig: die Ära Schaupensteiner

Im Jahre 2007 erfuhr die Organisation des „Compliance-Managements" der DB eine Reorganisation. Der LKC wurde aufgelöst und stattdessen ein eigener Bereich Compliance mit einem Chief Compliance Officer (CCO) an der Spitze geschaffen, der nun direkt dem Vorstandsvorsitzenden unterstand. Die Stelle des CCO übernahm Wolfgang Schaupensteiner, der bis dahin als Oberstaatsanwalt in Frankfurt/Main am-

20 ebd., S. 6 f.
21 Handelsblatt v. 4.5.2009
22 www.capconplc.com

tierte und sich nun – mit Rückkehrgarantie – aus dieser Funktion beurlauben ließ.

Im November 2008 hatte der Bereich Compliance 28 MitarbeiterInnen. „Eine personelle Aufstockung ist vorgesehen", verkündete Schaupensteiner in seinem Referat auf der Herbsttagung des BKA.[23] Hinzu kamen 24 Compliance Officers, die „als Ansprechpartner in allen Bereichen weltweit agieren". Der Bereich gliederte sich nun in drei Abteilungen: zum einen die für „Ermittlungen/Regressierung/Hinweisgebersystem", in die auch die bestehenden Ermittlungsmanagement-Anteile der Konzernsicherheit und der Revision eingegliedert wurden. Hier arbeiteten laut Schaupensteiner neben Bauingenieuren „Spezialisten mit kriminalistischer Berufserfahrung". Laut dem KPMG-Bericht konnte fallbezogen „eine Beauftragung der Konzernrevision erfolgen", wenn „personelle Ressourcen fehlten oder besondere fachliche Expertise für die Fallbearbeitung notwendig" war. Aufgebaut wurde auch eine Einheit „Ermittlungen international".[24] Zuständig war die Abteilung auch für das elektronische Hinweisgebersystem, „eine Internet-Hotline, die weltweit und rund um die Uhr angeklickt werden kann" und Meldungen über anonyme E-Mail-Accounts ermöglichte.

Eine neue „Risikominimierungsrichtlinie", gültig ab Januar 2009, verlieh der Compliance „uneingeschränkte Auskunftsansprüche und Befragungsrechte" und stattete sie – wie zuvor die Konzernrevision – mit der Befugnis aus, alle Informationen (auch IT-gestützte) einzuholen sowie Unterlagen einzusehen.[25]

Die zwei weiteren Abteilungen befassten sich mit „Schulung/Richtlinien/Information" und „Monitoring/Prozesse". An Letztere war auch das „Compliance-Committee" mit den Compliance Officers angegliedert.

Schon als staatlicher Strafverfolger hatte der Korruptionsspezialist Schaupensteiner Kontakt mit seinen neuen Brötchengebern. Mindestens 15 Korruptionskomplexe im Bahnkonzern mit über 200 Beschuldigten soll er als Oberstaatsanwalt bearbeitet haben. Konzernchef Mehdorn sprach von über 500 Verdachtsfällen.[26] Und auch in seiner neuen Rolle

23 Schaupensteiner, W.: Governance und Compliance, Referat auf der BKA-Herbsttagung, 13.11.2008, www.bka.de/kriminalwissenschaften/herbsttagung/2008/schaupensteiner_langfassung_deutsch.pdf

24 KPMG a.a.O. (Fn. 4), S. 76 f.

25 ebd., S. 77

26 Handelsblatt v. 29.5.2007; Neues Deutschland v. 4.2.2009

schien Schaupensteiner mit eisernem Besen kehren zu wollen. Bei Sanktionen, so erklärte er in seinem Vortrag beim BKA, sei „keine Rücksicht auf die hierarchische Einordnung betroffener Mitarbeiter“ zu nehmen. Bei der Compliance gehe es darum, „die loyalen Mitarbeiter zu schützen, die ethischen Werte des Unternehmens konzernweit zu implementieren und mit integren Geschäftspartnern ‚saubere Geschäfte‘ zu machen.“ Repressive und präventive Ansätze seien dabei zu kombinieren.

Als Schaupensteiner im November 2008 seinen Vortrag beim BKA hielt, war die Datenaffäre bereits am köcheln. Fünf Monate zuvor hatte der CCO vor dem Verkehrsausschuss des Bundestages auch die flächendeckenden „Screenings“ der Mitarbeiter und die Kooperation mit der Network Deutschland GmbH rechtfertigen müssen. Ziel sei die „Aufklärung von Nähebeziehungen im Kontext Korruption“ gewesen, wozu geschäftliche, private und persönliche Beziehungen, Wohnort und anderes gehörten. Nähebeziehungen könnten sich zu „Korruptionsbeziehungen“ auswachsen. Die „Compliance“ müsse tätig werde, bevor tatsächlich Anhaltspunkte für eine Straftat vorlägen.[27]

Im Mai 2009 musste der CCO den Hut nehmen, nachdem sich deutliche Hinweise ergeben hatten, dass er selbst die Vernichtung der „Ereignisdatenbank Ermittlungen“ angeordnet hatte, in der alle Compliance-Fälle seit 2001 registriert waren.[28] Statt in sein Amt als Staatsanwalt zurückzukehren, entschied er sich für den Verbleib in der Privatwirtschaft. „Da haben Sie ganz andere Gestaltungsmöglichkeiten.“ Er gründete sein eigenes Unternehmen: „Corporate Risk & Compliance Consulting“.[29]

Alles neu?

„Dr. Rüdiger Grube tritt am 1. Mai sein Amt als neuer DB-Chef an und folgt damit auf Hartmut Mehdorn, der den Posten fast zehn Jahre innehatte.“ So steht es in der „Chronologie“ des DB-Konzernberichts 2009, in der man nach den Gründen für Mehdorns Abgang und nach Spuren des Skandals umsonst sucht. Letztere finden sich erst im „Compliance-Bericht“, wo den LeserInnen mitgeteilt wird, dass der Aufsichtsrat „als Konsequenz aus der Datenaffäre … ein neues Vorstandsressort für Com-

27 BT-Verkehrsausschuss, Protokoll der Sitzung v. 25.6.2008
28 Süddeutsche Zeitung v. 28.5.2009
29 Handelsblatt v. 8.4.2010

pliance, Datenschutz, Konzernsicherheit und Recht geschaffen“ hat. Im dritten Quartal 2009 sei ein „Integriertes Compliance Management“ eingeführt worden, das über die Korruptionsbekämpfung hinaus sämtliche rechtlichen und internen Verhaltensregeln ins Auge fasse und nun nicht mehr in erster Linie repressiv, sondern präventiv ausgerichtet sei.[30]

Das Compliance-Team und das Compliance-Board beschäftigen sich nun in erster Linie mit dem Monitoring von Prozessen, der Ausarbeitung von „Guidelines“, der Beratung und dem Training. Das Compliance-Komitee, „welches sich mit Fällen von möglichen Regelverstößen beschäftigt und Empfehlungen für die weitere Behandlung ausspricht“, führt nun ähnlich wie vor 2007 der Lenkungskreis „keine eigenen Ermittlungen durch, sondern löst solche bei Bedarf lediglich aus.“ Die Ausführung übernimmt eine „Organisationseinheit Ermittlungen“ im Bereich der Konzernsicherheit, über die nichts Weiteres bekannt ist.[31]

Das „elektronische Hinweisgebersystem“ steht „aktuell nicht zur Verfügung“, heißt es auf der DB-Hompage, soll aber nach der „datenschutzrechtlichen Prüfung“ wieder in Betrieb genommen werden. Im November 2010 einigten sich Vorstand und Betriebrat auf eine Vereinbarung zum Beschäftigtendatenschutz, die „eine Verwendung personenbezogener Daten außerhalb der mit der Interessenvertretung vereinbarten IT-Systeme“ ausschließt und Ermittlungen zu Gesetzesverstößen „nur aufgrund hinreichender Verdachtsmomente und nur im Fall des Überschreitens einer Bagatellgrenze“ zulässt.[32]

Auswüchse wie in der „Datenaffäre“ scheinen damit fürs Erste gebannt. Das Grundproblem, dass ein (privatisierter) Konzern neben und in Zusammenarbeit mit staatlichen Polizei- und Strafverfolgungsbehörden und weitgehend nach eigenen Regeln interne Ermittlungen betreibt, bleibt bestehen.

30 www.deutschebahn.com/site/ir/dbkonzern__gb__online__2009/de/start.html
31 www.deutschebahn.de/site/bahn/de/konzern/compliance/team/aufgaben.html
32 DB-Presseinformation v. 25.11.2010

Kooptierte Kameras

Hybride Netzwerke der Videoüberwachung

von Eric Töpfer

Im Vergleich zu zahlreichen anderen Ländern nimmt sich die polizeiliche Videoüberwachung in der BRD bescheiden aus. Der Blick auf die Zahl polizeieigener Kameras verschleiert aber den Umstand, dass die Nutzung fremder Überwachungssysteme durch die Polizei vielfältige Formen hat und undurchsichtige technische und informelle Netzwerke der Überwachung im Wachstum begriffen sind.

Die Aufnahmen, die die bewaffnete Verlegertochter Patricia Hearst beim Überfall der „Symbionese Liberation Army" auf die Hibernia Bank in San Francisco 1974 zeigen, sind eine „Ikone" aus den frühen Tagen der Kameraüberwachung. Dass sie erhalten geblieben sind, ist nicht nur den Investitionen der Bank zu verdanken, sondern auch den gesetzlichen Auflagen, die die Installation von Videokameras für US-amerikanische Geldinstitute bereits in den 60er Jahren zur Pflicht machten.[1]

In der alten Bundesrepublik gab es solche Gesetze nicht, allerdings forderten und förderten Politik und Sicherheitsorgane auch hierzulande die Expansion der „optischen Raumüberwachung" – zum Teil gegen erbitterten Widerstand. Mehr als sechs Jahre hatte eine „Arbeitsgruppe zur Bekämpfung der Banküberfälle" unter Vorsitz des Bundeskriminalamtes (BKA) verhandelt, bevor sich das Kreditgewerbe im „Heißen Herbst" 1977 mit dem damaligen Bundesinnenminister Werner Maihofer auf ein millionenschweres Maßnahmenpaket zur Bankensicherung einigte. Zuvor hatte das BKA Marktstudien erstellt, Kameras in seinen eigenen Eingangshallen getestet und Leistungsanforderungen definiert. Als „optimale Lösung" wurde ein kombiniertes Fernseh- und Fotoüber-

1 Nieto, M.: Public Video Surveillance. Is it an Effective Crime Prevention Tool?, Sacramento 1997, www.library.ca.gov/CRB/97/05/

wachungssystem vorgeschlagen, das sowohl innerbetriebliche Überwachungsfunktionen als auch polizeiliche Interessen an verwertbaren Fahndungsbildern bedienen sollte. Diskutiert und vereinzelt getestet wurde bereits damals die Aufschaltung von Bankenkameras in polizeiliche Einsatzzentralen. Doch die geschätzten Kosten für die Aufrüstung der damals 44.000 Kassenstellen – mehr als 500 Millionen DM – ließen die Banken zögern. Erst nachdem SPD-Fraktionschef Herbert Wehner im Oktober 1977 gepoltert hatte, die Banken seien „Selbstbedienungsläden zur finanziellen Ausstattung von Terroristen" und die Drohung mit gesetzlichen Maßnahmen im Raum stand, verpflichtete sich der Zentrale Kreditausschuss, selbst tätig zu werden: Alle Geldinstitute der Bundesrepublik sollten Kameras einbauen und zwar Einzelbildkameras, weil diese die besten Fahndungsfotos garantierten. Terroristenfahndung und polizeiliche Interessen hatten obsiegt, und angesichts der folgenden Massenbestellungen halbierten sich die Stückkosten für Anlagen zur Raumüberwachung in wenigen Wochen.[2]

Die Indienstnahme Privater und ihrer elektronischen Augen für Zwecke staatlicher Verbrechensbekämpfung hat also durchaus Tradition. Allerdings hat sie sich mit der Normalisierung der Überwachung und dem Siegeszug der Netzwerktechnik sowohl in quantitativer als auch qualitativer Hinsicht deutlich gesteigert. Unterscheiden lassen sich drei Formen der polizeilichen Nutzung fremder Überwachungsinfrastrukturen: die Verwertung von Videoaufzeichnungen zur Strafverfolgung, die technische Aufschaltung zur Echtzeitüberwachung und die persönliche Vor-Ort-Indienstnahme eines Systems durch PolizistInnen.

Sachbeweissammelmaschinen

Rechtlich ist es für die Polizei kaum ein Problem, nicht-polizeiliche Videoaufzeichnungen für die Strafverfolgung zu nutzen. Gebietet § 94 der Strafprozessordnung die Sicherstellung von Beweismitteln, ergänzt § 6b des Bundesdatenschutzgesetzes (BDSG), dass Bilddaten aus der Videoüberwachung öffentlich zugänglicher Räume für andere als die festgelegten Zwecke nur dann genutzt werden dürfen, „soweit dies zur Abwehr von Gefahren, für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist". Und dies auch dann, wenn

2 Bankensicherung perfekt?, in: Sicherheitstechnik 1978, H. 2, S. 23-27; Der Spiegel v. 17.10.1977, S. 84 f. und v. 4.9.1978, S. 52

die Überwachung selbst unrechtmäßig war, wie der spektakuläre Fall des Nagelbombers von Köln illustriert. Nach diesem wurde im Sommer 2004 mithilfe von Aufnahmen einer Kamera des Privatfernsehsenders VIVA gefahndet, die – den Grenzziehungen durch § 6b BDSG zum Trotz – öffentliches Straßenland filmte.[3] Doch selbst in weniger schwerwiegenden Fällen scheint die Abwägung zwischen effektiver Rechtspflege und den Interessen der Betroffenen vor Gerichten in der Regel zuungunsten der letzteren auszufallen.[4]

Private Kameras, die öffentlich zugängliche, aber private Räume und vielfach auch – wenngleich illegal – öffentliche Straßen und Plätze überwachen, gehören heute zur Normalität. Mit ihrer massiven Verbreitung erschließt sich der Polizei zumindest theoretisch eine bedeutende Ressource. Bereits 2002 erklärte der damalige sächsische Innenminister Klaus Hardraht (CDU) auf einer Arbeitstagung zur Zusammenarbeit von Polizei und Sicherheitsgewerbe die Videoüberwachung zu einem beispielhaften Kooperationsbereich: Bei einer Überwachung durch Private seien die verfassungsrechtlichen Bedenken, die bei einem staatlichen Einsatz bestünden, geringer.[5]

In der Praxis ist die Nutzung fremder Videoaufnahmen für die Polizei allerdings nicht ohne Probleme. Sie ist konfrontiert mit unzureichender Qualität von Bildmaterial, der Inkompatibilität von Dateiformaten, der mangelnden Kenntnis von Kamerastandorten oder dem Zeitaufwand, den das Einsammeln und Auswerten von Videomaterial erfordert. Um Abhilfe zu schaffen, beteiligen sich Polizeivertreter an der Entwicklung technischer Normen und Richtlinien, empfehlen entsprechend konforme Anlagen und zertifizierte Errichterfirmen. Kriminaltechniker arbeiten an der digitalen Aufbereitung und Verbesserung von schlecht auswertbaren Bildern,[6] und Informatiker entwickeln Technologien zur Metadatierung von digitalem Videomaterial, damit die Bilderfluten leichter zu durchforsten sind. Und so gehören Videoaufzeichnun-

3 Lietz, H.: Videoüberwachung – Sicherheit oder Scheinlösung?, in: Telepolis v. 6.7.2004, www.heise.de/tp/r4/artikel/17/17813/1.html

4 Stolle, P.: Zur Verwertung von privat gewonnenen Videoaufzeichnungen im Strafverfahren, in: JurPC Web-Dok. 211/2003, Abs. 1-3, www.jurpc.de/aufsatz/20030211.htm

5 Braun, S.: Polizei und privates Sicherheitsgewerbe – gemeinsam für die Sicherheit der Bürger. Arbeitstagung in Dresden, in: DSD – Der Sicherheitsdienst 2002, H. 2, S. 3-6 (5)

6 z.B. die Gruppe „Technologien“ beim BKA, www.bka.de/kriminalwissenschaften/forschung/ki22.htm

gen längst nicht mehr nur bei Schwerverbrechen zum Standardrepertoire der Strafermittlung. Die Berliner Polizei forderte im Jahre 2010 allein vom Verkehrsbetrieb BVG fast dreitausendmal Videoaufzeichnungen an.[7]

Überwachungsnetze

2007 ließ die Polizei Baden-Württemberg einen „Videoatlas" von 4.202 Überwachungskameras an 536 Objekten erstellen und machte damit einen ersten Vorstoß zur systematischen Kartierung von Kamerastandorten.[8] Vorbilder hierfür finden sich in Großbritannien, wo die London Metropolitan Police als Reaktion auf IRA-Anschläge bereits Mitte der 90er Jahre im Rahmen der „Operation Rainbow" begann, eine Datenbank zu „CCTV locations" anzulegen.[9]

Inzwischen ist die Londoner Met allerdings deutlich weiter: C3I, Command-Control-Communication-Information, heißt das Projekt, mit dem die Hauptstadtpolizei 33 Bezirksleitstellen durch drei vernetzte Kommandozentralen ersetzt hat und damit nicht nur den Zugriff auf die zahlreichen Kameras kommunaler „open-street"-Systeme integriert, sondern sich auch anlassbezogen auf mehr als 30.000 Kameras anderer Betreiber aufschalten kann.[10] Zwar ist London sicherlich Spitzenreiter in Sachen vernetzter Überwachung, allerdings beschränkt sich der Trend zur polizeilichen Aufschaltung in Videosysteme anderer Betreiber keineswegs auf die britische Hauptstadt. Als Reaktion auf die fragmentierte und als ineffizient wahrgenommene Überwachungslandschaft entwickelten das Innenministerium und die Association of Chief Police Officers 2007 eine „National CCTV Strategy". Sie wünschen sich darin nicht nur eine Datenbank zur Registrierung aller existierenden Überwachungssysteme, sondern auch die umfassende Vernetzung von Systemen für die polizeiliche Echtzeitaufschaltung und den Online-Zugriff auf Videoaufzeichnungen.[11]

In vergleichbarer Weise wird in Frankreich seit der Novelle des Antiterrorgesetzes („Loi Antiterrorisme") im Jahre 2007 versucht, technische

7 Berliner Abgeordnetenhaus: Drs. 16/15150 v. 21.2.2011
8 die tageszeitung v. 5.5.2007
9 Fussey, P.: Observing potentiality in the global city. Surveillance and counterterrorism in London, in: International Criminal Justice Review 2007, No. 3, pp. 171-192 (175)
10 Capital command, in: CCTV Image, April 2008, pp. 10-14 (11)
11 Joint Home Office ACPO Team: National CCTV Strategy, London 2007

Standards durchzusetzen und auf diese Weise zumindest die Systeme großer Einzelhandels- und Verkehrsunternehmen für den polizeilichen Zugriff zu öffnen.[12] Der „Heimatschutz" hat auch in den USA, wo staatliche Videoüberwachung lange Zeit nur ein nachrangiges Thema war, zu einem Boom der Vernetzung von Systemen geführt: Bilder tausender Kameras aus Nahverkehr, Shopping Malls, Schulen und Wohnanlagen können in den zentralen nach dem Vorbild der „Kriegstheater" des US-Militärs modellierten Kontrollraum der Polizei von Washington, D.C. aufgeschaltet werden; ähnlich ist die Situation in New York, Chicago und vermutlich zahlreichen weiteren US-amerikanischen Großstädten.[13] Angesichts dieser Entwicklung warnt die American Civil Liberties Union eindringlich vor einer „dritten Welle" der Videoüberwachung: „Bereits jetzt beobachten wir den Beginn eines weiteren radikalen Wandels der Nutzung von Überwachungskameras, in denen die Privatkameras der ersten Welle in die zentralen staatlichen Systeme der zweiten Welle integriert werden. Zugleich beobachten wir erste Schritte der Behörden, die Installation privater Kameras zur Pflicht zu erklären … Und da die alten Analogkameras durch neue digitale Modelle ersetzt werden, wird es immer preiswerter und leichter, enorme Überwachungsnetze zu knüpfen und die in diesen Netzwerken generierten Daten zu nutzen und zu missbrauchen."[14]

Auch in Deutschland werden Pläne zur Ausweitung der Überwachung mit Notwendigkeiten der Terrorismusbekämpfung gerechtfertigt. Im Gefolge der gescheiterten Kofferbombenanschläge von Dortmund und Koblenz sprach sich die Innenministerkonferenz im September 2006 dafür aus, „das Instrument der Videoüberwachung stärker als bisher zu nutzen", insbesondere zur „gezielten Beobachtung von Gefahrenschwerpunkten" z.B. im Bereich von Bahnhöfen, Flughäfen und Häfen.[15] Unterstützung erhielten die Innenminister von europäischer Seite: Die Terrorismus-Arbeitsgruppe des Rates der Europäischen Union gab im Oktober desselben Jahres eine Studie zur Nutzung von Videoüberwachung in Auftrag. Die Ergebnisse wurden 2008 präsentiert, und zwischenzeitlich

12 heise news v. 26.7.2007, www.heise.de/newsticker/meldung/93368

13 Washington Post v. 1.5.2008

14 Stanley, J.; Steinhardt, B.: Even bigger, even weaker. The emerging surveillance society – where are we now? (ACLU-Report), New York 2007, p. 7

15 Beschlüsse der 181. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder am 4. September 2006 in Berlin

war sogar eine Schlussfolgerung des Rates zum Thema im Gespräch – ein Plan, der aber verworfen wurde. Was bleibt, ist die klare Aussage: „Es besteht die Notwendigkeit, alle verfügbaren Ressourcen einzusetzen, um Konvergenz, Interoperabilität und in bestimmten Fällen die gemeinsame Nutzung der von allen Anlagen generierten Mittel zu fördern.“[16]

Der oben erwähnte „Videoatlas“ Baden-Württembergs diente denn auch nicht allein der Kartierung der Kameras, sondern zielte auf die Vernetzung der kartierten Systeme mit der Polizei. Hierzu fehlte allerdings die rechtliche Grundlage, und der Koalitionspartner FDP blockierte bei der Novellierung des Landespolizeigesetzes 2008 eine entsprechende Änderung. Anders hingegen zum Beispiel in Niedersachsen: „Der Zugriff auf Videobilder anderer Überwachungsträger soll im Rahmen einer gemeinsamen Strategie forciert werden. Gerade an Orten verschiedener Infrastrukturen müssen die Übergänge gezielt abgedeckt werden. Dabei geht es nicht darum, die Bürgerinnen und Bürger lückenlos zu beobachten, sondern es geht um die Beobachtung besonders sensibler Bereiche wie Bahnhöfe, Bahnhofsvorplätze, Flughäfen, Bushaltestellen sowie U- und S-Bahnhöfe oder aber Großveranstaltungen“, heißt es in einem Bericht der Landesregierung zur Inneren Sicherheit von 2007.[17] Mit der Ergänzung des Sicherheits- und Ordnungsgesetzes im November des Jahres wurden die Vorschriften für die Videoüberwachung durch die Polizei „den Bedürfnissen der polizeilichen Praxis“ angepasst.[18]

Katalysator der Vernetzung war hierzulande – noch vor Kofferbomben und Verrechtlichung – die Fußball-Weltmeisterschaft von 2006. So hatte Niedersachsen im Vorfeld des Spektakels 370.000 Euro bereitgestellt, um die Verfügbarkeit von „einsatzbezogenen Videoinformationen“ zu verbessern.[19] Inzwischen kann sich die Polizei in Hannover zu mehr als 800 Fremdkameras insbesondere der Verkehrsgesellschaft Üstra aufschalten.[20] Auch die Polizeien in Frankfurt/Main und Berlin nahmen die WM zum Anlass, um sich Direktleitungen zu den Überwa-

16 Ratsdok. 11746/1/08 v. 9.9.2010
17 Niedersächsisches Ministerium für Inneres und Sport; Niedersächsisches Justizministerium: Bericht zur Inneren Sicherheit Niedersachsens 2002-2006, Hannover 2007, S. 11
18 ebd.
19 ebd., S. 211
20 Hannoversche Allgemeine Zeitung v. 22.8.2006

chungsanlagen des städtischen Nahverkehrs einzurichten;[21] und im Rahmen ihrer „Ordnungspartnerschaft“ weihten Deutsche Bahn (DB) und Bundespolizei in Berlin einen gemeinsam genutzten Masterkontrollraum für die 3S-Überwachung von DB-Bahnhöfen ein. 3S steht für „Service, Sicherheit, Sauberkeit“. In den Kontrollraum können seither Bilder der mehr als 20 regionalen 3S-Zentralen übertragen werden, die zusammen etwa 3.000 Kameras an 300 Bahnhöfen betreiben.[22]

Zu Gast im Kontrollraum

Trotz der wachsenden Verdrahtung von landespolizeilichen Einsatzzentralen mit fremden Überwachungssystemen scheint die Kooperation von Bundespolizei und DB typischer für den gegenwärtig vorherrschenden Modus der polizeilichen Nutzung von Fremdanlagen: Seit die DB Mitte der 90er Jahre mit ihrem 3S-Programm Videoüberwachung zu einer zentralen Säule ihres Sicherheitskonzeptes machte, sind in den 3S-Zentralen Plätze für BundespolizistInnen reserviert. Während die 3S-MitarbeiterInnen der DB rund um die Uhr vor den Monitoren sitzen, nutzen BundespolizistInnen ihre Möglichkeiten nur anlassbezogen, z.B. um die An- und Abreise von Fußballfans zu kontrollieren oder Einsätze gegen Taschendiebe zu koordinieren.

Vergleichbares wird auch aus Berlin berichtet, wo die Polizei mittlerweile häufig Gast in der Sicherheitszentrale der Nahverkehrsgesellschaft BVG ist, etwa um gegen Drogenszenen und informellen Fahrkartenhandel in U-Bahnhöfen vorzugehen oder die eigenen Kräfte bei Großlagen zu steuern. Noch fehlen auf Seiten der Polizei, wo aufgrund limitierter Datenleitungen jeweils nur Bilder einer Bahnhofkamera beobachtet werden können, eine der BVG-Sicherheitszentrale vergleichbare Infrastruktur und Arbeitsbedingungen. Ein routinierter Bildwechsel zwischen Kameras ist vermutlich nur in den angezapften Systemen möglich.[23]

Die erheblichen Kosten für Datenleitungen und -übertragung bremsen bislang die umfassende Vernetzung von Fremdanlagen mit der Polizei. Und selbst eine Strategie der Ausweitung der Aufschaltungen in

21 faz.net v. 19.10.2006; Berliner Zeitung v. 1.6.2007

22 Töpfer, E.: Jeden Bahnhof erfassen, in: Telepolis v. 31.8.2005, www.heise.de/tp/r4/artikel/20/20832/1.html; BT-Drs. 17/2750 v. 13.8.2010

23 Besuch der BVG-Sicherheitszentrale am 19.2.2010

Einsatzzentralen scheint den Planern nicht befriedigend. Geträumt wird von einer vollkommenen Flexibilität: „Überwachungskameras sollten so vernetzt sein, so dass ihre Bilder auf jedem anderen Gerät im Netzwerk betrachtet werden können“, visioniert ein Thesenpapier, das die Beratungen der Zukunftsgruppe über das Stockholm-Programm für die Innere Sicherheit der EU informierte.[24]

Solange solche Ideen jedoch Zukunftsmusik bleiben, dürfte der vorübergehende Mitgebrauch von Kontrollräumen nicht-polizeilicher Überwachungsnetze die bevorzugte Variante für ihre Echtzeitnutzung durch die Polizei sein.

Konflikte und Gefahren

Der Boom der nicht-polizeilichen Videoüberwachung wirkt also mittelbar als Machtverstärker für die Polizei – als Hilfe bei der Strafermittlung, aber eben auch bei der Einsatzplanung und -leitung. Die Vorteile liegen auf der Hand: Anschaffung, Betrieb und Wartung der Anlagen ist Sache der Betreiber, während die Polizei relativ flexibel auf das Instrument zugreifen kann. Doch insbesondere die Kosten der Überwachung bergen Zündstoff: So beklagte sich die Gewerkschaft der Polizei (GdP) Anfang 2011 darüber, dass die Banken der Polizei die Überlassung von Fotos auf Überwachungskameras in Rechnung stellen und brachte eine Änderung des Zeugenentschädigungsgesetzes ins Gespräch.[25] Auch als Bundesinnenminister Otto Schily und DB-Chef Hartmut Mehdorn 2005 die Sicherheitszentrale in Berlin besuchten, wurde deutlich, dass die Aufteilung der Kosten für die Videoüberwachung zwischen den „Ordnungspartnern“ umstritten ist. Im Gegensatz dazu beschäftigt die Berliner BVG eigens vier Mitarbeiter, um die wachsende Zahl polizeilicher Anfragen nach Überwachungsbildern systematisch, aber kostenlos zu bearbeiten.

Die Frage, welche Priorität die polizeiliche Nutzung der Videoüberwachungsanlage hat, stellt sich allerdings nicht nur bei den Kosten. Bei der Errichtung von Anlagen des Nahverkehrs stehen beispielsweise eher

24 Future Group (Portugal): Public security, privacy and technology in Europe. Moving forward. Concept paper on the European strategy to transform public security organizations in a connected world, www.statewatch.org/news/2008/jul/eu-futures-dec-sec-privacy-2007.pdf

25 GdP Nordrhein-Westfalen: Pressemitteilung v. 11.1.2011

Betriebsabläufe im Vordergrund, so dass nicht immer polizeilich für relevant gehaltene Örtlichkeiten im Blick der Kameras sind. Strittig ist auch, ob die Polizei bei Echtzeitaufschaltungen die Fernbedienung der Systeme übernehmen darf und ob sie bei Besuchen in Kontrollräumen nicht über Gebühr Ressourcen beansprucht, die von den eigentlichen Betreibern benötigt werden. Die Polizei Regensburg, die für das bayerische Pilotprojekt zur Videoüberwachung öffentlicher Straßen und Plätze 2000/2001 die existierende Anlage der lokalen Verkehrsbetriebe nutzte, bilanzierte: „Die Polizei ist nur ‚Gast' auf der Anlage … Es gebietet schon die Höflichkeit, sie nicht ständig für polizeiliche Belange zu nutzen. Für polizeiliche Zwecke sind deshalb polizeieigene Anlagen unabdingbar."[26]

Wie auch immer solche Interessenkonflikte letztlich entschieden werden, fest steht, dass sich mit der wachsenden Vernetzung der Überwachung die informationelle Selbstbestimmung verflüssigt, weil es – selbst bei Existenz datenschutzkonformer Partnerschaftsvereinbarungen und Techniken – für die Betroffenen immer undurchschaubarer wird, wann, wer und warum überwacht. Wer dennoch meint, dass die Grundrechtsbeschneidung angesichts terroristischer Bedrohung gerechtfertigt sei, ignoriert die jeder Überwachung inhärente Aufweichung der Zweckbestimmung: In Wolfsburg schaltete sich die Polizei noch während der Verhandlungen um die Novellierung des niedersächsischen Polizeigesetzes im Oktober 2007 auf Kameras der Wolfsburger Dienstleistungs- und Meldezentrale (WDZ) auf, die in Bahnhofsnähe installiert sind. Hatte die Stadtwerke-Tochter WDZ, die zu dieser Zeit mit Stadtverwaltung, einem großen Einkaufszentrum, Verkehrsgesellschaft, Stadtmarketing, Landes- und Bundespolizei in einem Projekt „Sichere Innenstadt" organisiert war, zuvor noch die Polizei über „Auffälligkeiten" informiert, nahm fortan die Polizei selbst die „auffällige" Jugend ins Visier.[27] In einer Antwort der Landesregierung auf die Frage nach dem Stand der polizeilichen Videoüberwachung wurde Wolfsburg mit keiner Silbe erwähnt.[28]

26 Polizeidirektion Regensburg: Pressemeldung v. 31.8.2001

27 Braunschweiger Zeitung v. 17.9. und 20.10.2007; www.wolfsburg.de/irj/portal/anonymous?NavigationTarget=navurl://43712da60a7e99a3db4933026dd05784

28 Niedersächsischer Landtag: Drs. 15/4376 v. 18.12.2007

In einer durchsichtigen Welt

Die „Open Source Intelligence"-Industrie

von Ben Hayes

Das Geschäft mit Informationen aus „offenen Quellen" ist im vergangenen Jahrzehnt schnell gewachsen. Private Unternehmen, die keinerlei datenschutzrechtlichen Beschränkungen unterliegen, sammeln Daten in großem Stil – zur Freude von Sicherheitsinstitutionen der EU und ihrer Mitgliedstaaten.

Das US-Militär definiert „Open Source Intelligence" (OSINT) als die Gewinnung „relevanter Information aus der systematischen Sammlung, Aufbereitung und Analyse öffentlich zugänglicher Daten für nachrichtendienstliche Zwecke."[1] Unter einer „offenen Quelle" sei „jede Person oder Gruppe" zu verstehen, „die Informationen ohne Anspruch auf Schutz der Privatsphäre liefert". Öffentlich zugängliche Information umfasse alles, „was auf Nachfrage für die breite Öffentlichkeit verfügbar ist, legal von irgendeinem Beobachter gesehen oder gehört oder an einer öffentlichen Versammlung kundgetan wurde." „Open Source Intelligence" wird also durch das definiert, was sie nicht ist: „vertraulich", „privat" oder sonst „für eine bestimmte Person, Gruppe oder Organisation gedacht". In der Praxis wird diese Unterscheidung jedoch dadurch unterlaufen, das weblogs, chat-rooms und „soziale Netzwerke" als „öffentliche Diskussionsforen" kategorisiert werden.

Vor der informationstechnischen Revolution waren OSINT-Beschaffer in erster Linie mit der linken Presse und den Auslandsnachrichten beschäftigt. Sie sogen ihre Erkenntnisse aus der Zeitungslektüre, dem Abschöpfen von Geschäftsleuten und Touristen und der Zusammenarbeit mit Akademikern. OSINT-Spezialisten beklagten denn auch, dass die großen Zeitungen als Ergebnis ihres finanziellen Niedergangs immer

1 so das „field manual" v. Dezember 2006, www.fas.org/irp/doddir/army/fmi2-22-9.pdf

weniger AuslandskorrespondentInnen haben. Dieser Verlust ist jedoch durch die Fülle von Informationen aus dem World Wide Web längst ausgeglichen. OSINT verwandelte sich in eine Schreibtischtätigkeit, für die es nichts weiter braucht als einen Internet-Anschluss, einen Web-Browser und ein Telefon. „Die rasche Ausbreitung der (Online-)Medien und die schnelle Greifbarkeit von Forschungspapieren haben zur Folge, dass ein Großteil der Informationsbedürfnisse eines Staates heute durch eine umfassende Beobachtung offener Quellen gedeckt werden kann", kommentiert die RAND Corporation.[2] Von der CIA heißt es sogar, dass „80 Prozent ihrer Erkenntnisse von Google stammen".[3]

Vom Standpunkt der Sicherheitsbehörden aus erscheint das völlig selbstverständlich. Aus einer bürgerrechtlichen Perspektive ist die Aneignung von persönlicher Information für Zwecke der „Sicherheit" jedoch problematisch. Die Information, dass sich jemand öffentlich gegen den Krieg ausgesprochen hat, an einer Demonstration teilnahm oder einen Freund hat, der bekanntermaßen als „Sicherheitsrisiko" gilt, kann irgendwann zum Nachteil des Betreffenden verwendet werden. Auch bei der Informationssammlung aus offenen Quellen stellt sich die Frage, wer wie und warum hier beobachtet – oder anders gesagt: die Frage der demokratischen Legitimität.

OSINT und die Polizei

In einer Rede vor der „Eurointel"-Konferenz 1999 beschrieb ein Sprecher der OSINT-Einheit von New Scotland Yard (NSY) offene Quellen als „alle Informationen, die für uns entweder frei oder als zahlende Kunden verfügbar sind".[4] Dabei gehe es sowohl um strategische als auch um taktische Zwecke. Strategische Informationen würden bei längeren Projekten zum Beispiel zu organisierter Kriminalität, Geldwäsche oder Drogen gesammelt. „Taktische" würden dagegen möglichst schnell gebraucht: „Wo wohnt diese Person und wer sind ihre Partner?", „Ich habe

2 Rathmell, A.: The Privatisation of Intelligence, in: NATO Open Source Intelligence Reader, February 2002, www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf

3 Best, C. (Gem. Forschungsstelle der EU-Kommission): Open Source Intelligence, http://media.eurekalert.org/aaasnewsroom/2008/FIL_000000000010/071119_MMDSS-chapter_CB.pdf

4 Edwards, S.: SO11 Open Source Unit, Eurointel '99, www.oss.net/dynamaster/file_archive/040319/c7f74b0455dda7c58e7dd31d909c9d31/OSS1999-E1-05.pdf

den Vornamen einer Frau und weiß, dass sie in Manchester lebt". „Wann findet die nächste anarchistische Demo zum Parlament statt?" Glaubt man dem NSY, dann können viele solcher „taktischer" Fragen „überraschend einfach mit einigen sehr simplen Tools" beantwortet werden. „Die Beamten, die mit wenig mehr als einem Vornamen zu uns kommen, sind erstaunt, wenn wir ihnen Listen mit Familiennamen, Adressen, Firmen, Angaben über deren Besitzer und Beteiligte sowie finanzielle Details zurückgeben."

Die OSINT-Spezialisten der Polizei benutzen Personensuchmaschinen, die auf „Adressverzeichnisse, öffentliche Register, elektronische Telefonbücher, E-Mail- und Homepage-Finder etc." zurückgreifen können. Bezeichnenderweise erfolgen alle Online-Transaktionen von Scotland Yard verdeckt: „Wir gebrauchen dabei Scheinfirmen und Pseudonyme genauso wie bei jeder anderen verdeckten Operation." Man vermeide so, „dass jemand sieht, dass die Polizei etwas gesucht hat." Ein solches Vorgehen hinter dem Rücken der Betroffenen wirft Fragen der Kontrolle und Kontrollierbarkeit auf. Dem Sprecher des Yard erschien Datenschutz als eine unsinnige „Barriere" gegen seine Arbeit. „Schwierigkeiten kamen und kommen auch weiterhin vom Datenschutzbeauftragten ... Regelmäßig führen wir harte Auseinandersetzungen um die legitime Sammlung von Daten, die ein so wertvolles Instrument ist im Kampf gegen raffinierte und organisierte Kriminelle ..."

Privatisierung der Überwachung

Im Jahre 2002 plädierte Andrew Rathmell vom europäischen Zweig der RAND Corporation für eine Privatisierung von Intelligence-Arbeit. Es spreche kaum etwas dafür, dass diese Arbeit „von eigenen Experten besser erledigt werden könnte als von etablierten privaten Forschungsinstituten oder Firmen."[5] So wie in anderen Bereichen von Sicherheit und Verteidigung wurde auch hier argumentiert, dass eine Auslagerung den „Druck auf die Haushalte mindern" würde. Offene Quellen seien heute nicht nur besser verfügbar, vielmehr würden auch die „Grenzen zwischen offenen und verdeckten Quellen immer mehr verschwimmen." Um von diesen Segnungen der informationstechnischen Revolutionen größtmöglichen Nutzen zu ziehen, empfahl die RAND eine „engere

5 Rathmell a.a.O. (Fn. 2)

europäische Zusammenarbeit, sowohl zwischen den Regierungen als auch mit dem privaten Sektor."

Die OSINT-Industrie ist im vergangenen Jahrzehnt massiv gewachsen. Dieser Trend zeigte sich zunächst in den USA. Wie die American Civil Liberties Union (ACLU) in einer Studie von 2004 erklärte, sind „Unternehmen wie Acxiom, Choicepoint, LexisNexis und viele andere für den Durchschnittsbürger weitgehend unsichtbar. Sie stellen aber eine Multi-Milliarden-Industrie dar."[6] Datenschutzbestimmungen mögen zwar die staatliche Informationssammlung über unverdächtige BürgerInnen begrenzen, aber, so die ACLU, „Polizei- und Strafverfolgungsbehörden umgehen diese Beschränkungen in wachsendem Maße, indem sie schlicht und einfach Informationen kaufen, die von ‚data aggregators' gesammelt wurden."

Zu den europäischen Unternehmen dieser Art gehört World-Check. Die Firma bietet ihren Kunden „risk intelligence" über „Organisationen oder Leute, mit denen sie Geschäfte machen."[7] An World-Check wendet man sich, wenn man wissen will, ob ein möglicher Geschäftspartner auf einer der vielen Terroristen-Listen auftaucht, die Großbritannien, die EU, die USA, die Vereinten Nationen und andere seit 2001 zusammengestellt haben. Nach Angaben auf seiner Website (www.world-check.com) zählt das Unternehmen „über 4.500 Organisationen" zu seinem Kundenstamm. Seine Forschungsabteilung stelle zielgerichtet Profile über Personen und Körperschaften zusammen, bei denen eine genauere Überprüfung angesagt sei. Seine „hochstrukturierte Datenbank" stütze sich „auf Tausende zuverlässiger öffentlicher Quellen". Zu den Diensten, die World-Check anbietet, gehört auch ein „Pass-Check", bei dem die „Authentizität der maschinenlesbaren Zone von Pässen aus über 180 Staaten" überprüft wird.

Ein Blick zurück in die 80er Jahre macht die Tragweite dieses Prozesses deutlich: In Großbritannien führte damals die Economic League ihre eigenen Schwarzen Listen. Diese rechtsgerichtete Agentur ermöglichte Arbeitgebern, die politische Gesinnung von Angestellten oder Bewerbern zu überprüfen. Die League verfügte nachweislich über beste Beziehungen zu den Sicherheitsbehörden. Sie generierte einen Jahresumsatz von über einer Million Pfund, mehr als 2.000 Unternehmen

6 ACLU: The Surveillance-Industrial Complex, New York 2004, www.aclu.org/surveillance
7 www.world-check.com/

waren auf ihre Dienste abonniert. Zu den mindestens 30.000 Personen, über die sie Unterlagen gesammelt hatte, gehörten politische und gewerkschaftliche Aktivisten, Abgeordnete der Labour Party aber auch Leute, die in Leserbriefen gegen die Politik der Regierung protestiert hatten. Bei alledem betonte die League, Unschuldige hätten nichts zu befürchten. Man sammle nur Informationen über „bekannte Mitglieder extremistischer Organisationen". Nach kritischen Medienberichten und einer öffentlichen Kampagne musste sich die League 1993 auflösen. (Ihre Direktoren gründeten im folgenden Jahr mit denselben Dienstleistungen und denselben Unterlagen eine neue Firma.[8]) An die Stelle dieser Unternehmen, die Anfang der 90er Jahre als illegitim galten, ist heute eine ganze Branche getreten.

Infosphere AB mit Sitz in Schweden ist eine solche „kommerzielle Intelligence- und Strategieberatungsfirma": „Weltweit verfügt kein Unternehmen und keine Organisation über mehr Erfahrung in der Nutzung und Entwicklung von OSINT-Methoden", erklärt das Unternehmen auf seiner Homepage.[9] „Viele Nationen und Konzerne folgen unseren Empfehlungen und nutzen regelmäßig unsere Unterstützung." Die Profiling-Dienste von Infosphere bieten „fakten-basierte Hintergrund-Checks", Medienanalysen und „Mapping" der Beziehungsgeflechte von Personen, Firmen und Organisationen in allen „Winkeln der Welt". Infosphere brüstet sich damit, an diversen hochmodernen Intelligence-Diensten beteiligt zu sein und „Zugang zu elektronischen und menschlichen Quellen weltweit" zu haben.

Sandstone AB („Because You Need To Know") mit Sitz in Luxemburg bietet „handlungsrelevante intelligence" auf Anfrage.[10] Infosphere and Sandstone organisieren gemeinsam „Naked Intelligence" („Erkenntnisse sammeln in einer durchsichtigen Welt"), eine OSINT-Konferenz, bei der „Experten und Macher … unter einem Dach zusammenkommen".[11] 2009 fand die erste Konferenz in Luxemburg, im Oktober 2010 die zweite in Washington statt.[12]

8 s. Statewatch Bulletin v. Juli 1993 und Juni 1994
9 www.infosphere.se
10 www.sandstone.lu
11 Pressemitteilung v. 5.7.2009, www.prlog.org/10274607-unique-open-source-intelligence-event-in-the-heart-of-europe.html
12 www.nakedintelligence.org/extra/pod

OSINT – Theorie und Praxis

Die Informations- und Kommunikationstechnologie eröffnet neue Potenziale für die „open source intelligence". Wissenschaftler und Computer-Programmierer arbeiten an der Automatisierung der Datensammlung und -analyse. So hat beispielsweise die Universität von Süd-Dänemark in Odense ein Institut gegründet, das die angewandte Mathematik für die Terrorismusbekämpfung nutzbar machen soll. Das „Counterterrorism Research Lab" (CTR Lab) betreibt Forschung und Entwicklungsarbeit zu „fortgeschrittenen mathematischen Modellen, innovativen Techniken und Algorithmen sowie software tools." Letztere sollen die Analysten in allen Phasen der Suche und Auswertung Terrorismus-bezogener Informationen unterstützen – von der Sammlung von Daten und ihrer Filterung bis hin zur Visualisierung von Ergebnissen.[13] Die Produkte des Labors heißen „iMiner" (eine „Terrorimus-Wissensdatenbank mit Analyse-tools"), „CrimeFighter" (eine „toolbox für die Terrorismusbekämpfung") und „EwaS" (ein „Frühwarnsystem und Portal für Terrorismus-Ermittlungen"). Das CTR Lab organisierte darüber hinaus internationale Konferenzen zu Themen wie „Terrorismusbekämpfung und OSINT", „Fortschritte in der Analyse und im Mining von Sozialen Netzwerken" und „OSINT und Web Mining".

Wie die Gemeinsame Forschungsstelle der EU-Kommission ausführt, hat die enorme Zunahme von Blogs „einen neuen Forschungszweig namens ‚opinion mining' entstehen lassen. Blogs sind besonders einfach zu beobachten, weil die meisten als RSS-Feeds verfügbar sind. Blog-Aggregatoren wie Technorati und Blogger erlauben den Nutzern in einer Vielzahl von Blogs nach relevanten Einträgen zu suchen. Für eine aktive Beobachtung von Blogs kommen Techniken zur Extrahierung von Informationen zum Einsatz, um Blog-Einträge nach den darin erwähnten Leuten, der Einstellung, dem angeschlagenen Ton oder ähnlichem zu rubrizieren..."[14] Regierungen gebrauchen diese Techniken, um sich einen Überblick über die aktuelle öffentliche Meinung zu verschaffen. Dieselben Methoden können aber auch genutzt werden, um Gruppen oder Personen zu identifizieren, die „radikale" oder „extremistische" Meinungen vertreten.

13 www.ctrlab.dk

14 s. Best a.a.O. (Fn. 3)

In den USA bietet das Mercyhurst College Studien in „Intelligence Analyse“ an und verspricht den Absolventen unter anderem Arbeitsstellen bei der CIA oder der Armee.[15] Im Juli 2010 organisierte Mercyhurst ein „Global Intelligence Forum“ in Dungarvan (Irland) mit Podiumsdiskussionen über Medizin, Recht, Finanzen, Technologie, Journalismus, aber auch Nationale Sicherheit, Verbrechensbekämpfung und kommerzielle Intelligence.[16] Am Londoner King's College kann man ein OSINT-Diplom erwerben. Der Studiengang deckt „sowohl theoretische als auch praktische Aspekte der OSINT, einschließlich Datensammlungs- und -analysemethoden“ ab.[17] Studierenden, die dieses Modul wählen, empfiehlt das College, sich für eine Nachwuchsstelle im „Institut für Schutz und Sicherheit des Bürgers“ (IPSC), einer der Einrichtungen der Gemeinsamen Forschungsstelle der EU-Kommission, zu bewerben.

Auf dem privaten Sektor bietet auch Jane's Strategic Advisory Services (die Consulting-Abteilung des Rüstungsfirma Jane's) Kurse und Seminare zum Thema OSINT.[18] Zu den Tutoren gehört unter anderem Nico Prucha, der auf der Homepage als Experte angepriesen wird – für „dschihadistische Bewegungen und Ideologien“ im Internet, für „Muster von Online-Rekrutierung und Radikalisierung“, für die „Nutzung von Blogs und sozialen Netzwerken für die intelligence-Sammlung“, für die Suche nach und die Bewertung von Informationen aus Foren und im „Deep Web“, für Schlüsselwort- und Stimmungsanalyse.

Verschwimmende Grenzen

Mit der informationstechnischen Revolution, so stellt die RAND Corporation fest „verschwimmen die Grenzen zwischen offenen und geheimen Quellen“. Einerseits können OSINT-Methoden für das „Mining“ öffentlich verfügbarer (privater) Datenbestände, mit anderen Worten: für eine faktische Überwachung bestimmter Gruppen oder Einzelpersonen genutzt werden. Andererseits hat die Community der Wissenschaftler, Programmierer und Hacker eine ganze Palette so genannter „spy-ware“-Anwendungen, die den Benutzern verdeckte Überwachungsmöglichkei-

15 www.mercyhurst.edu
16 Global Intelligence Forum, Dungarvan Conference, 11-13.7.2010, www.regonline.com/builder/site/Default.aspx?eventid=826351
17 www.kcl.ac.uk/schools/sspp/ws/grad/programmes/options/opensource
18 www.janes.com/consulting/OSINT.html

ten eröffnen, zum Beispiel „phishing"-tools, mit denen Benutzernamen, Passwörter oder PIN-Codes ausspioniert werden, oder „Key-loggers", die die verdeckte Aufzeichnung der Aktivitäten auf einem Computer ermöglichen. Mittlerweile ist die Überwachung von Mobiltelefonen „billig und einfach und wird immer einfacher".[19] Dass die EU die Nutzung von spyware-, Hacker- und Abhörtechniken ohne Genehmigung verboten hat, konnte die Entwicklung dieser Techniken nicht stoppen. Sie stoßen bezeichnenderweise bei den Polizeien diverser europäischer Staaten auf großes Interesse, weil sie das Eindringen in fremde Computer ohne das Wissen der Betroffenen – verharmlosend: die Online-Durchsuchung – ermöglichen. Sowohl Polizeien als auch private Ermittlungsdienste haben in den vergangen Jahren die Fähigkeiten – und zum Teil auch die rechtlichen Voraussetzungen – für Methoden der Überwachung erworben, die früher nur den Geheimdiensten zugänglich waren.

Offene Quellen für die Europäische Union

Das EUROSINT-Forum ist eine belgische gemeinnützige Vereinigung, die sich die Förderung der europäischen Kooperation und die Nutzung von Open Source Intelligence zur „Prävention von Risiken und Gefahren für Frieden und Sicherheit" zum Ziel gesetzt hat.[20] 2006 mit der Hilfe der Generaldirektion „Freiheit, Sicherheit und Recht" (heute: Generaldirektion Innenpolitik) der EU-Kommission gegründet, will der Verein eine „Europäische Intelligence-Ökologie" und ein positives Bild der Open Source Intelligence in der EU schaffen. Die Nutzung von OSINT in Intelligence- und Sicherheitsbereichen soll angeregt und gefördert werden. Der Verein will explizit auch „Akteuren des privaten Sektors, die sich mit Sicherheits- und Intelligence-Fragen beschäftigen, eine Stimme geben" und „Partnerschaften zwischen privaten Firmen und/oder öffentlichen Organismen" sowie die „Bildung europäischer Konsortien, die neue Projekte hervorbringen," fördern. Zu den Mitgliedern des EUROSINT-Forums gehören EU-Institutionen, Verteidigungs-, Sicherheits- und geheimdienstliche Stellen der Mitgliedstaaten, private Intelligence-Anbieter, Technologie-Entwickler, Universitäten, think-tanks und For-

19 Hulton, D.: Intercepting Mobile Phone/GSM Traffic, Black Hat Briefings, 2008, www.blackhat.com/presentations/bh-europe-08/Steve-DHulton/Presentation/bh-eu-08-steve-dhulton.pdf

20 www.eurosint.eu/publications

schungsinstitute. Unter den Firmen, die den Jahresbeitrag von 5.000 Euro entrichten, finden sich Jane's, LexisNexis, Factiva, Oxford Analytica – alle aus Großbritannien – die Compagnie Européenne d'Intelligence Stratégique (CEIS-Europe, Frankreichs größte Firma im Bereich der Strategischen Intelligence) sowie Columba Global Systems aus Irland.

„OSINT gibt EU-Institutionen eine perfekte Plattform für eine völlig legitime Intelligence-Kooperation", heißt es in einer Power-Point-Präsentation von EUROSINT.[21] Mit dieser Vorstellung steht das Forum offensichtlich nicht allein. Auch das gemeinsame Lagezentrum SITCEN, die geheimdienstliche Komponente des EU-Ratssekretariats, stellte die Open Source Intelligence an den Anfang seiner Arbeit.[22] SITCEN, die EU-Grenzschutzagentur FRONTEX, die Gemeinsame Forschungsstelle sowie drei Generaldirektionen der Kommission beteiligen sich an EUROSINT. Axel Dyèvre, Gründungsmitglied des Forums und Direktor von CEIS-Europe, erklärte schon 2008, Institutionen der EU und vieler Mitgliedstaaten seien geradezu vernarrt in die Open Source Intelligence.[23]

Kein Wunder also, dass EUROSINT und seine Mitgliedsorganisationen bei seinen Tätigkeiten auf die Unterstützung der EU zählen können. 2008 wurde ein Projekt des Forums über „Open Source Intelligence in der Bekämpfung Organiserter Kriminalität" aus dem Mehrjahresprogramm zu Verbrechensbekämpfung und Prävention (ISEC) der Generaldirektion Recht, Freiheit, Sicherheit der Kommission gefördert. EUROSINT gehört auch zu den 18 Mitgliedern des VIRTUOSO-Konsortiums, das gerade 8 Millionen Euro aus dem Sicherheitsforschungsprogramm der EU (ESRP) erhielt. VIRTUOSO verspricht eine „paneuropäische Plattform für die Sammlung, Analyse und Verbreitung von Open Source Intelligence" mit „Echzeit-Aggregation" von Informationen und Tools für das „Mining" von Texten, die „Frühwarnung" und die „Entscheidungsunterstützung". Zu dem Konsortium gehören weiter CIES und Colomba, die Rüstungsgiganten EADS and Thales sowie die niederländische Militärforschungsagentur TNO. Die Europäische Vertei-

21 www.eurosint.eu/files/Eurosint%20Presentation.pdf

22 Van Buren, J.: Secret Truth. The EU Joint Situation Centre, Amsterdam 2009, www.statewatch.org/news/2009/aug/SitCen2009.pdf

23 Dyèvre, A.: Intelligence cooperation: The OSINT option, Europolitics.info v. 28.10.2008, www.europolitics.info/dossiers/defence-security/intelligence-cooperation-the-osint-option-art151325-52.html

digungsagentur bezahlte EUROSINT für Studien über „OSINT-Suchmaschinen“ und die Entwicklung von Tools für „Intelligence-Analysten“ sowie für gemeinsame OSINT-Fortbildungskurse, darunter ein 30-Wochen-Kurs im Jahre 2009.[24]

Die Gemeinsame Forschungsstelle der Kommission hat mittlerweile ihre eigene „OSINT-Suite“ aufgebaut. Sie benutzt dabei ein „Tool für Web-Mining und die Extraktion von Informationen, das nunmehr bei mehreren nationalen Polizeibehörden im Versuchsstadium eingesetzt wird.“[25] Diese Software „lädt Textinhalte von überwachten Websites herunter und wendet Techniken zur Extraktion von Informationen an. Diese Tools helfen den Analysten dabei, strukturierte Daten aus großen Mengen von Dokumenten herauszufiltern.“

Viele OSINT-Anbieter setzen auf derartige Software, um durch die Analyse von Informationen aus dem Netz potentiell gefährliche Leute zu identifizieren. Derartige Techniken werden mittlerweile unter dem Begriff „counter-radicalisation“ gehandelt. SAFIRE ist ein weiteres Projekt, das mit 3 Millionen Euro aus dem EU-Sicherheitsforschungsprogramm gefördert wird. Es verspricht eine „wissenschaftliche Herangehensweise an die Bekämpfung des radikalen Extremismus“. Ziel ist, „durch ein tieferes Verständnis des Radikalisierungsprozesses Prinzipien zu entwickeln, mit denen die Interventionen zur Prävention, zum Stoppen und zur Umkehr der Radikalisierung verbessert werden können.“ Das SAFIRE-Konsortium wird angeführt von TNO, der bereits erwähnten niederländischen Militärforschungsagentur, beteiligt sind ferner die RAND Corporation, die israelische International Counter-Terrorism Academy und CEIS. „Radikalisierung im Internet“ ist einer der Gesichtspunkte, mit denen sich SAFIRE befassen soll.[26] Das Thema „Radikalisierung und Rekrutierung“ war seit 2005 ständiger Bestandteil der Anti-Terror-Aktionspläne der EU. Mit dem Projekt eines „standardisierten, multidimensionalen, semistrukturierten Instruments“ zur Erfassung von Daten über „Radikalisierungsprozesse“ hat der Rat das zu überwachende politische Spektrum massiv ausgedehnt. „Radikale Botschaften“ sollen re-

24 www.eda.europa.eu/genericitem.aspx?area=organisation&id=308

25 s. Best a.a.O. (Fn. 3)

26 http://neoconopticon.wordpress.com/2010/06/16/tno-rand-and-israeli-counter-terrorism-academy-awarded-e3-million-ec-radicalisation-and-recruitment-contract

gistriert werden – egal ob sie „extrem rechts/links, islamistisch, nationalistisch“ sind oder von „Globalisierungsgegnern“ kommen.[27]

Schlussfolgerungen

Professor John Naughton schrieb kürzlich im „Guardian“:

> „Das Internet ist nahe daran, eine perfekte Überwachungsmaschine zu sein. Alles was man im Netz tut, wird geloggt – jede gesendete E-Mail, jede besuchte Website, jedes Herunterladen einer Datei, jede Suche wird irgendwo aufgezeichnet und gespeichert, entweder auf den Rechnern des Providers oder jenen der Wolke, zu denen man Zugang hat. Für eine totalitäre Regierung, die über das Verhalten, die sozialen Aktivitäten und das Denken ihrer Untertanen Bescheid wissen will, ist das Internet ein geradezu perfektes Instrument.“[28]

Die gegenwärtige Bedrohung für die Bürgerrechte geht jedoch weder vom Internet noch von totalitären Regierungen aus, sondern von einer neo-McCarthyistischen Hexenjagd auf „Terroristen“ und „Radikale“ sowie einer privaten Sicherheitsindustrie, die sich darum bemüht, das „perfekte“ Instrument zur Überwachung der neuen Feinde zu entwickeln. Trotz aller Beunruhigung über die Datenschutzpolitik von Unternehmen wie Facebook,[29] bleibt festzuhalten, dass sie für die Selbstentblößung ihrer NutzerInnen genauso wenig verantwortlich sind wie ein Reisebüro für den Tourismus. Selbstverständlich muss Facebook für einen maximalen Schutz der Privatsphäre seiner NutzerInnen sorgen. Wer um Freiheit und Demokratie besorgt ist, muss aber das ganze Bild zur Kenntnis nehmen und die Frage stellen, wer da wie und warum überwacht.

27 s. Bunyan, T.: Intensive surveillance of „violent radicalisation“ extended to embrace suspected radicals from across the political spectrum, London Juni 2010 www.statewatch.org/analyses/no-98-eu-surveillance-of-radicals.pdf

28 Observer v. 20.6.2010, www.guardian.co.uk/technology/2010/jun/20/internet-everything-need-to-know

29 ACLU: Blogeintrag v. 16.6.2010, www.aclunc.org/issues/technology/blog/privacy_groups_to_facebook_theres_more_to_do.shtml

Netzwerke der Information

Wirtschaft und Staat als „Sicherheitspartner“?

von Randalf Neubert

Mehr Kooperation, mehr Informationsaustausch, eine echte „Public Private Partnership“ wolle man erreichen. Was wirklich in den im letzten Jahrzehnt entstandenen Netzwerken von staatlichen Sicherheitsbehörden und privaten Unternehmen passiert, ist für die Öffentlichkeit nicht durchschaubar.

„Das Bundeskriminalamt (BKA) baut das Netzwerk im Kampf gegen die Kriminalität aus.“ Mit diesen Worten beginnt eine Presseerklärung des Amtes vom 20. April 2006. Zu vermelden war eine „Tagung zur Zusammenarbeit von Sicherheitsbehörden des Bundes mit der Wirtschaft“, die das BKA zusammen mit der „Arbeitsgemeinschaft für Sicherheit der Wirtschaft“ veranstaltete. BKA-Präsident Jörg Ziercke referierte über die innere Sicherheit, weitere Vorträge beschäftigten sich mit Wirtschaftskriminalität, Geldwäsche und Korruption. Die Tagung, an der etwa siebzig Sicherheitsverantwortliche von Unternehmen teilnahmen, lief hinter verschlossenen Türen ab. Es war die erste der seither jährlich stattfindenden „Wirtschaftskonferenzen“ des BKA.

Von einer ganz anderen Qualität ist das Netz, das das BKA einen Monat vorher zu weben begonnen hatte. Am 23. März 2006 hatten Ziercke sowie Mitarbeiter der Abteilung Internationale Koordinierung (IK) mit den Sicherheitschefs von Großunternehmen getagt. Vertreter von 18 Konzernen, darunter BASF, Siemens, Daimler, die Deutsche Bank, die Deutsche Bahn und die Lufthansa, waren zu diesem ersten Treffen erschienen. Zwei Jahre später waren 42 Unternehmen an dieser „Global Player Initiative“ beteiligt.[1] Damit war die Obergrenze, die sich das BKA zu Anfang gesetzt hatte, erreicht. Ein beschränkter Kreis, so Ziercke Anfang 2008 in einem Interview, sei „Garant für Effektivität“ und Voraussetzung für

1 Zeit v. 20.4.2006; Financial Times Deutschland v. 16.8.2008

„Maßnahmen der Vertrauensbildung, Prozesse der Entscheidungsfindung und auch die Weitergabe von sensiblen Informationen".[2]

Die Initiative, so Ziercke weiter, ziele auf „weltweit aufgestellte deutsche Großunternehmen: Unternehmen, die an internationalen Brennpunkten starke Interessen haben und von daher auch Wissensträger sind sowie einen eigenen Security-Bereich mit Zuständigkeit für In- und Ausland besitzen." Solche Firmen hätten einerseits wegen ihrer internationalen Präsenz „einen intensiven Beratungsaufwand". Zum anderen – so die Erwartung des Amtes – „sollte sich im Umkehrschluss aus der internationalen Positionierung der Unternehmen zumindest die Möglichkeit ergeben, dem BKA strategisch relevante Informationen liefern zu können."

Eine konkrete Festlegung auf spezifische Delikte oder Ermittlungsbereiche sucht man in den wenigen Verlautbarungen und Meldungen zur Initiative vergebens. Von Wirtschaftskriminalität, Korruption, Geldwäsche und Finanzermittlungen ist die Rede, vom Schutz der MitarbeiterInnen deutscher Firmen im Ausland vor Entführungen, aber auch von der angeblichen Notwendigkeit, dem „Netzwerk des Terrorismus" und dem der „organisierten Kriminalität" eines der „Informationen" entgegenzusetzen.[3] Zudem erwartete sich das BKA eine Kooperation bei der Entwicklung neuer Sicherheitstechniken.

Die fehlende thematische Festlegung zeigt vor allem eines: dass es den Sicherheitsabteilungen der Konzerne darum geht, vom BKA als Partner auf „Augenhöhe" anerkannt zu werden, während das BKA seinerseits daran interessiert ist, das Wissen dieser ausgedehnten Apparate für die polizeiliche Arbeit nutzbar zu machen. Allerdings, so Ziercke, wolle das BKA „die Unternehmen in keiner Weise dazu anhalten, gezielt Informationen zu sammeln" oder zu seinem „Handlanger" zu werden.[4] Dem BKA schien es dabei insbesondere um die Ausdehnung seines internationalen Informationsnetzes zu gehen, das sich bisher vor allem auf seine 65 rund um den Globus stationierten (ständigen) VerbindungsbeamtInnen stützt.

Dass es sich bei der Global Player Initiative um eine gezielte Form des Informationsaustausches handelt, die über die halbjährlichen Treffen der TeilnehmerInnen weit hinaus geht, zeigt sich an den Formen der Kommunikation: Sowohl das BKA als auch die jeweiligen Unternehmen richte-

2 Glitza, H.: Informationsaustausch zwischen Behörden und Wirtschaft. Interview mit J. Ziercke (BKA), in: W&S 2008, H. 1-2, S. 15-17, www.sicherheit.info/SI/cms.nsf/si.ArticlesByDocID/1100809?Open

3 Ziercke zit. n. Zeit v. 20.4.2006

4 ebd.

ten „single points of contact“, SPOCs, ein, „eine zentrale Anlaufstelle mit koordinierender Funktion … über die zentral die Informationsflüsse ein- und ausgehen sollen.“ Der SPOC des BKA bei der Abteilung IK sei „ein Servicedesk, das … Weiterverbindungsschleifen und Bin-nicht-zuständig-Marathons vermeiden soll … Von dieser Stelle aus werden die Nachfragen nach einer ersten Bewertung direkt beantwortet oder, falls erforderlich, gezielt an die zuständigen Stellen im BKA gegeben. Bei Bedarf werden im Rahmen der rechtlichen Möglichkeiten nationale sowie internationale Verbindungen genutzt, um eine möglichst schnelle Beantwortung zu gewährleisten.“ Umgekehrt könnten Anfragen des BKA an die Unternehmen „entweder wie bisher über bereits bestehende Kontakte, unter Benachrichtigung des Spoc initiiert oder über den Spoc direkt gestellt werden.“ Wichtig sei dabei der „personifizierte“ Kontakt.[5] Den hat man u.a. durch Informationsbesuche und durch gegenseitige Hospitationen herzustellen versucht. „Um ein stärkeres Networking umzusetzen“, so berichtete BKA-Vizepräsident Jürgen Stock im Jahre 2008, „nimmt das BKA an einer wöchentlichen von der Securicon GmbH organisierten Telefonschaltkonferenz teil, bei der einige Global Player vertreten sind.“ Zudem sei es als Folge der Initiative „zu verstärkten Kontakten zwischen Firmenvertretern und BKA-Verbindungsbeamten im Ausland“ gekommen.[6]

Die Frage, ob die Initiative zu konkreten Ergebnissen führte, lässt sich anhand der vorliegenden Informationen jedoch nicht beantworten.

Wirtschaftsschutz

Die Global Player Initiative des BKA ist keineswegs der einzige Versuch staatlicher Sicherheitsbehörden, mit privaten Unternehmen zusammenzuarbeiten. Ein wesentlicher Teil dieser Partnerschaften spielt sich auf dem Feld des „Wirtschaftsschutzes“ ab. Der Begriff impliziert sowohl die „Konkurrenzausspähung“, für deren Abwehr die Unternehmen (und ihre Sicherheitsabteilungen) selbst zu sorgen haben, als auch die durch ausländische Geheimdienste betriebene oder unterstützte Wirtschaftsspionage. Für deren Aufdeckung sind die Ämter für Verfassungsschutz, für die Strafverfolgung Polizei und Staatsanwaltschaften zuständig.

Seit 2008 gibt es beim Bundesinnenministerium (BMI) einen „Ressortkreis Wirtschaftsschutz“. Vertreten sind darin erstens die mit dem

5 Glitza a.a.O. (Fn. 2)

6 Stock, J.: Internationale Zusammenarbeit zur Bekämpfung von Gefahren für die Wirtschaft, in: Die Kriminalpolizei 2008, H. 3, S. 85-89 (88)

Thema befassten Ministerien – neben dem BMI auch das Bundesministerium für Wirtschaft, das Auswärtige Amt sowie das Bundeskanzleramt. Präsent sind zweitens „Sicherheitsbehörden des Bundes" – im Klartext: das Bundesamt für Verfassungsschutz (BfV), der Bundesnachrichtendienst, das BKA und das Zollkriminalamt. Dazu gesellt sich drittens die bereits genannte Arbeitsgemeinschaft für die Sicherheit der Wirtschaft (ASW).

Der Ressortkreis sei das „Kernstück" der staatlichen Initiative in diesem Bereich, meint der Leiter der Abteilung Spionageabwehr im BfV, Burkhard Even. Das Gremium trifft sich zweimal jährlich. Hier würden „wirtschaftsschutzrelevante Informationen und Erkenntnisse ausgetauscht, bewertet, koordiniert und – das ist ein besonderes Anliegen – in geeigneter Weise der Wirtschaft zur Verfügung gestellt. Besondere Aufmerksamkeit wird der Effizienz der Kommunikationswege und dem Informationsaustausch zwischen den Sicherheitsbehörden und der Wirtschaft auf dem Gebiet gewidmet. Hierbei möchte ich unterstreichen, dass wir gerade den Dialog suchen; Wirtschaftsschutz darf keine Einbahnstraße sein!"[7] Die ASW übernehme dabei die „Bündelung und Koordinierung sicherheitsrelevanter Informationen aus der Wirtschaft an die Behörden wie auch in umgekehrter Richtung".[8]

Zusammen mit der ASW veranstaltet das BfV jährlich eine „Sicherheitstagung". Innerhalb seiner Abteilung Spionageabwehr befasst sich ein eigenes Referat mit dem Wirtschaftsschutz. Das BfV stellt den Unternehmen, vermittelt über die ASW, „Analysen, Referenten und Hilfsmittel zur Verfügung, u.a. für Tagungen der Arbeitskreise der Sicherheitsbevollmächtigten der Wirtschaft oder für überregionale Fachveranstaltungen von Firmen."[9] Even betont, dass das Referat Wirtschaftsschutz seine „Sensibilisierungsvorträge" nicht nur bei den Global Players, sondern auch bei „kleinen und mittelständischen Unternehmen" ausrichte. Das BfV gebe einen regelmäßigen Newsletter heraus, man führe mit einzelnen Unternehmen „bilaterale Informationsgespräche zu konkreten Sicherheitsthemen".[10] Das BfV betont dabei die Vertraulich-

7 Even, B.: Wirtschaftsschutzkonzept des Bundesamtes für Verfassungsschutz, in: BfV; ASW: Proaktiver Wirtschaftsschutz. Prävention durch Information, 4. Sicherheitstagung des BfV und der ASW am 18.3.2010 in Köln, Tagungsband, Köln 2010, S. 8-16 (13); www.verfassungsschutz.de/de/aktuell_thema/meldungen/me_100518_sicherheitstagung.pdf

8 Kaller, W.: Wirtschaftsschutz – eine Herausforderung für Staat und Wirtschaft, in: BfV; ASW: Braucht Ihr Sicherheitsbewusstsein ein Update. 3. Sicherheitstagung des BfV und der ASW am 11.12.2008 in Köln, Tagungsband, Köln 2009, S. 8-14 (9)

9 BfV: Spionage gegen Deutschland – aktuelle Entwicklungen, Köln November 2008, S. 11

10 Even a.a.O. (Fn. 7), S. 13

keit jeder Information: „Da wir besonders auf den Schutz unserer Quellen achten und – anders als die Polizei – nicht dem Legalitätsprinzip unterliegen, können wir unseren Hinweisgebern Vertraulichkeit zusichern. Keine der Firmen, die sich wegen möglicher Ausforschungen an die Spionageabwehr wendet, muss befürchten, dass die zur Verfügung gestellten Informationen ohne ihr Wissen und Wollen publik gemacht werden und sich womöglich negativ auf das Firmenimage auswirken. Die Verfassungsschutzbehörden stehen jederzeit für Beratungsgespräche zur Verfügung."[11]

Zudem erarbeite man gemeinsam mit der ASW auf spezielle Zielgruppen orientierte „Sensibilisierungskonzepte". „Durch einen stetigen wechselseitigen Informationsaustausch über Angriffsmethoden fremder Nachrichtendienste können sicherheitsrelevante Informationen kanalisiert und den Wirtschaftsunternehmen zeitnah für strategische Entscheidungen zur Verfügung gestellt werden."[12]

Auch beim BfV betont man die Notwendigkeit, dass sich die Partner „kennen und verstehen". Wesentliches Mittel dazu sei ein „regelmäßiger und strukturierter Personalaustausch", zum Beispiel in Form von Hospitationen, für die sich wohl insbesondere der letzte ASW-Vorsitzende Thomas Menk eingesetzt hatte. Menk war bis 2010 Chef der Daimler-Konzernsicherheit und davor selbst Mitarbeiter des BfV.

Wie eng der Austausch zwischen den Unternehmen und dem BfV tatsächlich ist und welche Qualität die vom BfV zur Verfügung gestellten Informationen haben, lässt sich aus den vollmundigen öffentlichen Erklärungen nicht ablesen.

Sicherheitspartnerschaften auf Landesebene

Einen Austausch zwischen Wirtschaft und staatlichen Sicherheitsapparaten gibt es auch auf Landesebene – meist in Form so genannter Sicherheitspartnerschaften. Von staatlicher Seite sind dabei in der Regel das Innenministerium, das Landeskriminalamt und das Landesamt für Verfassungsschutz beteiligt. Ihr Gegenpart sind meist die regionalen Industrie- und Handelskammern sowie die jeweilige „Vereinigung für Sicherheit der Wirtschaft" (VSW). Letztere sind Mitgliedsorganisationen der ASW und bilden deren regionale Standbeine.

11 BfV a.a.O. (Fn. 9), S. 11 f.
12 ebd., S. 11

Tagungen, Foren oder Symposien gehören auch auf Landesebene zum Repertoire der Kooperation. Darüber hinaus findet ein Informationsaustausch statt, der in der Regel über die VSW gesteuert wird. In Niedersachsen beispielsweise hat man sich auf folgenden Katalog von Themen geeinigt: „Wirtschaftsspionage, Proliferation, Konkurrenzausspähung, IT-Sicherheit, Marken- und Produktpiraterie, Produkterpressung, sonstige Wirtschaftskriminalität in ihren verschiedensten Erscheinungsformen, Korruption, politischer Extremismus/Terrorismus, polizeiliche Prävention/Beratung." Anders als im Falle der Global Player Initiative des BKA gibt es hier für die VSW respektive die beteiligten Unternehmen keine „sensiblen Informationen", sondern nur „allgemeine Lagebilder sowie Mitteilungen zu aktuellen bzw. speziellen Erscheinungsformen" der genannten Kriminalitätsbereiche, „allgemeine und abstrakte Gefährdungsanalysen" sowie „Zielgruppenorientierte Warnmeldungen".[13]

Fazit

Die praktische Bedeutung der diversen „Netzwerke der Information", die im letzten Jahrzehnt geknüpft wurden, bleibt von außen undurchschaubar. Die Betonung, dass es vor allem auf den persönlichen Kontakt und die Kenntnis des Gegenübers ankomme, lässt vermuten, dass hier neue informelle Kanäle des Austauschs entstehen, über die die auch unter Datenschutzgesichtspunkten „sensiblen" Informationen fließen. Unklar ist auch, welcher Effekt – etwa gemessen in Ermittlungsverfahren – aus den „Netzwerken" resultiert. Transparenz gibt es hier nicht.

Sicher ist hingegen, dass die Sicherheitsapparate der Unternehmen, die privaten Sicherheitsdienste und Ermittlungsfirmen, mit denen sie zusammenarbeiten, sowie die Organisationen wie die regionalen VSW und die ASW auf Bundesebene, die sie repräsentieren, durch die Netzwerke und Sicherheitspartnerschaften mit Polizei und Verfassungsschutz eine politische Aufwertung erfahren haben. Sie erscheinen als legitime Partner des Staates bei der Wahrnehmung der gemeinsamen Aufgabe „Sicherheit". Die Datenskandale der letzten Jahre bei Konzernsicherheitsabteilungen z.B. der Bahn und der Telekom haben in dieser Diskussion erstaunlicherweise keine Rolle gespielt.

13 www.vswn.de/downloads/sipaniedersachsenkonzept.pdf

TSC, FACI & TCS

Privatisierte Sicherheit im globalen Kontext

von Norbert Pütter

Dass neue, nicht-staatliche Akteure auf dem Sicherheitsmarkt auftauchen, ist ein internationales Phänomen. Ihre grenzüberschreitende Natur verschärft die mit ihnen verbundenen Probleme: fehlende Öffentlichkeit, rechtliche und politische Unkontrollierbarkeit, Abhängigkeit von den Aufraggebern und – in wechselnden Konstellationen – Arbeit mit, neben oder gegen staatliche Sicherheitsapparate.

Die öffentliche und wissenschaftliche Aufmerksamkeit beschränkt sich nach wie vor auf zwei Bereiche der Privatisierung von Sicherheit: die Übertragung militärischer Aufgaben auf privatwirtschaftlich ausgerichtete Unternehmen auf der einen, die Wahrnehmung einfacher polizeilicher Tätigkeiten wie Streifendiensten oder Bewachungsaufgaben auf der anderen Seite. Zwischen diesen Polen und teilweise sie überlappend existiert und entwickelt sich ein unübersichtliches Feld von „Sicherheitsanbietern", die mit spezifischen Dienstleistungen „Sicherheit" für jene zu produzieren versprechen, die dafür zahlen können. Insgesamt ist über diese Märkte wenig bekannt: Anbieter und Nachfrager, Aufgaben und Methoden, Erfolge und Gefahren, Zusammenarbeit mit der oder Konkurrenz zur staatlichen Polizei, Folgen für Gemeinwesen und Bürgerrechte – nur exemplarisch sind bisher einige Aspekte einer neuen „globalen Sicherheitsarchitektur" kritisch gewürdigt worden. Im Folgenden werden drei Varianten transnationaler profitorientierter Sicherheitsbranchen vorgestellt. Das zugrunde liegende Material stammt aus dem angloamerikanischen Raum, die Autoren hegen aber keine Zweifel, dass ihre Befunde für die gesamte westliche Welt zutreffen. Denn die beschriebenen Phänomene seien eine direkte Folge der neoliberal forcierten Globalisierung. Auffallend ist, dass es im Exportweltmeisterland Deutschland bisher so gut wie kein Interesse an der globalen Industrie der inneren Sicherheit gibt.

TSC = Transnational Security Consultancies

Mit „TSC", wörtlich übersetzt: transnationale Beratungsfirmen für Sicherheitsfragen, bezeichnet der Kriminologe Conor O'Reilly jene internationalen Unternehmen, die ein breites Spektrum unterschiedlicher Sicherheitsdienstleistungen anbieten, das über herkömmliche Beratungstätigkeiten hinausreicht.[1] Er nennt neben den im engeren Sinne betriebswirtschaftlichen die folgenden „typischen" Tätigkeiten:

- vertrauliche/verdeckte Untersuchungen/Ermittlungen
- Krisenmanagement, inklusive des Umgangs mit Entführungsfällen
- Betrugsbekämpfung
- Analyse von politischen und von Sicherheitsrisiken
- Schutz von intellektuellem Eigentum und vor Markenpiraterie
- Ausbildung von Sicherheitspersonal, einschließlich Vorschlägen zur Gestaltung des Sicherheitsbereichs (etwa in Unternehmen)
- Sicherheit bei Reisen (von Betriebsangehörigen).

Nach O'Reilly begann die Entwicklung der TSC in den 1970er Jahren als Begleiterscheinung der Expansion internationaler westlicher Konzerne in unsichere Regionen der Erde. Als Initialzündung identifiziert er die wachsende Zahl von Entführungen von Mitarbeitern dieser Firmen in Lateinamerika. Entführungen und Lösegeldzahlungen hätten zu einem Markt geführt, auf welchem den Unternehmen nicht nur die „Abwicklung" des Erpressungsgeschäfts, sondern – in Zusammenarbeit mit Versicherungen – auch die Absicherung dieses Risikos angeboten wurde. Aus diesem punktuellen Problem sei in den folgenden Jahrzehnten ein Industriezweig entstanden, der den gerade genannten weiten Kranz spezialisierter und auf die Kundenwünsche maßgeschneiderter Dienstleistungen anbiete. TSC sind aus dieser Perspektive zugleich Folge wie Voraussetzung weltweiter ökonomischer Expansion. Indem sie den transnational tätigen Unternehmen versprechen, Unsicherheiten und Risiken zu kalkulieren, zu managen und potentielle Schäden zu versichern, übersetzten sie politische und soziale Instabilitäten in wirtschaftlich kalkulierbare Größen. Das bilde die Basis für (weitere) Investitionen in unsicheren Regionen; zugleich werde derart der Markt für TSC ausgeweitet.

Ausmaß und Tätigkeiten der TSC, so O'Reilly, sind unbekannt. Zumindest der öffentliche Eindruck werde dominiert von den Großen der

1 O'Reilly, C.: The transnational security consultancy industry: A case of state-corporate symbiosis, in: Theoretical Criminology 2010, No. 2, pp. 183-210

Branche: „Control Risk“, „Dilicence“, „Kroll“, „The Risk Advisory Group“ (TRAG), „Clayton Consulting“ oder „Pinkerton Consulting“. Ein Einblick in die Tätigkeitsprofile werde mit Verweis auf betriebsinterne Vorgänge oder Betriebsgeheimnisse verwehrt, selbst die veröffentlichten Bilanzen seien kaum aussagekräftig, da es sich mitunter um Tochterfirmen handele oder sie in größere Mischkonzerne einverleibt würden. Allein „Control Risk“ (CR), eine der historisch ersten und größten auf dem TSC-Markt verfüge über ein Netzwerk von 27 Niederlassungen auf allen Kontinenten. Den Kunden würden täglich aktualisierte Nachrichten und Analysen angeboten; u.a. diese drei Dienste:

- „City Brief“: Sicherheitslage und Reiseumfeld für 320 Städte weltweit.
- „Country Risk Forecast“: Online verfügbare Analyse jüngster Entwicklungen in 200 Ländern in politischer und „operativer“ Hinsicht und in Bezug auf Terrorismus, Sicherheit und Reisebedingungen.
- „CR24“: Ein rund um die Uhr mit erfahrenen Beratern besetzter Dienst, die die Kunden anlassbezogen bei der Bewertung und Bewältigung von Sicherheitsszenarien unterstützen.

Das Verhältnis zwischen TSC und staatlicher Polizei bezeichnet O’Reilly als „symbiotisch“. Die TSC seien durchsetzt mit ehemaligen Polizisten bzw. Polizeiführern (FPO, Former Police Officer). Es bestünden lose institutionelle Verbindungen, die den informellen Informationsaustausch zwischen privaten und staatlichen Sicherheitsapparaten gewährleisten. Professionelle Sozialisation und gegenseitiges Informieren führten gemeinsam mit der Orientierung an zukünftigen Bedrohungsszenarien und risikoorientierten Bewältigungsstrategien zu einem Konsens über weltweite Sicherheitsgefahren. Die privat-staatliche Sicherheitssymbiose vollziehe sich in verschiedenen Varianten: Sie reichten von Vorteilen, die beide Seiten in gleicher Weise aus der Kooperation zögen, über die „Ausbeutung“ des einen durch den anderen Akteur bis zum unbeeinflussten Nebeneinander. Insgesamt entstehe durch die globalisierten Wirtschaftsbeziehungen und die sie begleitenden TSC ein neuer Ort privater Regulierung im weltweiten Kontext. Zu dieser nichtstaatlichen transnationalen Sicherheitsstruktur trügen nicht nur die Expansion in risikoreiche Weltregionen und die Privatisierung vormals staatlicher Sicherheitsaufgaben in den Nationalstaaten bei, sondern auch der Umstand, dass unter globalisierten Wettbewerbsbedingungen, nicht allein die Unternehmen, sondern mit ihnen die Staaten in Konkurrenz träten. Im Entstehen sei ein „hybrid transnational policing marketplace“, auf dem private wie staatliche Akteure ihre Lösungen anböten. In der

Sphäre transnationaler Sicherheitsarbeit („policing“) entwickelten sich Interessen und Ziele von Staat und Markt zunehmend ununterscheidbar.

FACI = Forensic accounting and corporate Investigation

Eine andere Variante transnationaler staatlich-privater Polizei- bzw. Sicherheitsarbeit entwickelte sich nach den Beobachtungen des kanadischen Kriminologen James W. Williams aus der Bekämpfung der Wirtschaftskriminalität seit den 1970er Jahren.[2] Ausgangspunkt sei gewesen, dass den staatlichen Ermittlern die notwendigen Qualifikationen fehlten, um in Wirtschaftsstrafverfahren ermitteln zu können. Deshalb habe man zunächst Fachleute aus Buchprüfungsfirmen beteiligt, die quasi im Nebenerwerb die wirtschaftlichen Sachverhalte so aufarbeiteten, dass sie in strafrechtliche Kategorien übersetzt werden konnten. Über die Jahre habe sich aus diesen Anfängen ein Markt und eine regelrechte Industrie entwickelt, für die Williams den Ausdruck „FACI“ vorschlägt. FACI könnte man übersetzten als „forensische (= kriminaltechnische) Buchprüfung und unternehmensbezogene Ermittlungen“. Sie bestehe, so zitiert er aus dem Bericht einer kanadischen Kommission von 2002, „aus einer Mischung von betrieblichen und externen forensischen Buchhaltern, Ermittlern, Beratern, Experten zur Prävention von Schadensfällen und Computerspezialisten, die mit Sicherheitsaufgaben befasst sind, u.a. im Auftrag von Banken, Kreditinstituten, Versicherungsgesellschaften, Einzelhandelsgeschäften, Börsen oder von Regierungseinrichtungen“.

Nach Williams besteht die FACI-Industrie aus drei deutlich unterscheidbaren Anbietergruppen: An der Spitze stünden spezialisierte Abteilungen für „forensische Buchprüfung“ innerhalb großer Buchprüfungs- und Beratungsfirmen. Als Beispiele nennt er KPMG, Deloitte & Touch, PriceWaterhouseCoopers, Ernst and Young und Kroll Lindquist Avey. Die kriminalistische Ermittlung und Untersuchung, ausgeführt von ehemaligen Polizisten, privaten Ermittlern für Wirtschaftsdelikte und Computer-Analysten, stellten einen Bereich innerhalb des Angebotsspektrums dieser weltweit tätigen Firmen dar. Auf einer mittleren Ebene existierten Firmen, die sich auf bestimmte Dienstleistungen spezialisiert hätten. Dazu zählten betriebsinterne Ermittlungen, Überwachung von

2 Williams, J.W.: Governability Matters: The Private Policing of Economic Crime and the Challenge of Democratic Governance, in: Policing & Society 2005, No. 2, pp. 187-211; ders.: Reflection on the private versus public policing of economic crime, in: British Journal of Criminology 2005, No. 3, pp. 316-339

Vermögenswerten und deren Beitreibung im Verlustfall sowie die Gewährleistung gebotener Sorgfaltspflichten. Schließlich gebe es eine dritte Gruppe von Anbietern auf dem FACI-Markt, die aus kleinen Ermittlungsfirmen bestehe. Diese verfügten über spezialisierte Ermittlungsmethoden z.B. in den Bereichen Überwachen von Vermögenswerten, Video- und Audioüberwachung oder industrielle Gegenspionage. Häufig bestünden zwischen dieser letzten und den beiden anderen Gruppen vertragliche Beziehungen über Beschaffung und Weiterleitung von Informationen.

Im Unterschied zu O'Reilly sieht Williams keine staatlich-private Symbiose, sondern eine „Gabelung" („bifurcation") in unterschiedliche Kontrollregime. Die FACI-Industrie habe nur deshalb entstehen können, weil sie eine „customized justice", d.h. eine auf die Unternehmenswünsche maßgeschneiderte Justiz ermögliche. Denn Untersuchungen im Unternehmensauftrag ermöglichten, sowohl die Gegenstände von Ermittlungen als auch die Verwendung von Erkenntnissen zu bestimmen. Polizeilich-strafrechtliche Untersuchungen könnten sich zum einen nur auf rechtlich relevante Sachverhalte beziehen und wären zum anderen von der Gefahr begleitet, dass Unternehmenspraktiken öffentlich würden, die dem Ruf oder der Geschäftstätigkeit des Unternehmens schaden könnten. Wirtschaftsdelikte würden von der Polizei unter rechtlichen Kriterien betrachtet, von FACI und ihren Auftraggebern unter wirtschaftlichen. Dementsprechend stünden nicht die Aufrechterhaltung der Rechtsordnung oder die Abwehr von Schäden für die Allgemeinheit im Vordergrund, sondern die wirtschaftlichen Interessen des Unternehmens.

Die Reaktionen auf Verhalten, das vom Unternehmen als schädigend angesehen wird, ließen sich drei Zielen zuordnen. Primär für die Unternehmen sei, eine aktuelle Schädigung zu stoppen („Stop the Bleeding"), sodann gehe es um eine Wiedergutmachung des entstandenen Schadens („Recovery") und zuletzt um Strafe und Abschreckung („Retribution/ Deterrence"). Während für das erste Ziel Verhandlungen mit dem Beschuldigten und/oder dessen Entlassung aus dem Unternehmen zur Verfügung stünden und der Schadensausgleich auf zivilrechtlichem Weg erreicht werden könnte, komme das Strafrecht und die öffentliche Untersuchung nur im Hinblick auf Strafe und Abschreckung in Betracht – ein Weg, der nur (noch) beschritten werde, wenn er den unternehmerischen Interessen nicht entgegenstehe.

Die rechtlichen und politischen Probleme der FACI sind nach Williams offenkundig: Ermittlungen im privaten Auftrag bedrohten deren Objektivität; es bestehe ein dauerhaftes Spannungsverhältnis zwischen

den wirtschaftlichen Interessen der Auftraggeber und den professionellen Standards der FACI-Firmen. Der Einsatz fragwürdiger Ermittlungstechniken – vom illegalen Abhören bis zum Bruch der Privatsphäre – stelle eine Gefahr für Demokratie und Rechtsstaat dar. Die Weitergabe von Erkenntnissen aus dem privaten in den staatlichen Bereich gefährde das Recht auf einen fairen Prozess und die Rechtsstellung von Beschuldigten.

Der Autor sieht fünf zentrale Hindernisse („key barriers"), die einer Regulierung („governability") der FACI-Industrie entgegenstehen:

- der Umstand, dass die FACI-Ermittlungen häufig im „privaten" Bereich der Unternehmen bleiben, sie öffentlich nicht sichtbar werden und die Lösungen nach Unternehmenskalkülen ausgewählt werden,
- die unterschiedlichen rechtlichen Standards, in die die Tätigkeiten eingebunden sind, sowohl national in der Wahl zwischen zivil- und strafrechtlichen Folgen als auch international in der Auswahl nationaler Rechtsordnungen,
- die Unüberschaubarkeit des FACI-Marktes (Zahl und Organisation der Anbieter, beteiligte Professionen, professionelle Standards etc.),
- die Vielzahl der beteiligten Interessen(gruppen): neben Auftraggebern und Anbietern auch die Opfer von Wirtschaftskriminalität, die Aktionäre oder die Öffentlichkeit insgesamt,
- die Trennung in private und öffentliche Sphären, die dazu führt, dass Wirtschaftsunternehmen wie Privatpersonen behandelt werden, die „ihre" Angelegenheiten zunächst selbst und ohne staatlichen Eingriff regeln sollen.

Williams interpretiert die institutionalisierte Aufteilung zwischen öffentlicher Polizei und FACI als eine Folge struktureller Probleme der kapitalistischen Ökonomie und ihrer Regulierung: Während der Eingriff in „private" wirtschaftliche Sachverhalte dem Selbstverständnis der öffentlichen Polizei widerspreche und sie deshalb keine besonderen Anstrengungen in diese Richtung entwickelt habe, böte sich die FACI-Industrie als Anbieter kundenorientierter, rascher und vertraulicher Lösungen an.

TCS = Transnational commercial security

Einen dritten Zugang zu globalisierten Sicherheitsmärkten wählen Les Johnston und Philip C. Stenning. Ihr Ausgangspunkt sind die zunehmenden transnationalen Aktivitäten in Sicherheitsfragen. Ein Element dieser Entwicklung sei die Herausbildung „privater transnationaler" Firmen, die außerhalb der Reichweite von Regierungen („beyond gov-

ernment") existierten.[3] Die Branche, die Sicherheit im internationalen Kontext verkaufe, sei, so die Autoren, alles andere als homogen. Sechs Anbietergruppen ließen sich auf dem Markt deutlich unterscheiden:

1. Sicherheitsabteilungen großer internationaler Unternehmen.
2. Firmen, die spezialisierte Dienstleistungen anbieten, genannt wird SECOM als Anbieter elektronischer Überwachung.
3. Neue Anbieter, die auf die durch die Privatisierung vormaliger Staatsaufgaben geschaffenen neuen Märkte drängen, z.B. Sodexho oder Serco für den Strafvollzug.
4. Firmen, die militärische Dienstleistungen anbieten, z.B. Blackwater oder MPRI (mittlerweile umbenannt bzw. aufgekauft).
5. Anbieter mit einem weiten Spektrum an Sicherheitsdienstleistungen, wie die britische G4S oder die schwedische Securitas.
6. Beratungsfirmen in Sicherheitsfragen mit Schwerpunkt auf Risikomanagement, z.B. Kroll oder Control Risk.

In ihren weiteren Ausführungen beschränken sich die Autoren auf die Anbieter der 4. Kategorie, die sie mit dem von ihnen selbst bevorzugten Begriff der „peace and stability operations industry" bezeichnen. Obgleich es sich von der Unternehmensgeschichte und der Ausrichtung dieser Unternehmen her um private Militärdienstleister handelt, sind die Überschneidungen zu eher polizeilichen Tätigkeiten nicht zu übersehen: Aufrechterhaltung eines Besatzungsregimes, Bewältigung von Konflikten „geringerer Intensität", Aufrechterhaltung von Sicherheit in Nachkriegsgesellschaften etc. Das Tätigkeitsprofil dieser Firmen deckt denn auch ein breites Spektrum ab: der Bereitstellung eigener Sicherheitsdienste, Reform des öffentlichen Sicherheitssektors und Ausbildung des Personals, Überwachung von Entwaffnungen oder Integration vormaliger Kriegsparteien, Beratungen in Sicherheitsfragen und Risikoanalysen, logistische und operative Unterstützungsleistungen, Umsetzung humanitärer Hilfen.

Johnston und Stenning problematisieren dieses weite Spektrum von bezahlten Sicherheitsdienstleistungen unter dem Aspekt der politischen Regulierung und Verantwortlichkeit („governance and accountability"). Sie spielen Rechtsgrundlage und politische Verantwortlichkeit für fünf Szenarien durch, in denen ein TCS-Anbieter Sicherheit in einem fremden Staat gewährleisten soll, und machen damit deutlich, dass derartige

3 Johnston, L.; Stenning, Ph.C.: Challenges of governance and accountability for transnational private policing, in: Lemieux, F. (ed.): International police cooperation, Portland 2010, pp. 281-297

transnationale Arrangements sich der rechtlichen und politischen Kontrolle entziehen.

Die Problemlösung der Autoren bleibt unbefriedigend: Da unter modernen Verhältnissen Sicherheit „pluralisiert" sei (weil neben den Staat andere Anbieter getreten seien), seien auch „plurale Formen der Regulierung und Verantwortlichkeit" („plural modes of governance and accountability") erforderlich. Auch wenn sie selbst Zweifel an der Wirksamkeit „multipler Regime" äußern, die im Zusammenwirken von Industrie, Zivilgesellschaft und Staat entstehen sollen, sehen sie darin die einzige Perspektive für eine demokratische Kontrolle der TCS.

Vage Schemen

Es gehört zu den Eigenarten des staatlichen Sicherheitssektors, dass er nur das an Öffentlichkeit zulässt, was den eigenen Interessen nützt. Deshalb sind weite Teile der staatlichen Sicherheitsapparate vor öffentlichen Einblicken geschützt. Durch die drei kurz umrissenen Ausprägungen einer transnationalen und auf Marktprozessen beruhenden Sicherheitskomplexes werden die demokratischen und politischen Probleme potenziert.

Die wechselnden Bezeichnungen, die unterschiedlichen Kontexte, in denen ihr Entstehen verortet wird, die verschiedenen Konstellationen zwischen öffentlicher und privater Gewalt deuten nicht nur auf einen empirisch wenig erhellten und sich im raschen Wandel befindenden Gegenstand hin, sondern sie verdeutlichen auch, wie sehr unter globalisierten Bedingungen die herkömmlichen Unterscheidungen ins Rutschen geraten. Das gilt für das vermeintliche Gegenüber von „privat" und „öffentlich", das gilt für die Alternative von marktförmiger oder rechtlich-bürokratischer Steuerung, und das gilt für die Illusion nationaler Politiken gegenüber transnationalen Aktivitäten. Es ist naheliegend, dass die bürgerrechtlichen Gefahren nicht kleiner, sondern größer werden, wenn aus den vormals halbwegs getrennten Sphären ein undurchschaubares privat-öffentlich-bürokratisch-marktförmiges-transnationales Sicherheitsnetzwerk entsteht, das uns als moderne „pluralistische" Sicherheitsarchitektur angepriesen wird. Politisch und bürgerrechtlich dringend nötig wäre, die vagen, eher episodenhaften Einblicke zum Anlass einer systematischen Bestandsaufnahme zu nehmen.

Der Weg in die Sicherheitsgesellschaft

Notizen zu einem Buch von Peter-Alexis Albrecht[1]

von Wolf-Dieter Narr

Auf 1040 Seiten hat Peter-Alexis Albrecht sein Wissen, seine Erfahrungen, seine Kritik, seine (Gegen-)Vorschläge und schließlich seine verhaltene Verzweiflung ausgebreitet. Von Strafrecht, Strafjustiz, Strafverfolgung und Strafvollzug in ihrer bundesdeutschen Entwicklung von etwa 1970 bis zur Gegenwart ist die Rede.

49 Abhandlungen von Peter-Alexis Albrecht, gegliedert in sieben Teile, enthält dieses an Material und Aspekten üppige, alles in allem faszinierende Werk. Sie werden „vor dem Hintergrund sich wandelnder Formen und Zugriffe sozialer Kontrolle sowie gesellschaftlicher Entwicklungen – in ihrem zeitlichen Verlauf" präsentiert. Sie sind werkbiographisch verknotet und mit pointierten Bilanzierungen versehen.

Eine Doppelperspektive ordnet Gegenstände und Gedanken. Sie zieht sich wie zwei Fäden durch die tausend Seiten: Der erste „realrechtliche"[2] Faden wird gewirkt durch die „kontinuierliche Erosion rechtlicher Fundamentalprinzipien" (S. 1). Der zweite muss „auf den Bürger … aus menschenrechtlicher Perspektive in jedem Fall unter Rückgriff auf verfassungsrechtlich abgesicherte unverfügbare Freiheitsgarantien begründet werden" (S. 34). Hierbei haben Albrechts Darlegungen den Vorzug, dass er in seiner Karriere als universitärer Strafrechtslehrer von Beginn an den (Jugend-)Strafvollzug intensiv erforscht hat; dass er ein praktizierender Anhänger der verblichenen Einphasenausbildung für JuristInnen gewesen ist und dass er sozialwissenschaftlicher Wahrnehmung wirklichkeitswissenschaftlich ebenso kundig ist wie

1 Albrecht, P.A.: Der Weg in die Sicherheitsgesellschaft. Auf der Suche nach staatskritischen Absolutheitsregeln, Berlin 2010

2 Realrechtlich ist analog zu realpolitisch gebildet. Darum meint es das aktuell herrschende Recht in der Interpretation durch die „hM", die herrschende Meinung.

historischen und rechtsphilosophischen, genetischen wie systematischen Entwicklungen und Bezügen. Darum nutzt er seine unverhältnismäßig breite juristische Karriere als Hebelkraft, um Rechts- und Politikentwicklung primär im Rahmen der BRD fundamental kritisch, nicht zuletzt stimuliert von ihrer nationalsozialistischen Vorgeschichte, nachzuvollziehen. Darum leitet der Untertitel seines repräsentativen Werkes Analyse und Urteil: Regeln gilt es zu finden und wie Deicharmierungen zu errichten wider eine das Recht entsichernde Gesetzesflut und ihre administrative Verfingerung, die das Recht und seine bürgerliche Freiheit konstituierende Pfeilerfunktionen überspülen und versumpfen und verfaulen lassen.

Die Versprechungen des Wohlfahrtsstaates

Mit der Gegenwart, dem „herrschenden Präventionsparadigma", hebt dieses Buch an. Nach einer „biographischen Zuführung" – eine solche ist allen sieben Teilen vorangestellt – folgt ein Beitrag über den „interdisziplinären präventiven Kontext von Kriminalität und Kriminalisierung" – ein Auszug aus Albrechts 2005 neu aufgelegten Studienbuchs zur Kriminologie.[3] Schon dieser erste, die Debatte und ihre Entwicklung eher retrospektiv grundlegende Teil, enthält eine Fülle materialgestützter Hinweise darauf, dass der „normative Schuldbegriff" verwässert zu werden droht und – präventiv fixiert – die Intransparenz der europäischen Rechtsentwicklung zunehme. Wie immer erneut schließt dieser Teil mit Folgerungen, die Albrecht für die Lehr- und Lernprozesse der JuristInnen fordert. Allerdings fehlen durchgehend Hinweise zum Wie, zu den Lehr- und Lernformen einschließlich der Prüfungsordnungen. Kund wird in jedem Fall ein Professor, der die Lehre ernst nimmt – und das ist alles andere als üblich.

Der 2. Teil gilt dem „sozial-integrativen Strafrecht" des Wohlfahrtsstaates, der zeitlich der präventiven Kehre vorhergeht. Die insgesamt positive Akzentuierung des wie eine feste Größe behandelten Wohlfahrtsstaates und seines ums Strafen kreisenden Gebarens – Untertitel: „Das Aufscheinen von Menschenrechten in den späten 60er und 70er Jahren" – hält Albrecht nicht davon ab, ja motiviert ihn geradezu, wie er in der „biographischen Zuführung" bekennt, die „Empörung über ver-

3 Albrecht, P.A.: Kriminologie: eine Grundlegung zum Strafrecht. Ein Studienbuch, 3. Aufl. München 2005

letzte Menschenrechte“ im Strafvollzug präzise zu verorten. Die Grenzen des Sicherheitsvollzugs erfordern die „Gewährung eines realen Freiheitsraums innerhalb des Strafvollzugs“ (S. 42).

> „Das sind die Grundbedingungen der durch den Staat zu fördernden und zu achtenden Menschenwürde. Pflicht des Staates wäre es, die Würde jener, denen er die Freiheit nimmt, strikt zu achten und dafür Voraussetzungen der Förderung zu schaffen. Das sind Menschenrechte des Strafgefangenen“ (S. 43).

Der Feststellung zur „prognostischen Irrelevanz des Haftverhaltens“ u.a. (S. 48), die mit den Erfahrungen des Rezensenten als eines „freiwilligen sozialen Helfers“ in Haftanstalten übereinstimmen, folgt diese empirische Summenformel eines emphatischen Normativisten:

> „Der Antagonismus zwischen Vollzugsrealität und der Theorie des Strafens lässt sich im Begriff ‚Resozialisierung‘ nicht auflösen. Zu groß ist der auf die Vollzugsrealität gestützte und damit reale Pessimismus, der dem ideologischen Vollzugsziel entgegensteht, wonach der Gefangene im Vollzug der Freiheitsstrafe fähig werden (soll!), ein Leben ohne Strafe zu führen.“

Daran schließt Albrecht die universitär fast allgemein geltende Bemerkung zum Mangel des „Learning by doing“ an:

> „Den meisten jungen Studierenden fehlt jede Praxiserfahrung im Kriminaljustizsystem und im Strafvollzug, und zumeist auch jede allgemeine Lebenserfahrung. Ein zentraler Strukturmangel des deutschen Universitätssystems“ (S. 48).

Hinweise zur Rolle der Psychiatrie unter Haftbedingungen folgen. Trotz aller Kritik urteilt Albrecht m.E. hier zu sanft, betrachtet man die knetmassige Bedeutung der psychiatrisch-psychologischen Gutachterei und ihrer pseudo-szientifischen Anmaßungen von der strafgerichtlichen Verurteilungswiege bis zur Entlassungsbahre (einer Bahre, die manches Mal ganz ohne Metaphorik im Strafvollzug realisiert wird).

Die präventive Kehre

Der 3. Teil befasst sich mit der „Wende zum Präventionsstaat“ der 80er und 90er Jahre (S. 149-506). „Prävention“ wird als „Zauberwort und argumentativer Alleskleber“ erkannt (S. 149).

> „Der vollmundigen Steuerungsomnipotenz der Normen dieser rechtspolitischen Betätigungsfelder aller politischen Parteien steht die minimale strafrechtliche Anwendungshäufigkeit gegenüber“ (S. 155).

Die repressiv gekehrte Prävention, ihre andauernde sich überschlagende Vorverlagerung, die alle Hürden überspringt, die Bevölkerung einspannt, Ursachen ausspart u.v.a., werden überzeugend apostrophiert, ebenso Resozialisierungshindernisse oder Irrtümer und Irrverhalten jugendstraflicher Erziehungskonzepte. Strafvollzugsexempel und Ausführungen zur Jugendstrafe, die meist kontraproduktive Ideologeme und Praktiken berühren, finden sich, bald kürzer, bald länger in (fast) allen Teilen erhellend eingestreut. Immer wieder finden sich übrigens auch merkwürdige Albrechtsche Tabuformeln, denen er in anderen Bemerkungen teilweise selbst widerspricht.

> „Hinter die Gebote der Menschenwürde, der elementaren Grundrechtsverwirklichung und elementarer rechtsstaatlicher Garantien gibt es kein Zurück mehr" (S. 207).

Kleine Empfehlung: Albrecht möge Albrecht lesen! Wie sehr sich der Autor empirisch analytisch selbst immunisiert, tritt im zweiten Abschnitt dieses Teils zutage: „Die Bewährung rechtsstaatlich abgesicherter Spezialprävention angesichts neuer Herausforderungen" (S. 218 ff.). Trefflich arbeitet er heraus, dass und wie Prävention der herrschend inszenierten Art zu einer Individualisierung und Pathologisierung gesellschaftlicher Konflikte führt. Dazu passt Albrechts Kritik der regierungsamtlichen, von Hans-Dieter Schwind seinerzeit – selbstredend wissenschaftlich ununabhängig – geleiteten Gewaltkommission, eingesetzt im Dezember 1988 (S. 469 ff.).[4] Die Kommission formte „Gewalt" nach dem Bilde einzelner Täter. Gesellschaftliche oder gar staatliche Ursachen kamen nicht in den Blick. Präventive Erwägungen wurden konsequent repressiv gehärtet.

> „1. ... Das der Kommission im Auftrag der Bundesregierung erklärungsbedürftige Gewalt-Phänomen ist allein personale, vom Bürger ausgeübte und vom Staat deklarierte Gewalt. Bezogen auf diese Form der Gewalt befinden wir uns nach der unbestrittenen Ansicht von Sozialhistorikern im gewaltärmsten Abschnitt unserer Geschichte. 2. ... Ausdrücklich nicht zum Untersuchungsgegenstand und nicht zur ‚Gewalt' zählen nach dem Verständnis der Kommission strukturelle und staatliche Gewalt, beispielsweise die drohende oder eingetretene Verletzung oder Tötung von Menschen durch die Zerstörung ihrer natürlichen Lebensgrundlagen mit den Mitteln des ‚technischen Fortschritts'; die drohende oder eingetretene Verletzung oder

4 Schwind, H.D. u.a. (Hg.): Ursachen, Prävention und Kontrolle von Gewalt. Analysen und Vorschläge der Unabhängigen Regierungskommission zur Verhinderung und Bekämpfung von Gewalt, 4 Bde., Berlin 1990

> Tötung von Menschen durch die Bereitstellung und Erprobung von Massenvernichtungswaffen; die immer komplizierter werdenden, knebelnden Lebensräume einer Gesellschaft, die für viele Menschen eine undurchschaubare und ängstigende Gestalt annehmen; die Anwendung von Gewalt durch staatliche Zwangsorgane ... 4. ... Die Kommission lockert ihre rückwärtsgewandten Vorschläge mit Geschick durch liberale Lösungsangebote für den Umgang mit Gewalt auf (Kindesmisshandlung wird an Kinderschutzzentren delegiert, Gewalt gegen Frauen an Frauenhäuser; das elterliche Züchtigungsrecht gegenüber Kindern soll beseitigt werden). Die erdrückende Masse der an Polizei und Strafjustiz adressierten Interventionsvorschläge konterkariert und überdeckt allerdings gründlich die wenigen Präventionsvorschläge. Übrig bleibt ein eindeutig polizeistaatlicher Kern des Gutachtens. Anpassung und Disziplinierung sind die Konsequenzen der Kommissionsempfehlungen" (S. 472 f.).

Wir erleben gegenwärtig die Wiederkehr des Gleichen. Das Gewaltmonopol und seine allgemein selbsterzeugte Legitimation macht den Wendeltreppengang bürgerlich kostenreicher Torheiten möglich.

Entkriminalisierung!

Nach der füllig belegten präventionsstaatlichen „Kehre" inmitten der seinerzeit regierungsamtlich verheißenen „geistig moralischen Wende" resümiert der vierte Teil wider den Strich „Ansätze einer Gegenreform: Normative Entkriminalisierung und soziale Sicherheit im Strafvollzug" (S. 527-666). Präsentiert werden hier unter anderem die Vorschläge der von der niedersächsischen Landesregierung einberufenen Reformkommission zum Strafrecht. „Wie ein roter Faden durchzieht der Gedanke der Entkriminalisierung den Bericht", notiert Albrecht, der seinerzeitige Kommissionsvorsitzende, in seiner „biographischen Zuführung" (S. 528).

Die begründeten Entkriminalisierungen spitzen sich auf eine „Revision der Anti-Terrorismus-Gesetzung" zu – insbesondere der in der Zwischenzeit erweiterten, einem erhabenen „Kernstrafrecht" (Albrecht) in jeder Hinsicht zuwider ausufernden §§ 129, 129a des Strafgesetzbuchs. Die Überlegungen zur Entkriminalisierung enden in der Präsentation des Gutachtens einer von Albrecht präsidierten „Expertenkommission Hessischer Strafvollzug" (S. 541 ff.). In den Albrechtschen „Conclusionen zur normativen Entkriminalisierung und sozialen Sicherheit im Strafvollzug"(S. 661 ff.) werden sie verdichtet:

> „Soziale Sicherheit im Strafvollzug berücksichtigt, dass Strafvollzug stets eine Art von sozialem Tod, soziale Isolierung, aber auch Entwürdigung durch depravierende Lebensumstände bedeutet ... Die Ineffektivität und Kontraproduktivität des Strafvollzugs ist unübersehbar" (S. 662).

Die Sicherheitsgesellschaft

Der 5. Teil (S. 667-817) markiert die Wende in der präventiven Wende, genauer: deren exekutivrechtliche, polizeilich-bürokratisch verbreiterte Veralltäglichung: „Vom Präventionsstaat zur Sicherheitsgesellschaft – Jenseits des rechtsstaatlichen Strafrechts nach der Jahrtausendwende". Nun hagelt's dicht. Unter der Abschnittsüberschrift „Präventiv-Folter: Der Weg in den Staatsterrorismus" stellt Albrecht fest: „das hätte ich nie für möglich gehalten" (S. 669). Von der „Sicherheitsgesellschaft" als „neuem Gesellschaftstyp" ist die Rede (S. 673); von der „neuen Polizei" (S. 674); einer „Vernichtung des Rechts" (S. 687), begleitet von einer „präventiven Aufrüstung" (S. 693). Die „Krise des Wohlfahrtsstaats" erzeuge einen „wachsenden Steuerungsbedarf"; sie werde vom „Rechtsstaat im Rückzug" begleitet, der ein „nachpräventives Strafrecht" (S. 702) schaffe. Belegt werden diese Kennzeichen einer „Sicherheitsgesellschaft", die nach manchem Vorlauf am 11. September 2001 auf den Plan getreten sei, durch eine Verpolizeilichung auf dem breiten und proteusartig wechselnden Rücken der „Organisierten Kriminalität" jenseits nationaler Grenzen (S. 715 ff.); durch die globalisierte und globalisierende „Überlagerung des Rechtscodes durch einen Code der Ökonomie", die den Rahmen der seither nebeneinander wirksamen „Subsysteme" „Recht" und „Ökonomie" zerbersten ließe (S. 737 f.). Die „neu verfasste Polizei" (S. 761 ff.) verwische maßstabslos alle rechtsstaatlichen Grenzen, nicht zuletzt diejenigen zwischen „öffentlich" und „geheim". Beispielhaft führt Albrecht die G 10-Entscheidung des Bundesverfassungsgerichts an (S. 771 ff.). Er zeigt an dem inflationär gebrauchten Adjektiv „operativ", dass und wie die Grenzen des polizeilichen Handelns und Möglichkeiten der Judikative, diese Grenzen zu markieren, schwinden:

> „Die beschriebenen rechtsstaatlichen Bindungen sind rechtsstaatlich und praktisch in Auflösung begriffen. Das Aufgelöstsein dieser Bindung entspricht der normalen historischen Situation im Verhältnis von Polizei und Strafrecht. Die Auflösung rechtsstaatlicher Grenzen beginnt zunächst im Polizeirecht. Seit Mitte der siebziger Jahre hat das ‚operative Konzept der Kriminalitätsbekämpfung' Hochkonjunktur. Die Trennung von Prävention und Repression und damit die Differenz von konkreter Gefahr und Anfangsverdacht ist durch eine staatsmachtorientierte Kriminal- und Innenpolitik als zu eng verworfen worden. Nicht mehr die Aufklärung einer Einzeltat, sondern die Aufdeckung krimineller Strukturen ist die Zielbestimmung polizeilicher Arbeit. ‚Operativ' als Oberbegriff für diese neue Zielbestimmung steht im Gegensatz zu ‚bloß' präventiv oder ‚bloß' repressiv. Der Begriff des Operativen legt bereits nahe, worauf es polizeilicher Tätigkeit ankommt. Wichtig sind ausschließlich die bereitgestellten Mittel, die zur

> Erreichung kriminalstrategischer Ziele Wirksamkeit zu versprechen scheinen. Zweck- und Prinzipienbindung sind keine wesentlichen Bestandteile operativer Polizeikonzeptionen“ (S. 775 f.).

Zwischen fast panisch stimmende Apostrophen von allgemeinen Entwicklungen der Erosion und Grenzenverwischung streut Albrecht immer erneut bekenntnishafte Hinweise auf Rettungsanker.

> „Die bisherige Entwicklung der Menschheit gibt nur eine Möglichkeit vor, globale Katastrophen der Herrschaftspositionierung zu verhindern. Die *uneingeschränkte Herrschaft des Rechts*, für die es eines Organisationsrahmens der uneingeschränkten Herrschaft der Vereinten Nationen bedürfte, ist die einzig legitime Alternative zur Regulierung gewaltsamer Herrschaftsansprüche des Starken gegenüber dem Schwachen. Gelingt es nicht, … (die Makrokonflikte, WDN) … durch Recht einzudämmen und zu regulieren, eliminiert sich die Menschheit selbst. ... Die Gründung des Internationalen Strafgerichtshofs ist ein vielversprechender Ansatz, ...“(S. 703; siehe auch Europa-bezogen S. 707). „Das Recht hat im ‚Kampf gegen Terrorismus‘ eine Kontrollfunktion für politische Übermaßreaktionen“ (S. 731; ähnlich S. 734). „Auf Rechtsstaat und Judikative kommt alles an“, S. 806 f.).

Hoffnungen und Postulate

Der 6. Teil, „Hoffnung Europa?“ (S. 818-926), liegt etwas wie ein unbehauener Findling in Albrechts argumentationsdicht bestellter Landschaft. Es wird nirgendwo aus Elementen und Fermenten der Verfassungswirklichkeit ohne Verfassung, welche die EU darstellt, ersichtlich gemacht, worin die Hoffung bestand oder bestehen sollte – in der allgemein verbreiteten europäischen Aufbruchstimmung nach 1945,[5] zu Zeiten der EWG und vollends der EU samt ihren Erweiterungen. Ein „neuer Gesellschaftsvertrag“, Albrechts leer geleierter Fetisch, eine „europäische Verfassung“, werden angemahnt wie ein europäischer Strafrechtsraum samt selbstredend „unabhängiger Judikative“, ohne in irgendeiner Weise die Schwierigkeiten allein schon der Größenordnung anzudeuten und institutionell-prozedurale Vorkehrungen zu markieren. Schon im Beitrag zum europäischen Haftbefehl verweht die europäische, mit hohen Worten vernebelte Stimmung. Es bleibt Albrechts Festung, deren

5 Wer verstehen will, wie und warum damals uns Junge – dem Zugriff des Nationalsozialismus entsprungen, bevor er uns voll einvernehmen konnte, in den Dreißigern geboren, antinational gehäutet, voll radikaldemokratisch verstandener Reeducation – Europa als realisierbare Utopie begeisterte, mag die frühen Jahrgänge der „Frankfurter Hefte“ und ihre Autoren konsultieren: Walter Dirks, Eugen Kogon, Karl Heinz Knappstein u.a.

Gedankenkonstruktion und -basis er im Motto dieses Beitrags selbst gekennzeichnet hat. Sie wird im vorletzten Absatz dieses Teils unter der Überschrift „Europäische autonome und unabhängige Dritte Gewalt“ voll der schönen Fiktionen resümiert.

Im siebten und letzten „Teil“ begibt sich Albrecht auf die schon im Untertitel verheißene „Suche nach staatskritischen Absolutheitsregeln“ (S. 927-1040). Dieser gedanklich sympathische und – im Sinne des rechtsphilosophischen Kronzeugen Immanuel Kant gesprochen – „gut gesinnte“ Abschluss des großen Albrechtschen Wurfs, in dem die in vierzig Jahren aus der Präventions- und Sicherheitsbüchse entfleuchten Übel betrachtet werden, geht postulativ in die Zukunft. Eine „gerechte Sozialordnung“, die „individuelle Freiheit“, die „freiheitssichernden Prinzipien“ eines Kernstrafrechts und die „Stärkung und Autonomie der Judikative“ – die Postulate, denen man gerne folgte, bleiben indes ohne historische und soziomaterielle Herleitung. Sie werden pauschal und abgehoben gesetzt. Sie orientieren sich an ihrerseits nicht ausgeführten und ideengeschichtlich nur nominell benannten Vorbildern des – idealisch – historischer Wirklichkeit enthobenen bürgerlichen 18. Jahrhunderts. Man kann nicht von einem Weberschen Idealtyp sprechen, so sehr Albrecht den fast durchgehend missverstandenen Ausdruck liebt. Durchgehend fehlen institutionell organisatorische Hinweise, wie sie sich aus einer sozialen (politischen) Phantasie ergäben. Vor dem Hintergrund einer nüchternen Analyse der dynamischen, zugleich in ihren Größenordnungen nur technologisch fassbaren Faktoren der globalisierten und sich weiter globalisierenden Gegenwart wären diese aber notwendig.

Die „staatskritischen Absolutheitsregeln“ fallen eher armselig aus. Wie sie abgelöst gewonnen worden sind und was sie bewirken sollten, bleibt dunkel. Sie erinnern an Tabus und Fetische. Sie enden mit einem Hinweis auf das angeblich die Erfahrung des Nationalsozialismus widergebende „Recht zum Widerstand“ nach Art. 20 Abs. 4 des Grundgesetzes. Dieses wurde 1968 als süßsaueres, irrelevantes Zückerchen im Zuge der Notstandsverfassungsänderung ins Grundgesetz eingefügt (S. 1040).

Mängel und Lücken

Einige sind hier zu benennen. Das umfängliche Buch, ein Handbuch zu einem zentralen Gegenstand, verliert darum nicht sein Gewicht. Die Gründe dafür, dass es so widersprüchlich ausgefallen ist – voll der empi-

risch analytischen Kenntnis und voll eines unvermittelten Maßstabs scheinexakter Markierungen –, kann ich nur ahnen:

- Der werthafte Bezugsrahmen Albrechts wirkt durchgehend normativ überhöht und abstrakt à la „rechtsstaatliche Vorbildfunktion des strafenden Staates“ (S. 218).
- Möglicherweise einer professionellen Eigenart der Juristerei geschuldet, findet häufig eine unbemerkte und schier unmerkliche Vermischung von „Ist-Aussagen“ und Postulaten statt. Nicht selten werden unkenntliche Postulate behandelt, als seien sie wirklich. Dies gilt etwa für die Demokratiebehauptung in Bezug aufs Grundgesetz oder auch den Verfassungstorso der EU. Nicht nur wird die Verfassungsnorm nach US-amerikanischem Vorbild wie eine heilige Wirklichkeit behandelt. Abweichend Verfassungswirkliches wird jeweils seinerseits normativ geschönt.
- „Recht“, „Rechtsstaat“, „Schuldstrafe“, „individuelle Menschenrechte als Abwehrrechte“ u.a.m. werden nicht nur wie Gegebenheiten, sondern wie sachliche, übersachliche Subjekte behandelt, aber eben nicht soziohistorisch fundiert. Emphatisches Schweben ist die Folge.
- Solches Wandlungswunder passiert bei Albrecht von Anfang an und dickt sich am Ende. Die Judikative, auch die juristischen Fakultäten und ihre VertreterInnen werden ohne materielle soziale Begründung, ohne alle allemal prekären Kontextbedingungen zu Instanzen erhoben, die als gesellschaftliche, ja als übergesellschaftliche Pouvoirs neutres inmitten aller globalen Spannungen und Kräfte das erhabene Recht zu gewährleisten vermöchten. Wie? Leere gähnt.
- Als ob die Judikative es vermöchte, auf eigenem Boden und mit dem eigenen Himmel ihrer „absolut“ gesetzten Normen (Regeln), die Freiheit aller zu sichern. Die Begründung der „absoluten“ Normen, die sie irdisch – ihren kasuistischen Gebrauch bedenkend – relativieren müssten, bildet eine Lücke.
- Aus dem Rahmen fällt darum auch jede nüchterne Staatsanalyse. Das staatliche Gewaltmonopol Albrechts, der doch mit Kollegen u.a. trefflich den rumpelstilzchenhaften Bericht der Gewaltkommission und ihren einseitigen Gewaltbegriff traktiert hat, dieses staatliche Gewaltmonopol wird noch über Hobbes hinaus ein kaum noch sterblicher Gott. Es erscheint allen Gegenbeispielen zum Trotz, die niemand besser kennt als Albrecht, als eine Konflikte zwischen Personen lösende schnurrende Tigerkatze. Dass modernes Recht und staatliches Gewaltmonopol zwei Seiten einer Medaille darstellen,

dass das staatliche Gewaltmonopol, unbeschadet der Änderungen staatlicher Institutionen und Funktionen, Gewalt nicht abbaut, sondern im eigenen Interesse präsent hält und schafft, wird nur randständig kund. Die normativen Prämissen verschlingen schlechte Materialität.

- Der Mangel materieller Analyse in einem weiten Sinne, bei einem empirisch mehrfach so Erfahrenen wie Albrecht kaum zu erklären, lässt es auch zu, dass auf idealisiertes Recht und seinen Staat im europäischen 18. Jahrhundert als Bezugsgrößen rekurriert wird. Dadurch werden weder die heutigen Freiheitsgefährdungen erklärlich. Noch wird möglich, sie aufgrund fundierter Analyse und sei es nur kognitiv zu bekämpfen.
- Seltsamerweise nutzt Albrecht nicht, dass er vierzig kataraktreiche Jahre der Rechts-, Staats- und Gesellschaftsentwicklung in engagierter Teilnahme nah beobachtet hat. Die Entwicklung wird nicht analytisch aufgedröselt. Selbst der begrifflich angegebene Wandel vom „Präventionsstaat“ zur „Sicherheitsgesellschaft“ wird nicht begrifflich erschlossen. Warum der Wandel der Makroeinrichtungen vom „Staat“ zur „Gesellschaft“? Was unterscheidet die präventive Kehre vom staatsbegleitenden, nun expandierenden Sicherheitsschatten? Welche Effekte sind auf globalisierende Phänomene und nicht mehr verantwortlich handhabbare, Recht in all seinen Formen entfesselnde Größenordnungen zurückzuführen? Welche Konsequenzen wären gerade diesbezüglich auch in demokratisch rechtsstaatlicher Absicht zu ziehen? „Dunkel war’s, der Mond schien helle.“

Albrechts gegenwartsbezogene Verzweiflung eines praktischen Faust ist mehr als verständlich: Dass wir nichts machen können, Verhängnisvolles nicht aufhalten, unsägliches von Menschen gemachtes Leid nicht zu beheben vermögen, das will mir schier das Herz verbrennen. Indes, so nahe es liegt, gerade dann verbieten sich Fluchtbewegungen, solche in „machtgeschützte Innerlichkeiten“ (das ist kein Weg für Albrecht) ebenso wie die zu fiktiven historischen Vorbildern. Als hülfe das Lob einer normativ idealisierten Vergangenheit über die Schwernisse der Gegenwart hinweg.

Castortransport ohne Grundrechte

Böse Schotterer und gute Sitzblockierer?

von Elke Steven

Im November 2010 wurde erneut hochradioaktiver Müll aus der Wiederaufarbeitung in Frankreich ins Zwischenlager Gorleben transportiert. Das Komitee für Grundrechte und Demokratie hat die Proteste gegen den Castortransport und das Vorgehen der Polizei beobachtet.

In verschiedenen Politikbereichen entsteht der Eindruck, dass sich die Regierungen mit Arroganz über den Willen der Bevölkerung hinwegsetzen und nicht einmal mehr versuchen, ihre politischen Entscheidungen zu vermitteln. Das ruft breite Empörung hervor. Erfahrungen mit polizeilicher Gewalt gegen die Protestierenden führen – wie unlängst das Beispiel „Stuttgart 21" zeigte – nicht zum Rückzug, sondern zur Haltung „jetzt erst recht". Dies hätte auch das Motto der Demos und Aktionen gegen den jüngsten Castor-Transport sein können. Kurz zuvor hatte die Bundesregierung mit der Atomlobby eine Laufzeitverlängerung für die bestehenden Atomkraftwerke ausgehandelt. Gegen die Aufkündigung des „Atomkonsenses", den die KritikerInnen wegen der noch viel zu langen Restlaufzeiten nie als Atomausstieg werten wollten, mobilisierte die Antiatombewegung seit längerem.

Wie in früheren Jahren wartete die Polizei auch diesmal mit Verboten auf. Mit Datum vom 23. Oktober 2010 erließ die Polizeidirektion Lüneburg eine Allgemeinverfügung, mit der sie „Versammlungen unter freiem Himmel und Aufzüge" für den „Zeitraum vom 6.11.2010, 00.00 Uhr, bis zum 16.11.2010, 24 Uhr" innerhalb eines für den Castor-Transport bestimmten Korridors und in einem Umkreis um Verladekran und Zwischenlager untersagte.[1] Schon für Samstag (6. November) waren

1 www.grundrechtekomitee.de/sites/default/files/Allgemeinverfuegung.pdf, siehe auch die Presseerklärung des Komitees: www.grundrechtekomitee.de/node/364

unangemeldete, ab Sonntag dann alle öffentlichen Versammlungen in diesem Bereich verboten. Die Verbote sollten außer Kraft treten, „sobald der Castor-Transport vollständig in das umzäunte Gelände des Zwischenlagers eingefahren ist".

Rechtlich fragwürdig war diese Allgemeinverfügung schon allein deshalb, weil sich die Polizeidirektion zunächst an die Stelle der eigentlichen Versammlungsbehörde, nämlich des Landkreises, setzen musste. Sie begründete dies vor allem mit § 102 Abs. 1 des Niedersächsischen Sicherheits- und Ordnungsgesetzes (NdsSOG), nach dem sie als Fachaufsichtsbehörde aber nur einzelne Maßnahmen zur Gefahrenabwehr übernehmen darf. Im vorliegenden Fall handelte es sich jedoch um die Verlagerung abstrakter Zuständigkeiten im Vorwege.

In der Einleitung ihrer Allgemeinverfügung stellte die Polizeidirektion richtig fest, dass die Behörden „grundsätzlich die Pflicht" haben, „Versammlungen zu schützen". Sie tat dies aber nur, um anschließend zu begründen, warum in diesem Fall die Rechte der Protestierenden außer Kraft zu setzen seien. Eigentumsrechte der Betreiber auf einen störungsfreien Transport sollten die Grundrechte aushebeln.

Die Polizeidirektion zitiert zwar rechtfertigend das Bundesverfassungsgericht, das sich immer wieder schützend vor das Grundrecht auf Versammlungsfreiheit gestellt hat. In seinem Brokdorf-Beschluss von 1985 hat das Gericht unmissverständlich festgehalten, dass Versammlungen „ein Stück ursprünglich-ungebändigter unmittelbarer Demokratie" enthalten, „das geeignet ist, den politischen Betrieb vor Erstarrung in geschäftiger Routine zu bewahren". Es stellte fest, dass „für die friedlichen Teilnehmer der von der Verfassung jedem Staatsbürger garantierte Schutz der Versammlungsfreiheit auch dann erhalten (bleibt), wenn mit Ausschreitungen durch einzelne oder eine Minderheit zu rechnen ist". Statt dieser Rechtsprechung zu folgen und zumindest tatsächliche Anhaltspunkte für einen insgesamt unfriedlichen Verlauf zu liefern, zählte die Behörde in ihrer 27-seitigen Verfügung eine Unmenge von Vorfällen aus den letzten 15 Jahren auf. Zur Begründung eines Versammlungsverbotes eigneten sie sich samt und sonders nicht.

Grundrechte – aber nur im kleinen Rahmen?

Im Kapitel „derzeitige Erkenntnisse" ihrer „Gefahrenprognose" listete die sich selbst ernennende Versammlungsbehörde vor allem auf, dass der Protest gegen den Castor-Transport – und damit gegen die aktuelle

Politik der Bundesregierung – breit sei. Die staatlich gewollte Wiederaufnahme der Erkundungsarbeiten für ein Endlager in Gorleben und die geplante Laufzeitverlängerung für Atomkraftwerke ließen befürchten, dass sich viele Bürger und Bürgerinnen am Protest beteiligen. Als Argument für ein Versammlungsverbot wurde angeführt, dass die den Protest tragenden Gruppen ihre Mobilisierungsbemühungen verstärkt hätten. Sie würden auch überregional, gar über das Internet, werben und Kinospots zeigen. Die „größte Anti-Atom-Manifestation in der Region um Gorleben" sei angekündigt worden. Viele Organisationen wollten sich daran beteiligen. Aufgerufen wurde auch zu einer Menschenkette von Lüneburg nach Dannenberg. Diese sollte allerdings auf der Straße stattfinden, die außerhalb der von der Verfügung erlassenen Verbotszone liegt, und hatte daher definitiv in der Verfügung nichts zu suchen.

Unter „bisherige Erfahrungen" führte die Polizeidirektion auf knapp acht Seiten diverse Ereignisse seit dem Jahr 2002 auf, die in den Kontext der Anti-Atom-Proteste gestellt werden: Diverse Sitz- und Stehblockaden hätten stattgefunden; 2008 hätten sich daran sogar Bundestagsabgeordnete beteiligt. Diese Blockade habe sich über zwei Tage hingezogen, andere bis spät in die Nacht gedauert. Einsatzfahrzeuge seien mit Wollknäueln eingesponnen und auch Ankettaktionen seien mehrfach erfolgreich betrieben worden. „Obwohl im Herbst 2007 kein Castor-Transport stattfand, kam es am 08.11.2007 zu einer Schülerdemonstration in Lüchow." Teilweise sei es am Rande solcher Aktionen zum Abschießen von Feuerwerkskörpern, zu „vereinzelten Steinwürfen", zum Anbringen von „Schienenhemmschuhen" gekommen.

Erwartungsgemäß erwähnte diese Gefahrenprognose nicht, wie oft die Polizei im Verlauf dieser Jahre unverhältnismäßig und rechtswidrig Gewalt angewendet hat. Wiederholt hat das Oberlandesgericht Celle entschieden, dass Einkesselungen und willkürliche Festnahmen größerer Gruppen keine zulässigen Maßnahmen der Polizei im Umgang mit Versammlungen sind: Als rechtswidrig eingestuft wurden der Karwitzer Kessel 1996, der Langendorfer Kessel 1997, die Festnahmen in Aljarn und Hitzacker 2001, der Kessel auf dem Gelände der Freien Schule in Hitzacker 2002, die Einkesselung in Grippel und die des Dorfes Laase 2003.

Feindbild „Schotterer"

Die „Gewaltbereitschaft", so gestand die Polizeidirektion im gleichnamigen Kapitel ihrer Verfügung zwar ein, habe wie auch die Aggressivität

„insgesamt quantitativ abgenommen“. Gleich im Anschluss an diesen Befund postulierte sie jedoch, dass seit 2008 eine „gesteigerte Gewaltbereitschaft zumindest gegen Sachen“ zu verzeichnen sei. Diese wurde hergeleitet aus diversen (angeblichen) Versuchen seit 2003, Straße oder Bahnstrecke zu unterspülen, aus einzelnen Brandanschlägen auf bahntechnische Einrichtungen, die allerdings nicht im Kontext von Versammlungen standen, aus Beschädigungen der Umzäunung des Erkundungsbergwerks und ähnlichen Ereignissen.

Als Beleg für die aktuelle Gewaltbereitschaft führte die Polizeidirektion den Aufruf „Castor schottern“ auf. Atomkraftgegner hatten aufgerufen, massenweise Schottersteine aus dem Bahngleis zu entfernen, das zwischen Lüneburg und Dannenberg nur für den Castortransport genutzt wird. Diese Aktion Zivilen Ungehorsams betonte explizit, dass keine Gewalt angewendet und die Polizei nicht angegriffen werden sollte. Auch in diesem Fall begründete die Polizeidirektion die angebliche Gefährdung vor allem mit der breiten Unterstützung der Aktion: Schon „200 Gruppen und 652 Einzelpersonen“ hätten den auch in der Presse verbreiteten Aufruf unterzeichnet (bis zum 5. November 2010 waren es: 283 Gruppen und 1.497 Einzelpersonen), darunter auch Bundestags- und Landtagsabgeordnete, Gewerkschafter, Künstler und Professoren.

Schon das in der Allgemeinverfügung ausgesprochene Versammlungsverbot stand für eine unzulässige Einschränkung der Grundrechte auf Versammlungs- und Meinungsfreiheit. Nicht tatsächliche Anhaltspunkte auf einen insgesamt unfriedlichen Verlauf der Demonstrationen begründeten das Verbot. Der eigentliche Grund für die Außerkraftsetzung der Grundrechte auf Versammlungs- und Meinungsfreiheit wurde darin gesehen, dass „zu erwarten (ist), dass die Proteste und verschiedenen Aktionen nicht nur von einer kleinen Gruppe getragen werden, sondern auch von einer bundesweiten Protestszene.“

Maßlose polizeiliche Gewalt gegen Schotterer

Vor Ort reichten die Versammlungsverbote weit über die in der Allgemeinverfügung benannten Räume hinaus. Versammlungen wurden außerhalb der 50-Meter-Grenze angegriffen. Wie selbstverständlich ging die Polizei davon aus, dass es jedem/r BürgerIn untersagt sei, Straßen und Schienen auch nur zu überqueren. Auch die angemeldeten Veranstaltungsorte und Mahnwachen außerhalb der Verbotszone waren folglich fast unerreichbar.

Schon in der Allgemeinverfügung war unterschieden worden zwischen unerwünschten Protesten und Sitzblockaden einerseits und „Straftaten“ andererseits, die angeblich im Rahmen der Aktion „Castor? Schottern!“ stattfinden würden. Tatsächlich war aber auch diese Aktion symbolisch angelegt, weil eine tatsächliche Gefährdung des Schienenverkehrs auf einer ständig bewachten und überprüften Strecke, die einzig für den Castortransport zur Verfügung steht, gar nicht möglich ist. Sie war bar jeder Heimtücke oder Gefährdung für die Sicherheit. Wie bei den Sitzblockaden, wollten die Protestierenden auf die Schiene vordringen, sich aber nicht hinsetzen, sondern Steine aus den Gleisen sammeln.

Den vielen großen Gruppen, die sich ab Sonntag früh in der Göhrde – zwischen Lüneburg und Dannenberg – von Nord und Süd durch den Wald wandernd – der Schiene näherten, begegnete die Polizei sofort mit massiver Gewalt, wenn sie in die Nähe der Bahnlinie kamen. Ohne jede Vorwarnung setzte sie Schlagstöcke, Gas- und Pfefferspray sowie Wasserwerfer ein und ging auch mit Pferden gegen die Protestierenden vor. Dies geschah selbst dann, wenn sie sich noch außerhalb der 50-Meter-Grenze aufhielten. Ihre Versammlungen wurden nicht als solche behandelt. Das Recht auf körperliche Unversehrtheit wurde missachtet. Sie wurden weder aufgefordert, außerhalb der Verbotszone zu bleiben, noch wurden ihre Versammlungen für aufgelöst erklärt. Der Einsatz von Gewaltmitteln wurde nicht angekündigt. Noch auf Menschen, die auf dem Boden lagen, wurde eingeschlagen oder -getreten. An vielen Stellen konnte beobachtet werden, wie Polizeieinheiten brüllend und Schlagstock schwingend in den Wald rannten. Ganze Gleisabschnitte lagen nach dem Abschuss von CS-Kartuschen zeitweise unter einer Gaswolke. Dieses Gas behinderte auch die PolizeibeamtInnen selbst. Pfefferspray wurde aus kurzer Distanz in Gesichter gesprüht. 2.190 Kartuschen mit synthetischem Pfefferspray hat die Bundespolizei in diesen Tagen verschossen. Schlagstöcke wurden gezielt auf Knöchel eingesetzt.

Die Polizei versuchte ihr Vorgehen nachträglich mit der Behauptung zu rechtfertigen, es hätte sich um „eine große Anzahl extrem gewaltbereiter Autonomer“ gehandelt.[2] Dass das der Realität nicht entspricht, zeigt unter anderem folgendes Beispiel: Eine Polizeieinheit aus Schleswig-Holstein begleitete eine große Gruppe Demonstrierender von dem Dorf Govelin aus eine knappe Stunde quer durch den Wald. Der zu-

2 Elbe Jeetzel Zeitung v. 8.11.2010

nächst gewählte Abstand ließ sich im Wald nicht lange einhalten, so dass PolizistInnen und AtomkraftgegnerInnen bald gemeinsam, Schulter an Schulter, weiterliefen. Es erfolgten keine Angriffe oder Übergriffe. Als sich diese Gruppe allerdings der 50-Meter-Verbotszone näherte, wurde sie von einer anderen Einheit, einer baden-württembergischen, unvermittelt mit Schlagstöcken und Pfefferspray traktiert.

Räumung der Sitzblockaden

Neben diesem Protest waren die großen Sitzblockaden auf der Schiene und auf der Straße angekündigt. Gemäß der Klassifikation, auf die sich Politik und Polizei bereits in der Allgemeinverfügung festgelegt hatten, waren hier eher die „guten" BürgerInnen beteiligt, deren Protest zumindest in Grenzen zu akzeptieren sei. Das ändert nichts daran, dass auch diejenigen, die sich an Blockaden beteiligen wollten, zunächst mit unverhältnismäßiger Gewalt angegangen wurden, als sie am Sonntag Nachmittag versuchten, die Schiene bei Harlingen zu betreten. Eine Frau wurde von einem Polizeipferd verletzt und musste ins Krankenhaus gebracht werden. Andere wurden von Schlagstöcken getroffen. Das polizeiliche Vorgehen änderte sich jedoch, nachdem sich die Protestierenden auf den Schienen festgesetzt hatten. Die Sitzblockade wurde nun akzeptiert und über Stunden konnten Bürger und Bürgerinnen ungehindert kommen und sich dazusetzen. Sie wurden nicht aufgefordert, dies zu unterlassen oder darüber belehrt, dass dies eine Straftat sei. Gewaltmittel wurden nicht angedroht. Scheinbar wurde das Versammlungsrecht, sogar entgegen der Allgemeinverfügung, auf den Schienen gewährt. Aber eben nur hoheitlich toleriert, nachdem BürgerInnen es sich zuvor erkämpft hatten.

Dass auch dieser Schein noch trügt, zeigt das weitere polizeiliche Vorgehen. Zwar führte die Polizei großzügig Gespräche mit der Bürgerinitiative und den OrganisatorInnen der Blockade über das Vorgehen bei der Räumung: Die Bürger sollten weggetragen werden. Man wollte sogar auf die Feststellung der Personalien verzichten. Gleichzeitig betrieb die Polizei jedoch ihre eigene Planung und setzte diese noch in der Nacht zum Montag um, ohne auf die körperliche Unversehrtheit der Protestierenden Rücksicht zu nehmen. Wer sich den ganzen Weg zur Gefangenensammelstelle tragen lassen wollte, dem wurden extrem schmerzhafte Polizeigriffe angedroht. Die Gefangenensammelstelle selbst muss als geplante und systematische Körperverletzung gewertet werden. In einer Wagenburg aus Polizeifahrzeugen sollten die BürgerInnen den Rest der

Nacht bei erheblichen Minustemperaturen unter freiem Himmel ausharren. Nach einiger Zeit bot ihnen die Polizei ein merkwürdiges „Geschäft“ an: Man könnte sie in die – warme – Gefangenensammelstelle in Lüchow verbringen, wenn sie vorher ihre Personalien angäben. Auch der verfassungsrechtlich verbürgte Richtervorbehalt bei Freiheitsentziehungen wurde wieder einmal übergangen. Es wurde kein Richter herbeigeholt, um über die Rechtmäßigkeit der Ingewahrsamnahme zu entscheiden.

Ähnlich erging es der großen Sitzblockade vor dem Zwischenlager, die dort seit Sonntag ausharrte. Die TeilnehmerInnen der Aktion X-tausendmal-quer galten als „friedlich“. Sie blieben trotz bitterer Kälte bis in die frühen Morgenstunden des Dienstags sitzen. Dann wurden auch sie geräumt. Anfangs und solange die Presse dort wachte, wurde überwiegend freundlich und verhältnismäßig weggetragen. Je mehr die Bundespolizei zum Einsatz kam, desto ruppiger wurde die Räumung. Später musste immer häufiger beobachtet werden, dass Gliedmaßen verdreht, Personen geschlagen oder an den Rand geworfen wurden.

Dieselben Leute, die zuvor bei der Aktion „Castor? Schottern!“ mitgemacht hatten, galten der Polizei bei diesen Blockaden als „gute“ (wenn auch kritische) BürgerInnen und erfuhren nun eine zumindest tendenziell andere Behandlung. Die BürgerInnen vor Ort jedoch machten diese Unterscheidung nicht mit, sondern beteiligten sich an allen Protestformen und freuten sich über jede Verzögerung des Transportes. Die Bauern der Region unterstützten die Aktionen überall im Landkreis durch Treckerblockaden, die die Nachschubwege der Polizei erheblich behinderten.

Immer wieder haben DemonstrationsbeobachterInnen, Angehörige des Ermittlungsausschusses und RechtsanwältInnen die Erfahrungen gemacht, dass die Polizei nicht zu Auskünften bereit war. Als Begründung für Absperrungen war zu hören: „Da ist die Transportstrecke; für Grundrechte gibt es jetzt keine Zeit mehr … die Polizeibeamten sind müde und da können wir nicht noch auf Grundrechte Rücksicht nehmen … wir wollen zumindest nicht viele Demonstrierende zu den angemeldeten Mahnwachen lassen … wir tun nur, was die Einsatzführung gesagt hat …“

Polizeiliche Maßnahmen

Einige weitere Verletzungen von Grund- und Menschenrechten können an dieser Stelle nur benannt werden.

- So ist am Dienstag (9. November) ein professioneller Kletterer, der sich an einen Baum gekettet hatte, ohne Vorwarnung in vier Metern

Höhe mit Reizgas angegriffen worden. Er fiel aus dieser Höhe vom Baum und erlitt eine Fraktur im Brustwirbelbereich.

- Der Republikanische Anwältinnen- und Anwälteverein (RAV) berichtet, dass Polizeibeamte am Montag (8. November) auf drei Höfen in Grippel, Zadrau und Langendorf ohne richterliche Anordnung die Scheunengelände durchsuchten. Zumindest in Grippel waren die Beamten auch gegenüber den Rechtsanwälten weder zu einer Begründung noch zu einer Erörterung des polizeilichen Vorgehens bereit. Sie waren vermummt und nicht gekennzeichnet.
- Bereits im Vorfeld der Proteste waren fünf AtomkraftgegnerInnen zu einer präventiven erkennungsdienstlichen Maßnahme vorgeladen worden, bei der sie nicht nur Fingerabdrücke abgeben, sondern sich auch körperlich vermessen lassen sollten.

Begleiterscheinungen der polizeilichen Einsätze im Wendland waren auch diesmal die Amtshilfen der Bundeswehr und die Präsenz ausländischer Polizisten (siehe Kasten auf S. 79). Im Kontext der Versammlungen setzte die Polizei ferner Drohnen ein – angeblich nur, um Überblicksaufnahmen vom Demonstrationsgeschehen zu machen. Allerdings erlauben die Videokameras dieser unbemannten Kleinflugzeuge auch das Heranzoomen einzelner Personen.[3]

Insgesamt lässt sich festhalten, dass die Grundrechte als Grundrechte aller Bürger und Bürgerinnen über Tage außer Kraft gesetzt waren. Nicht das Grundgesetz und die Menschenrechte bestimmten den Umgang, sondern die Durchsetzung einer Politik, die den Willen der Bürger ignoriert und Interessen der Atomlobby zum Maßstab macht. Die Ignoranz der Mächtigen wurde auch daran deutlich, dass nur wenige Stunden nach den Protesten das Landesamt für Bergbau, Energie und Geologie in Hannover den Sofortvollzug der Erkundung des möglichen Endlagers Gorleben angeordnet hat.

Versagt hat an erster Stelle die Politik. Eine Politik, die nur mit massiven Gewaltmitteln gegen „seine“ Bürger durchgesetzt werden kann, ist verfehlt. Versagt hat aber auch die Polizei, die bereit war, ihre Bindung an ein „rechtsstaatliches“ Vorgehen auszusetzen, um einen Transport zu gewährleisten, der mit verhältnismäßigen Mitteln kaum, allenfalls mit sehr viel mehr Zeit hätte durchgeführt werden können. Die Polizeibeamten und -beamtinnen wurden in diesem Einsatz politisch missbraucht,

3 siehe die Meldungen unter Inland aktuell auf S. 86 ff.

und sie ließen sich missbrauchen. Viele von ihnen scheinen noch immer zu glauben, Befehl sei Befehl und sie hätten ohne eigene Gewissensanstrengung zu gehorchen. Schlimmer noch, sie glauben, diese Haltung hätten auch die BürgerInnen gegenüber der Polizei einzunehmen. Bürger und Bürgerinnen dagegen haben gezeigt, dass es Hoffnung gibt auf einen Souverän, der die Dinge nicht in den Händen der PolitikerInnen belässt, sondern seine Anliegen selbst in die Hand nimmt.

Polizeitourismus im Wendland

Dass bei größeren Demonstrationen auch PolizistInnen aus dem Ausland zugegen sind, ist mittlerweile keine Seltenheit mehr. Bei den Protesten gegen die Castor-Transporte 2010 fiel insbesondere ein Beamter der Compagnies Républicaines de Sécurité (CRS), der Bereitschaftseinheiten der französischen Police Nationale, auf, der, wie Fotos beweisen, nicht nur zuschaute, sondern am Sonntag (7. November) beim Einsatz gegen „Schotterer" mit seinem Teleskop-Schlagstock tatkräftig mitmischte und den Ruf der CRS als Prügeltruppe bestätigte. Bundesregierung und Polizeidirektion Lüneburg behaupteten zunächst, nichts vom Einsatz ausländischer Polizei zu wissen.

Erst auf Nachfragen im Bundestag lieferte das Bundesinnenministerium (BMI) beschönigende und unvollständige Informationen zur Präsenz ausländischer Beamter: Vom 4. bis 9. November seien danach zwei CRS-Beamte „zur Einsatzbeobachtung innerhalb der Bundespolizei eingesetzt" worden – der eine unbewaffnet in einer „stationären Befehlsstelle", der andere – ausgerüstet mit Pistole und Schlagstock – in einer Beweissicherungs- und Festnahmeeinheit. Die genannten Fotos würden ihn „bei der Vornahme von Unterstützungsmaßnahmen anlässlich der Räumung" der Gleise zeigen. Die Fotos gäben die „sehr dynamische Einsatzsituation" und die „massiven Ausschreitungen" nicht wieder. Art. 24 des Prümer Vertrags erlaube auch die Ausübung hoheitlicher Befugnisse in einem anderen Vertragsstaat. Zusätzlich zu diesen beiden Beamten, die in ihrer eigenen Uniform auftraten, sei ein französischer Verbindungsbeamter in Zivil bei der Gesamteinsatzleitung in Lüneburg zugange gewesen.

„Verschiedene Befehlsstellen und Führungsstäbe im Einsatzraum besucht" hätten auch ein Beamter der türkischen Polizei und einer der russischen Grenzpolizei, die am aktuellen Ratsanwärterlehrgang der Bundespolizei teilnehmen. Vom 5. bis 7. November hätten ferner drei Beamte der niederländischen Marechaussee „die Gesamteinsatzleitung in Lüneburg … besucht" und seien „durch Beamte der Bundespolizei betreut und begleitet" worden. Nicht in der Aufzählung des BMI enthalten sind die polnischen und kroatischen Polizisten, die – ebenfalls in ihrer heimatlichen Uniform – im Wendland zu sehen waren. Laut Aussage des Sprechers des niedersächsischen Innenministeriums seien sie „bei den niederländischen Beamten angemeldet gewesen.

Quellen: BT-Drs. 17/4323 v. 21.12.2010, BT-Innenausschuss-Drs. 17 (4) 157, dpa-Meldung v. 13.11.2010

Netz mit Webfehlern

Europas DNA-Datenbankenverbund

von Eric Töpfer

Die europaweite Verknüpfung polizeilicher DNA-Datenbanken schreitet voran. Wirklich reibungslos funktioniert der grenzüberschreitende Informationsaustausch, der auf eine Initiative des ehemaligen Bundesinnenministers Otto Schily aus dem Jahr 2003 zurückgeht, bislang allerdings nicht.

Stichtag ist der 26. August 2011: Bis dahin soll die Vernetzung der nationalen DNA- und Fingerabdruckdatenbanken sowie der Kraftfahrzeugregister aller 27 EU-Mitgliedstaaten abgeschlossen sein; so gibt es der Ratsbeschluss der Europäischen Union (EU) 2008/615/JI zur „Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere des Terrorismus und der grenzüberschreitenden Kriminalität“ vor.[1] Gemäß den Prüm-Beschlüssen, mit denen das 2005 geschlossene Abkommen in den EU-Rahmen überführt wurde, sollen europäische Polizeien die entsprechenden Datenbestände anderer Staaten automatisch durchsuchen können. Mit der Teilautomatisierung der Rechtshilfe würden sich lange Dienstwege verkürzen auf die Anfrage bei nationalen Kontaktstellen, die als elektronische Schnittstellen für die Datenabfrage bei den Partnerländern zuständig sind. In Deutschland übernimmt das Bundeskriminalamt diese Funktion, bei Kfz-Registerdaten zusammen mit dem Kraftfahrzeugbundesamt. Erst im Falle eines „Treffers“ müssten auf dem Wege klassischer Rechtshilfeersuchen weitere Informationen angefragt werden.

Doch Mitglied des Prüm-Netzwerkes zu werden, ist ein komplexer politischer und technischer Prozess: Nationales Recht ist anzupassen und die zentralen Kontaktstellen sind zu benennen. Mitunter müssen

1 Die „Prüm-Beschlüsse“ sind mittlerweile auch auf die Nicht-EU-Mitglieder Norwegen und Island ausgedehnt, vgl. Amtsblatt der EU (ABl. EU) L 353/1 v. 31.12.2009.

die abzufragenden Datenbanken erst eingerichtet und an S-TESTA, das gesicherte Netzwerk der europäischen Verwaltung, angeschlossen werden. Ein kleinster gemeinsamer datenschutzrechtlicher Nenner ist zu garantieren. Suchkapazitäten müssen geklärt und technische Spezifikationen erfüllt werden. Fragebögen müssen beantwortet und Testläufe erfolgreich durchgeführt worden sein. Schließlich ist eine Vor-Ort-Evaluation zu bestehen, bevor schlussendlich der Ministerrat der EU einstimmig beschließen muss, dass ein Mitgliedstaat mit dem automatisierten Datenaustausch starten kann.

Vor dem Hintergrund dieses aufwändigen Prozederes verwundert es nicht, dass bereits jetzt feststeht, dass der Termin am 26. August nicht zu halten ist. Im Oktober 2010 funktionierte, so eine Umfrage der belgischen Ratspräsidentschaft, nur in zehn Staaten der Austausch von DNA-Profilen, in sieben jener von Informationen aus Fahrzeugregistern, und nur fünf Länder waren in der Lage, Fingerabdrücke elektronisch abzugleichen. Dennoch verkündeten die Belgier hoffnungsfroh, dass „die meisten Länder überzeugt sind, für alle drei Datenkategorien die Deadline zu halten", mussten aber zugleich einräumen, dass mindestens sechs Länder Ende August weder DNA- noch Fingerabdruckdatenbanken an das Prüm-Netzwerk angeschlossen haben werden. Fünf weitere Länder sehen sich außerstande, bis zum Stichtag ihre Kfz-Register grenzüberschreitend zu vernetzen.[2] In Reaktion auf die Schwierigkeiten mahnte der Rat der Innen- und Justizminister im November 2010, „dass die betreffenden Mitgliedstaaten ihre Anstrengungen verstärken sollten und dass die Mitgliedstaaten, die die Prümer Beschlüsse bereits anwenden, sich noch mehr bemühen sollten, technische Unterstützung zu leisten."[3]

Im Bereich DNA waren es im Oktober 2010 Deutschland, Finnland, Frankreich, Luxemburg, Niederlande, Österreich, Rumänien, Slowenien, Spanien und Bulgarien, die zum Prüm-Netzwerk gehörten, sowie – noch in der Testphase – Belgien. Die Slowakei trat dem Informationsverbund im November bei.[4] Doch selbst zwischen diesen zwölf Ländern ist es keinesfalls so, dass jedes Land Zugriff auf die DNA-Datenbanken aller Partner hat. Die Spinne im Netz der europäischen DNA-Datenbanken ist gegenwärtig Österreich, das allein zu allen anderen Ländern einen direk-

2 Ratsdok. 15567/10 v. 28.10.2010
3 Ratsdok. 15848/10 v. 8.11.2010
4 Ratsdok. 14606/10 v. 29.10.2010 verabschiedet auf dem Ratstreffen vom 8.11.2010

ten Draht hat. Deutschland hingegen kann nur mit fünf anderen Ländern DNA-Profile austauschen.[5] Eine deutsch-französische „Achse", ansonsten Motor der europäischen Integration, gibt es zum Beispiel nicht, was den bayerischen Innenminister Joachim Hermann bereits im August 2009 zu dem verärgerten Kommentar veranlasste, dass der Nachbar die Strafverfolgung in Europa „unnötig" behindere.[6]

Die Gründe für die schleppende Vernetzung sind vielfältig: Schwierigkeiten, politische Mehrheiten für die Anpassung des nationalen Rechts an die Vorgaben von Prüm zu mobilisieren, Kompetenzstreitigkeiten zwischen Behörden bei der Benennung der Nationalen Kontaktstelle, Ärger bei organisationsinternen Neustrukturierungen, die aus der Internationalisierung resultieren, sowie personelle und finanzielle Engpässe. Die größte Herausforderung scheinen aber technische Probleme zu sein. Mit ihnen kämpfen nach eigenen Angaben mindestens zehn Länder: Hardware oder Softwarekomponenten erweisen sich als inkompatibel oder der Anschluss ans S-TESTA-Netzwerk gelingt nicht reibungslos; mitunter müssen existierende Systeme komplett abgelöst werden. Durchschnittlich soll der Beitritt zum Prüm-DNA-Verbund knapp zwei Millionen Euro kosten, so das Ergebnis der belgischen Umfrage.[7] Allerdings dürften die Kosten insbesondere für Länder wie Italien, Griechenland, Malta oder Irland, die vor 2008 keine nationale DNA-Datenbank betrieben, weit höher liegen.[8]

Abhilfe schaffen sollen finanzielle Hilfen durch die EU-Kommission, ein „Helpdesk" bei Europol sowie eine Expertengruppe des deutschen Bundeskriminalamtes. Letztere eilt als „Mobiles Kompetenzteam" durch Europa, um überforderten Partnern mit Rat und Tat zur Seite zu stehen. Wie erfolgreich diese Maßnahmen sind, wird sich in den nächsten Monaten zeigen. Ab März 2011 wird eine Welle von abschließenden Evaluationen erwartet, die ihren Höhepunkt vermutlich in letzter Minute im Sommer des Jahres erreichen soll. Dass die absehbare Arbeitsbelastung allerdings von den wenigen Gutachtern in so kurzer Zeit zu stemmen sein wird, darf bezweifelt werden. Und dass die Evaluationen, die

5 Ratsdok. 5904/5/10 v. 17.9.2010
6 Focus Nr. 35/09 v. 24.8.2009
7 Ratsdok. 14918/10 v. 19.10.2010
8 Prainsack, B.; Toom, V.: The Prüm Regime. Situated Dis/Empowerment in Transnational DNA Profile Exchange, in: British Journal of Criminology 2010, No. 10, pp. 1117-1135 (1121)

Grundlage für das grüne Licht des Rates der EU zum Start des Datenaustausches sind, schließlich positiv ausfallen, ist keinesfalls garantiert: „Das Prüm-Prozedere allein für sich ist ein zeitraubender Prozess; sollte es unverändert bleiben, scheint es äußerst unwahrscheinlich, dass alle Mitgliedstaaten bis zum 26. August 2011 zum Wirkbetrieb übergehen können. Selbst wenn alle anderen Schwierigkeiten – seien sie technischer, organisatorischer oder finanzieller Natur – gelöst wären, könnte sich dies [der absehbare Stau an Evaluationen] als eine der größten zu bewältigenden Herausforderungen bei der Umsetzung der Prüm-Beschlüsse erweisen", warnt der Bericht der Belgier.[9] Nach den deutlichen Problemen mit der Installation von Europols Computersystemen und dem Schengen-Informationssystem II sieht es also sehr danach aus, als ob hochtrabende Pläne der europäischen Polizeikooperation erneut durch die Komplexität technischer Großprojekte ausgebremst werden.

Sechs Loci, ein Treffer?

Vermutlich ist es aber nur eine Frage der Zeit, bis die Anlaufschwierigkeiten bei der Vernetzung der DNA-Datenbanken gelöst sind und das Prüm-Netzwerk voll operabel ist. Wesentlich folgenreicher für die zukünftige Praxis dürfte ein anderes Problem sein. Kapitel 1 des Anhangs zum Ratsbeschluss 2008/616/JI, der die technischen Details der Umsetzung des Prüm-Beschlusses ausführt, definiert die Regeln für den Austausch von DNA-Daten wie folgt: Übermittelt werden Zahlenpaare, die die Allele – Varianten eines Gens an einer bestimmten Stelle auf einem Chromosom – repräsentieren. Übermittelte DNA-Profile müssen Allelwerte für mindestens sechs der sieben Genstellen (sogenannte „Loci") enthalten, die das „European Standard Set of Loci" (ESS, im Folgenden auch kurz „Europäischer Standardsatz") beinhaltet. Zusätzlich können sie je nach Verfügbarkeit weitere Loci – erlaubt sind insgesamt 24 – oder Leerfelder enthalten. Zwar wird empfohlen, „alle verfügbaren Allele in der Indexdatenbank für DNA-Profile zu speichern und für die Suche und den Abgleich zu verwenden", um die Treffergenauigkeit zu erhöhen. Allerdings gilt bereits die Übereinstimmung von sechs Loci als „Treffer".[10]

Doch mit der wachsenden Zahl der Mitglieder im Prüm-Netzwerk wächst das Risiko von „Zufallstreffern". So rechnete man vor dem

9 Ratsdok. 14918/10 v. 19.10.2010
10 ABl. EU L 210/20 ff. v. 6.8.2010

deutsch-niederländischen Massenabgleich von DNA-Profilen im Sommer 2008 mit 190 solcher falschen Treffer.[11] Zahlen zur tatsächlichen Bilanz wurden bis dato nicht veröffentlicht, und die Bundesregierung behauptet, dass hierzu keine Statistiken geführt werden.[12] Vor dem Hintergrund der sich abzeichnenden Schwierigkeiten empfahl die „Arbeitsgruppe Informationsaustausch" des Rates, „dass die nationalen DNA-Experten der anfragenden Mitgliedstaaten eine zusätzliche Prüfung solch möglicher Treffer vornehmen sollen, bevor sie das Ergebnis an andere Polizei- oder Justizbehörden übermitteln". Es gelte, „die Balance zu wahren zwischen der Bereitstellung von Ermittlungshilfen für die Strafverfolgung, die das Ziel des Prümer Datenaustausches war, und der Vermeidung unnötigen Aufwandes bei der Nachverfolgung falscher Treffer."[13]

Bekannt ist das Problem seit längerem. Bereits 2005 diskutierten Forensiker der European DNA Profiling Group (EDNAP)[14] und der DNA-Arbeitsgruppe des European Network of Forensic Science Institutes (ENFSI)[15] auf einem gemeinsamen Treffen die Möglichkeit, den Europäischen Standardsatz aus dem Jahr 2001 um weitere Loci zu erweitern.[16] Nachdem auf einem ENFSI-Treffen im Jahr 2008 die Erweiterung um fünf Loci beschlossen und eine entsprechende Vorlage erstellt worden war, verabschiedete der Rat der Innen- und Justizminister Ende November 2009 eine entsprechende Entschließung. Allerdings handelt es sich dabei im Gegensatz zu Beschlüssen des Rates nur um unverbindliches „soft

11 Van der Beek, K.: Exchange of DNA-profiles by the Treaty of Prüm, www.dna-conference.eu/ppt/Van%20der%20Beek.pdf

12 BT-Drs. 16/14150 v. 22.10.2009

13 Ratsdok. 8505/09 v. 15.4.2009

14 EDNAP wurde 1988 auf Initiative des „London Metropolitan Police Forensic Science Laboratory" als informelles Netzwerk forensischer Genetiker gegründet mit dem Ziel, die DNA-Analyse für die Strafverfolgung zu harmonisieren. Seit 1991 ist EDNAP formelle Arbeitsgruppe der „International Society for Forensic Genetics", die mit Sitz in Mainz die Interessen ihrer mehr als 1.100 Mitglieder aus 60 Ländern vertritt. Damit ist EDNAP vereinsrechtlich organisiert, übt aber – u.a. gefördert mit EU-Geldern – erheblichen Einfluss auf die offizielle Entwicklung der DNA-Analyse aus, vgl. www.isfg.org/EDNAP.

15 ENFSI wurde 1995 als Netzwerk staatlicher forensischer Institute gegründet. Gegenwärtig hat die Organisation 58 institutionelle Mitglieder in 33 Ländern, u.a. das Kriminaltechnische Institut beim Bundeskriminalamt. Inzwischen müssen ENFSI-Mitglieder nicht mehr notwendigerweise staatliche Einrichtungen sein. Es reicht, wenn sie einen „glaubwürdigen Status" in ihrem Heimatland genießen und die Qualität ihrer Arbeit nach ISO-Norm 17023 zertifiziert ist (oder werden soll); vgl. www.enfsi.eu.

16 Gill, P. et al.: The Evolution of DNA Databases – Recommendations for new European STR loci, in: Forensic Science 2006, No. 156, pp. 242-244

law“, mit dem den Mitgliedstaaten lediglich empfohlen wird, „den neuen Europäischen Standardsatz so bald wie möglich, spätestens jedoch 24 Monate nach der Annahme dieser Entschließung, anzuwenden“.[17]

Umgangen hat man damit eine Änderung der Prüm-Beschlüsse, die insbesondere nach Inkrafttreten des Lissabon-Vertrages und der neuen Mitspracherechte des Europaparlamentes im Bereich der Polizeikooperation politisch kaum durchsetzbar schien. Gestritten wird seither um den Status der Entschließung. So behauptet die niederländische Delegation in der „Arbeitsgruppe Informationsaustausch“ in einer Note vom Juni 2010, dass die Prüm-Beschlüsse ausdrücklich zur Umsetzung eines neuen Europäischen Standardsatzes verpflichten.[18] In der deutschen Version des bemühten Rechtsaktes heißt es allerdings: „Jeder Mitgliedstaat sollte, so bald wie praktisch möglich, die Loci eines neuen ESS, der von der EU übernommen wurde, einführen.“[19] Eine Soll-Vorschrift, die sich zudem an der praktischen Realisierbarkeit orientiert. Eben hier liegt der Haken, da die Anpassung der jeweiligen nationalen Infrastruktur an den neuen Europäischen Standardsatz zumindest bei einigen Mitgliedstaaten mit erheblichem technischem und finanziellem Aufwand verbunden wäre.

Entsprechend überrascht es nicht, wenn in der Auswertung der oben zitierten belgischen Umfrage zu lesen ist: „Ein Mitgliedstaat zögert, all seine Profile für den Datenaustausch zugänglich zu machen, da dies dazu führen könnte, dass eine exzessiv hohe Zahl von Profilen aufgrund falscher Treffer ins Ausland übermittelt wird, was datenschutzrechtliche Probleme aufwirft.“[20] Sehr wahrscheinlich handelt es sich bei dem zögerlichen Land um Großbritannien mit seiner knapp sechs Millionen Einträge schweren „National DNA Database“.[21] Im Zeichen von Wirtschaftskrise und drastischer Sparpolitik hält das Königreich wohl lieber die Mehrheit seiner gespeicherten DNA-Profile vom Prüm-Netzwerk fern, anstatt technisch von gegenwärtig zehn auf zwölf Loci umzurüsten. Zumindest vorübergehend scheint der Ausbau der pan-europäischen Überwachungsmaschinerie also an seine technischen und organisatorischen Grenzen zu stoßen. Vielleicht Zeit, um beim atemlosen Ausbau internationalisierter biometrischer Kontrolle kurz Luft zu holen und kritisch Bilanz zu ziehen.

17 ABl. EU C 296/1 v. 5.12.2009
18 Ratsdok. 11084/10 v. 16.6.2010
19 § 1.1 in Kapitel 1 des Anhangs zum Ratsbeschluss 2008/616/JI
20 Ratsdok. 14918/10 v. 19.10.2010
21 National DNA Database Statistics, www.npia.police.uk/en/13338.htm

Inland aktuell

Videoüberwachung von Demonstrationen

Gleich drei neuere Gerichtsentscheidungen beschäftigen sich mit der Zulässigkeit der Kameraüberwachung von Versammlungen. Bereits am 21. August 2009 stellte das Verwaltungsgericht Münster fest, dass die polizeiliche Videobeobachtung einer friedlichen Demonstration rechtswidrig war.[1] Das Oberverwaltungsgericht Nordrhein-Westfalen bestätigte diese Entscheidung in einem Beschluss vom 23. November 2010.[2] Am 5. Juli 2010 kam das Verwaltungsgericht Berlin zu einem nach Argumentation und Ergebnis ähnlichen Urteil.[3]

Alle drei Gerichte stellen fest, dass die Beobachtung einer Versammlung durch die Polizei mit Hilfe von Kameras sowohl einen Eingriff in die Versammlungsfreiheit als auch die informationelle Selbstbestimmung darstellt. Allein die Anfertigung von Übersichtsaufzeichnungen verbunden mit der technischen Möglichkeit des gezielten Heranzoomens einzelner Versammlungsteilnehmer könne zu einem Gefühl des Überwachtwerdens und damit zu einem Einschüchterungseffekt führen, der potentielle VersammlungsteilnehmerInnen in ihrer inneren Versammlungsfreiheit beeinträchtigen, im schlimmsten Fall sogar von der Teilnahme an einer Versammlung abhalten könne. Für einen solchen Grundrechtseingriff bedürfe es einer ausdrücklichen gesetzlichen Grundlage, die jedenfalls im Falle einer friedlichen Versammlung nicht durch das Versammlungsgesetz gegeben sei.

Nun könnte befürchtet werden, dass es die Bundesländer, auf die durch die Föderalismusreform die Gesetzgebungskompetenz im Bereich des Versammlungsrechts übergegangen ist, in der Hand haben, durch den schlichten Erlass von gesetzlichen Regelungen die umfassende anlasslose Datenerhebung bei Demonstrationen zu ermöglichen. Allerdings hat das Bundesverfassungsgericht in seiner einstweiligen Anordnung vom

1 Verwaltungsgericht (VG) Münster: Urteil v. 21.8.2009, 1 K 1403/08
2 Oberverwaltungsgericht Nordrhein-Westfalen: Beschluss v. 23.11.2010, 5 A 2288/09
3 VG Berlin: Urteil v. 5.7.2010, 1 K 905.09

17. Februar 2009 zum Bayerischen Versammlungsgesetz festgestellt, dass eine solche Regelung einen schweren Grundrechtseingriff darstellt und die entsprechenden bayerischen Normen deshalb vorläufig außer Kraft gesetzt.[4] Die Entscheidung im Hauptsacheverfahren steht noch aus.
(Angela Furmaniak)

Polizeidrohnen im Anflug

Seit 2008 experimentieren einige Landespolizeien mit fliegenden Kameras für den Polizeialltag. Sachsen ließ unter dem früheren Innenminister Albrecht Buttolo (CDU) ein gemeinsames Produkt der Firmen Diehl BGT Defence und Microdrones testen. Nachfolger Markus Ulbig (CDU) verfügte im Herbst die endgültige Anschaffung der Drohne.[5] Damit würde eine Lücke „zwischen den Videoaufnahmen aus einem Polizeihubschrauber und den mobilen/stationären Kameras am Boden" geschlossen. Anwenden will man das unbemannte Flugzeug für die Einsatzführung, die Überwachung und Aufklärung, die Unterstützung von Suchmaßnahmen, für Observationen und die „Dokumentation von Verkehrsmaßnahmen". Niedersachsen, Hessen, Nordrhein-Westfalen und die Bundespolizei haben Drohnen der Firmen EMT, Diehl bzw. Mikrokopter sowie des Konkurrenten AirRobot zu Testzwecken angeschafft.

Zuletzt sorgte eine fliegende Kamera beim Castor-Transport im November für Wirbel.[6] Einsatzleiter Friedrich Niehörster hatte ihre Nutzung zunächst geleugnet. Kritik kam von der Bürgerinitiative Lüchow-Dannenberg und vom niedersächsischen Datenschutzbeauftragten Joachim Wahlbrink: Die Polizei oder der Innenminister müssten vor dem Einsatz Informationen über Sinn und Zweck der Drohne zur Prüfung vorlegen. Mit dem Gerät könnten Fotos und Videoaufnahmen auch von Personen gemacht werden. Niedersachsens Innenministerium behauptete indes, die Drohne liefere bei „Einsätzen in normaler Flughöhe" lediglich Übersichtsaufnahmen. Die Aussage darf angesichts mittlerweile hochauflösender Videotechnik bezweifelt werden. Sie steht zudem im Widerspruch zu den Angaben des sächsischen Innenministeriums, wonach die Videoübertragung „in hoher Qualität" erfolge.

4 Bundesverfassungsgericht: Beschluss v. 17.2.2009, Az.: 1 BvR 2492/08
5 Sächsisches Staatsministerium des Innern: Pressemitteilung v. 23.11.2010; heise-online v. 24.11.2010
6 heise-online v. 16.11.2010; taz v. 17.11.2010; Süddeutsche Zeitung v. 17.11.2010

Wie die Berliner Senatsverwaltung für Inneres am 21. Februar 2011 auf unsere Anfrage bestätigte, verfügt auch die Polizei der Hauptstadt seit 2009 über eine eigene Drohne vom Typ Air Robot. Sie werde zur „luftgestützten fotografischen Dokumentation von Tat- und Ereignisorten" genutzt – so etwa am 24. Januar 2011 wegen eines Tötungsdeliktes in Kreuzberg. Der Einsatz der fliegenden Kamera bei Demonstrationen dürfte allerdings an rechtliche Grenzen stoßen, nachdem das Berliner Verwaltungsgericht die anlasslose Videoüberwachung von Versammlungen untersagt hat.[7]
(Matthias Monroy)

Körpervermessung von CASTOR-GegnerInnen

Fünf Atomkraftgegner, darunter der Kassenwart der Bürgerinitiative Lüchow-Dannenberg, waren im Vorfeld der CASTOR-Proteste von der Polizeiinspektion Lüneburg/Lüchow zu einer so genannten präventiven erkennungsdienstlichen Maßnahme vorgeladen worden: Sie sollten – notfalls auch gewaltsam – dazu gezwungen werden, Finger- und Handkantenabdrücke abzugeben sowie sich im Portrait und im Detail „zum Vermessen von Tätowierungen und anderen Körpermerkmalen wie z.B. Narben" fotografieren zu lassen. Zur „Begründung" zählte die Polizei eine imposante Liste von Ermittlungsverfahren auf – tatsächlich ist aber keiner der Betroffenen deswegen jemals rechtskräftig verurteilt worden! Unverdrossen geht die Polizei aber von einer „großen Rückfallwahrscheinlichkeit" aus; es könne „nicht ausgeschlossen" werden, dass „Sie sich in nächster Zeit erneut strafrechtlich relevant verhalten werden".[8]

Die fünf Betroffenen wollten gegen diese Vorladung rechtlich vorgehen. Nach einer Analyse auf „Legal Tribune Online" dürften ihre Klagen „gute Erfolgsaussichten" haben: Bereits 2007 hatte ein Oberverwaltungsgericht entschieden, dass die Aufzählung von eingestellten Ermittlungsverfahren die Komplettvermessung von Atomkraftgegnern nicht rechtfertigen könne. Die „einschüchternde Wirkung" der geplanten polizeilichen Vermessungen stehe „außer Frage": Die Betroffenen wüssten sich „im Fokus polizeilicher Beobachtung" und würden sich deshalb eine

7 VG Berlin: Urteil v. 5.7.2010, 1 K 905.09, siehe die vorstehende Meldung
8 www.bi-luechow-dannenberg.de/chronologisch/pressemitteilungen/protest-gegen-vorladungen-zur-erkennungsdienstlichen-behandlung

Teilnahme an Demonstrationen „sehr genau überlegen“. Die ED-Behandlung schränke damit die grundrechtlich geschützte Versammlungsfreiheit mittelbar ein. Die geplante körperliche Komplettvermessung sei zudem alles andere als ein „geringfügiger“ Eingriff in das Persönlichkeitsrecht der Betroffenen. Im Ergebnis sei die geplante Maßnahme – ohne den tatsächlichen Bezug auf eine rechtskräftige Verurteilung der Betroffenen im Zusammenhang mit Demonstrationen – schlicht unverhältnismäßig.[9]
(Mark Holzberger)

Kampagne gegen „DNA-Sammelwut“

2011 startet das Gen-ethische Netzwerk (GeN) eine Kampagne gegen die wachsenden DNA-Datenbanken deutscher Polizeibehörden und ihre internationale Vernetzung. 22 Jahre nach der ersten (west-)deutschen DNA-Analyse sind heute mehr als 700.000 Personendatensätze und 180.000 Spuren in der nationalen DNA-Analyse-Datei beim Bundeskriminalamt gespeichert. Diese soll bis zum 26. August 2011 im Rahmen der sogenannten Prüm-Beschlüsse für grenzüberschreitende Datenabgleiche europaweit vernetzt werden. Unter dem Motto „Finger weg von meiner DNA!“ will das GeN daher mit seiner Kampagne die schleichende Normalisierung der Kontrolltechnologien rund um den „genetischen Fingerabdruck“ skandalisieren und den Protest gegen die biopolitische Dimension staatlicher Überwachung wiederbeleben.[10]

Unterstützt durch ein überdimensionales Wattestäbchen, mit dem die Kampagne durch die Lande ziehen wird, soll darauf aufmerksam gemacht werden, dass DNA-Profile nicht selten jenseits rechtlicher Grenzen gespeichert werden, dass das Prinzip der „Freiwilligkeit“ in Verhörsituationen oder bei Massengentests regelmäßig ausgehebelt wird, dass Angehörige sozial schwacher Bevölkerungsgruppen überproportional häufig registriert werden und dass trotz Richtervorbehalt die Verhältnismäßigkeit des Eingriffs häufig fragwürdig ist. Angesichts der Potenzierung der Probleme, die mit der internationalen Vernetzung der DNA-Datenbanken aufgrund unterschiedlicher Datenschutzniveaus droht, plant das GeN, den Protest in europaweiten Aktionen am 26. August gipfeln zu lassen.
(Eric Töpfer)

9 www.lto.de/de/html/nachrichten/1738/polizeiliche-vermessung-von-atomkraftgegnern/
10 Website der Kampagne: www.fingerwegvonmeinerDNA.de

G 10-Maßnahmen 2009

Ende 2010 legte das Parlamentarische Kontrollgremium (PKGr) dem Bundestag seinen Bericht über die Überwachung des Brief-, Post- und Fernmeldeverkehrs durch die Geheimdienste des Bundes im Jahr 2009 vor.[11] Nach § 3 Artikel 10-Gesetz (G 10) dürfen das Bundesamt für Verfassungsschutz (BfV), der Militärische Abschirmdienst (MAD) und der Bundesnachrichtendienst (BND) die Telekommunikation überwachen und aufzeichnen sowie Postsendungen öffnen, wenn ein Anfangsverdacht für bestimmte Staatsschutzstraftaten vorliegt. Im Rahmen seiner „strategischen" Kontrolle darf der BND nach § 5 G 10 zudem die internationalen Telekommunikationsbeziehungen in definierten Gefahrbereichen mittels Suchbegriffen überwachen.

Im ersten Halbjahr 2009 lag die Gesamtzahl der Einzelmaßnahmen bei 65, im zweiten bei 67 Maßnahmen. Der MAD führte nur eine durch. Die Schwankungen zwischen den Halbjahren ergeben sich daraus, dass die Überwachungen jeweils auf maximal drei Monate befristet sind. Sie werden anschließend beendet, verlängert oder es werden neue angeordnet. Gegenüber 2008 hat sich die Zahl – deutlich – um elf pro Halbjahr erhöht. Auch die Zahl der sog. Haupt- und Nebenbetroffenen stieg: 728 im ersten Halbjahr 2009, 1.007 im zweiten (2008: 529; 639). Die Überwachungen wurden schwerpunktmäßig zur Bekämpfung des internationalen Terrorismus eingesetzt, betrafen aber auch „extremistische Bestrebungen" von links, rechts und von Ausländern, Spionage u.a.

Die strategische Kontrolle durch den BND fand in den Gefahrenbereichen „Internationaler Terrorismus", „Proliferation und konventionelle Rüstung" sowie unbefugtes Verbringen von Betäubungsmitteln in die BRD statt. Dabei zeigte sich, dass auch der BND-„Staubsauger" zugespammt wird. Die Anzahl der durch Suchbegriffe erfassten Telekommunikationsverkehre verdreifachte sich von 2.211.790 auf 6.841.725. Als „nachrichtendienstlich relevant" wurden jedoch nur 278 „Treffer" (2008: 394) eingestuft, das sind 0,004 Prozent. Von den 69 relevanten Funden im Bereich Internationaler Terrorismus waren 58 „Webforenerfassungen". Hinsichtlich des Drogenhandels gab es gar keine Treffer. Vier mal wurde die strategische Kontrolle im Zusammenhang mit Piraten auch zum Schutz einer Person im Ausland nach § 8 G 10 angeordnet.

11 BT-Drs. 17/4278 v. 17.12.2010

112 Betroffenen der Einzelmaßnahmen wurde die Überwachung mitgeteilt, bei 238 wurde die Benachrichtigung zurückgestellt. Sieben Betroffene der strategischen Kontrolle wurden informiert.

Anti-Terrormaßnahmen der Geheimdienste 2009

Mit dem Terrorismusbekämpfungsgesetz von 2002 und dessen Ergänzung von 2007 hatten BfV, MAD und BND die Befugnis erhalten, von Luftfahrtunternehmen, Banken, Finanzdienstleistungs-, Post- und Telekommunikationsunternehmen Auskünfte über Kunden und Nutzer einzuholen sowie den sog. IMSI-Catcher zur Ortung und Identifizierung eingeschalteter Mobiltelefone einzusetzen.

Der Ende Dezember 2010 vorgelegte Bericht des PKGr[12] listet 77 Auskunftsverlangen der Geheimdienste des Bundes für das Jahr 2009 auf, davon 72 durch das BfV, vier durch den BND und eines durch den MAD. 55 Mal wurde Auskunft bei Telekommunikationsanbietern eingeholt. Den IMSI-Catcher setzte das BfV 15 Mal, der BND ein Mal ein. Der Bericht zählt 334 Betroffene der Auskunftsverlangen und 26 beim IMSI-Catcher-Einsatz.

2009 wurde 28 Personen mitgeteilt, dass Geheimdienste entsprechende Auskünfte über sie eingeholt oder den IMSI-Catcher gegen sie eingesetzt haben; bei 32 Betroffenen wurde die Mitteilung vorerst zurückgestellt. Bei drei Personen wurde sie endgültig abgelehnt.

Seit die Befugnisse eingeführt wurden, hat sich ihre Nutzung kontinuierlich erhöht. Im Vergleich zu 2002 haben sich die jährlichen Zahlen mittlerweile mehr als verdoppelt, was auch an der Erweiterung der Befugnisse für das BfV im Jahr 2007 liegen wird. Nur bei Postdienstleistern hat es seit der Einführung keinerlei Anfragen gegeben.

In welchem Umfang die Landesämter für Verfassungsschutz Auskünfte verlangt haben, lässt sich anhand des Berichtes nicht mehr vollständig erkennen. Nur elf Bundesländer haben dem PKGr im Jahr 2009 Zahlen mitgeteilt; danach gab es 48 Auskunftsverlangen. Seit einer Gesetzesänderung 2007 sind sie dazu nicht mehr verpflichtet, sofern die jeweiligen Gremien der Landesparlamente die Maßnahmen adäquat kontrollieren.
(beide: Martina Kant)

12 BT-Drs. 17/4277 v. 17.12.2010

Meldungen aus Europa

Grenzüberschreitende Spitzelausleihe

Sieben Jahre lang hat Mark Kennedy alias „Mark Stone“ britische linke Bewegungen infiltriert.[1] Der Verdeckte Ermittler (VE) arbeitete für die „Associaton of Chief Police Officers“ (ACPO), die bis vor kurzem für Scotland Yard die VE-Führung besorgte. Seit Kennedys Enttarnung im Oktober 2010 tragen AktivistInnen auf Indymedia seine Aktionen zusammen. Heraus kam dabei ein Mosaik grenzüberschreitender Bewegungsgeschichte: Der Polizist nutzte die in Großbritannien entstandene weltweite Klimabewegung und die Mobilisierung zum G8-Gipfel im schottischen Gleneagles 2005, um fortan internationale Netzwerke zu unterwandern. Dabei war Kennedy nicht allein: Mit dem ebenfalls enttarnten „Marco Jacobs“ unterwanderte er unter anderem das linksradikale Dissent!-Netzwerk, beide beteiligten sich zuletzt an der Mobilisierung gegen den Straßburger NATO-Gipfel 2009. Insgesamt flogen bislang fünf Spitzel auf. Einige haben offenbar auch Sexualität zur Erschleichung von Vertrauen eingesetzt, einer hat sogar seine Zielperson geheiratet.

Laut Medienberichten unterhält die ACPO, die sich seit Ende der 90er Jahre verstärkt der „Extremismus“-Bekämpfung widmete, Dossiers zu 2.000 politischen AktivistInnen. Von der ACPO behauptet Kennedy bis zu 300.000 Euro jährlich erhalten zu haben. Zudem arbeitete er für eine private Sicherheitsfirma und gründete später selbst eine, um seine im Polizeisold erlangten Informationen mehrfach zu verwerten. Bislang ist unklar, ob er weitere Privatfirmen mit Informationen belieferte.

Kennedys Schnüffelei führte in Großbritannien u.a. zu einer Polizeirazzia und 114 Festnahmen, die die Blockade eines Kraftwerks des Energiemultis E.ON verhindern sollte. Wie umtriebig der Mann auch jenseits der britischen Inseln war, zeigt sein Einsatz in Island, wo er ab 2005 die Bewegung gegen die Aluminiumverhüttung durch ALCOA und den italienischen Berlusconi-Sponsor Impregilo infiltrierte. Auch aus Berlin, wo

1 mehr Details unter https://euro-police.noblogs.org/2011/01/entgrenzte-spitzel

Kennedy häufig zu Besuch war und an Protesten teilnahm, hat der VE laut Auskunft seiner Vorgesetzten „Beweismittel“ mitgebracht. Vermittelt durch das Bundeskriminalamt (BKA) heuerten die Landeskriminalämter Mecklenburg-Vorpommern und Baden-Württemberg die britischen Spitzel zur Unterwanderung von Gipfelprotesten an. Sie hätten, so der Stuttgarter Innenminister Heribert Rech (CDU), „Störerpotenziale, Zielpersonen, Örtlichkeiten und Absichten“ aufgeklärt und geholfen, dass der NATO-Gipfel „ohne Störungen friedlich verlaufen“ sei.

Unter deutscher Präsidentschaft startete die EU 2007 eine Initiative zur Vereinfachung der grenzüberschreitenden Spitzelausleihe. Regeln wollte man u.a. die Hilfe beim Ausstellen falscher Papiere, die Zusicherung der Anonymität in Gerichtsverfahren und die Möglichkeit zur Verwertung erlangter Beweise. Laut einem Vermerk des deutschen Ratsvorsitzes vom 25. Mai 2007 hätten die „bisherigen praktischen Erfahrungen“ gezeigt, dass ausländische VE „in gewissen Konstellationen leichter in kriminelle Vereinigungen eingeschleust werden können“.

BKA und Zollkriminalamt sind heute schon an der „European Cooperation Group on Undercover Activities“ beteiligt. Hier dürfte das BKA auch die „Vermittlung“ Kennedys an deutsche Landespolizeien arrangiert haben. Europol unterhält mit der „Cross-Border Surveillance Working Group“ zudem eine Arbeitsgruppe, die sich mit der Honorierung von Vertrauenspersonen und Informanten befasst.
(Matthias Monroy)

(Noch) mehr Macht für Frontex

Die EU-Grenzschutzagentur Frontex hat viel zu tun: Seit Anfang November 2010 helfen „Soforteinsatzteams“ (Rabits), 175 GrenzschützerInnen aus 23 Mitgliedstaaten, die griechisch-türkische Landgrenze zu überwachen. Am 25. Februar 2011 begann ferner die eigentlich erst für Juni geplante Frontex-Operation „Hermes“ rund um Lampedusa und Sizilien, an der neben Italien weitere zehn EU-Staaten sowie die Schweiz beteiligt sind. Italien stellt dafür die Schiffe, Flugzeuge kommen zusätzlich aus der BRD, Frankreich, Malta, den Niederlanden und Spanien.[2]

Am 27. Februar beklagte sich Frontex-Direktor Ilkka Laitinen in einem Interview mit der in Zürich erscheinenden „Sonntagszeitung“ über

2 s. die Materialien zu Rabit 2010 und Hermes Extension 2011 auf www.frontex.europa.eu

die „nicht genügende operationelle Beweglichkeit“ der Agentur. Frontex brauche ein „operationelles Reserveteam mit eigenem Material, mit Helikoptern, Flugzeugen und Booten“. Mit dem Vorschlag zur Änderung der Frontex-Verordnung, den die EU-Kommission bereits im Februar 2010 vorgelegt hat, könnte dieser Wunsch in Erfüllung gehen.[3]

Danach sollen die EU- und die assoziierten Schengen-Staaten künftig GrenzschützerInnen für jeweils ein halbes Jahr fest als „nationale Experten“ an Frontex abordnen. Für die Aufstellung von Frontex-Unterstützungsteams soll zudem ein verpflichtender „Mechanismus“ geschaffen werden, der die bisherigen (freiwilligen) Verwaltungsvereinbarungen mit den nationalen Behörden ablöst: Ähnlich wie für Rabit-Einsätze sollen die nationalen Grenzpolizeien „Pools“ von BeamtInnen bilden, die für „normale“ gemeinsame Operationen innerhalb von dreißig Tagen aufgeboten werden können. Eine vergleichbare Regelung ist für die Ausrüstung vorgesehen. Das von den Mitgliedstaaten bisher freiwillig zur Verfügung gestellte Material habe für den Übergang zu semipermanenten Operationen nicht ausgereicht. Frontex schätzt einen Bedarf von 92 Booten, 14 Flugzeugen und 18 Hubschraubern. Künftig soll die Agentur in stärkerem Maße eigene Ausrüstung anschaffen können. Zudem sollen sich die Mitgliedstaaten anhand eines Jahresplans verpflichten, Material zur Verfügung zu halten. Aus der bisher von Frontex geführten Liste der bei den nationalen Behörden vorhandenen Ausrüstung soll ein Register der Materialien werden, auf die die Agentur tatsächlich zugreifen kann. Für diese Operationen soll der Staat, in dessen Grenzzone der Einsatz stattfindet, künftig die Verantwortung mit Frontex teilen.

Die Agentur soll VerbindungsbeamtInnen in Drittstaaten entsenden. Sie soll auf der Basis monatlicher Angaben der Mitgliedstaaten einen „fortlaufenden Einsatzplan“ für Sammelabschiebungen erstellen. Während die Kommission noch daran festhält, dass Frontex bei seinen „Risikoanalysen“ keine personenbezogenen Daten bearbeiten soll, fordert die französische Ratsdelegation, dass die Agentur solche Informationen sammeln und analysieren soll, wenn es „hinreichende Gründe zu der Annahme“ gibt, dass die Betroffenen die „illegale Einwanderung“ erleichtern oder in den Menschenhandel verstrickt sind.[4]
(Heiner Busch)

3 KOM(2010) 61 endg. v. 24.2.2010, Folgenabschätzung: SEC(2010) 149 v. 24.2.2010
4 Ratsdok. 10528/10 v. 1.6.2010

Chronologie

zusammengestellt von Jan Wörlein

September 2010 (Nachtrag)

30.09.: **Stuttgart 21-Proteste:** Im Stuttgarter Schlosspark gehen 700 PolizistInnen gegen 5.000 Demonstrierende vor, die gegen das Fällen von Bäumen im Zusammenhang mit dem Stuttgart 21-Bauvorhaben protestieren. Wasserwerfer, Schlagstöcke und Pfefferspray werden eingesetzt. Viele Kinder einer kurz zuvor beendeten Schülerdemonstration sind von den Maßnahmen betroffen. 130 DemonstrantInnen und sechs PolizistInnen werden verletzt. Ein Rentner erblindet nach einem Wasserwerfereinsatz auf einem Auge. 26 Personen werden festgenommen. Die Behörden führen 147 Ermittlungsverfahren gegen 299 namentlich bekannte Beschuldigte und 69 gegen Unbekannt. Am 8. Oktober wird auch ein Ermittlungsverfahren wegen Körperverletzung im Amt gegen einen Polizisten eröffnet.

Oktober 2010

01.10: **Elektronische Fußfesseln:** Das baden-württembergische Justizministerium stattet in einem Modellversuch erstmals fünf Gefangene und Freigänger mit elektronischen Fußfesseln aus. Neben Hessen ist Baden-Württemberg das zweite Bundesland, das die Geräte testet.

04.10.: **Urteil gegen prügelnden Polizisten:** Das Amtsgericht (AG) Berlin-Tiergarten verurteilt einen 30-jährigen Beamten wegen Körperverletzung im Amt zu einer Geldstrafe von 4.800 Euro. Bei der „Freiheit statt Angst"-Demonstration im September 2009 in Berlin hatte er einen Demonstranten in den Rücken geschlagen, als dieser einem Gestürzten beim Aufstehen half. Am 28. Oktober verurteilt das AG Tiergarten einen weiteren Polizisten wegen Körperverletzung im Amt zu einer Geldstrafe von 1.500 Euro. Der 41-Jährige Beamte hatte auf derselben Demonstration einen 17-Jährigen mit der Faust ins Gesicht geschlagen.

07.10.: **Rechtswidrige Festnahmen:** Das Verwaltungsgericht (VG) Schwerin erklärt mehrere Festnahmen von Demonstranten während des G8-Gipfels in Heiligendamm 2007 für rechtswidrig. Insbesondere die Inhaftierung in Käfigen sei zu beanstanden.

12.10.: **Datentransfer an NATO rechtswidrig:** Das VG Wiesbaden entscheidet, dass die anlässlich des Straßburger NATO-Gipfels 2009 erfolgte Weitergabe von Daten über deutsche Journalisten durch das Bundeskriminalamt (BKA) an die NATO rechtswidrig war. Ein polnischer Journalist, dem daraufhin die Akkreditierung verweigert worden war, hatte gegen die Übermittlung geklagt.

13.10.: **Höhere Strafen bei Widerstand gegen Polizei:** Das Bundeskabinett beschließt einen Gesetzentwurf, mit dem das Strafmaß für Widerstand gegen Vollstreckungsbeamte von zwei auf drei Jahre erhöht werden soll.

14.10.: **Rechtsstreit um Überwachung:** Im Rechtsstreit zwischen Bodo Ramelow, dem Fraktionschef der Linken im Thüringer Landtag, und dem Landesamt für Verfassungsschutz um die Überwachung des Politikers wird ein Vergleich geschlossen. Der Vergleich beinhaltet die Feststellung der Rechtswidrigkeit der Überwachung. Nachdem das Bundesverwaltungsgericht im Juli 2010 Ramelows „Beobachtung" durch das Bundesamt für Verfassungsschutz (BfV) für rechtmäßig erklärt hatte, erhebt der Politiker am 19. Oktober Beschwerde vor dem Bundesverfassungsgericht (BVerfG).

15.10.: **Haft für Terrorhelfer:** Das Oberlandesgericht (OLG) Frankfurt am Main verurteilt einen 28-Jährigen wegen Mitgliedschaft in einer terroristischen Vereinigung zu drei Jahren und drei Monaten Haft. Salih S. soll für die „Islamische Jihad Union" (IJU) ein Nachtsichtgerät, GPS-Geräte sowie Outdoor-Kleidung besorgt haben. (Az.: 5-2 StE 8/10 – 5 – 4/10)

21.10.: **Keine Anklage gegen Polizisten:** Das OLG Nürnberg weist einen Antrag der Eltern des 2009 von Polizisten erschossenen Regensburger Studenten Tenessee Eisenberg auf Erhebung einer Anklage zurück. Die Beamten hätten „mit hoher Wahrscheinlichkeit in Notwehr gehandelt", so dass kein Anlass für eine Klageerhebung gegeben sei. Am 26. November erhebt die Familie des Toten Verfassungsbeschwerde vor dem BVerfG ein.

Klage gegen Sicherungsverwahrung abgelehnt: Der Europäische Gerichtshof für Menschenrechte (EGMR) verwirft die Beschwerde eines 65-jährigen Gefangenen. Die Sicherungsverwahrung an sich verstoße nicht gegen die europäische Menschenrechtskonvention, sondern lediglich die deutsche Rechtspraxis ihrer nachträglichen Anordnung.

25.10.: **Bewährungsstrafe für Flaschenwurf:** Das AG Berlin-Tiergarten verurteilt einen 20-Jährigen wegen schweren Landfriedensbruchs und versuchter gefährlicher Körperverletzung zu acht Monaten Haft auf Bewährung. Der Sozialassistent hatte am Berliner 1. Mai eine Flasche auf Polizisten geworfen. Am 17. November wird ein 24-Jähriger wegen versuchter gefährlicher Körperverletzung zu einer Bewährungsstrafe von acht Monaten verurteilt. Er hatte ebenfalls am 1. Mai im alkoholisierten Zustand eine Sektflasche auf einen Polizisten geworfen.

27.10.: **Polizisten verprügeln Hausmeister:** Die Frankfurter Polizei ermittelt wegen Körperverletzung im Amt gegen eigene Beamte. Die Beamten waren wegen eines Einbruchs zu einem Kindergarten gerufen worden, nahmen aber bei der Durchsuchung des Gebäudes statt des Einbrechers den Hausmeister fest, der sie alarmiert hatte. Der 44-Jährige erlitt mehrere Knochenbrüche und Prellungen.

29.10.: **Bomben entdeckt:** Nachdem saudische Sicherheitsbehörden über mögliche Bomben in aus Jemen kommenden Flugzeugen informieren, werden an Flughäfen in Großbritannien und Dubai zwei in Druckerkartuschen versteckte Sprengsätze entdeckt. Die in Großbritannien aufgefundene Bombe war am Flughafen Köln/Bonn unbemerkt umgeladen worden. Adressat der Paketbomben war eine Synagoge in Chicago. Der Airline Jemenia wird in der Folge die Flugerlaubnis entzogen.

November 2010

02.11.: **Bombe im Kanzleramt:** MitarbeiterInnen des Kanzleramts entdecken ein verdächtiges Paket aus Griechenland bei einer Vorkontrolle. Die als Büchersendung des griechischen Wirtschaftsministeriums getarnte Rohrbombe wird von ExpertInnen des BKA entschärft. Die Bombe ähnelt einem Sprengsatz, der am selben Tag an die deutsche Botschaft in Athen zugestellt wird.
Hessischer „Intrigantenstadl“: Der hessische Innenminister Boris Rhein (CDU) versetzt den Landespolizeipräsidenten Norbert Nedela in den

einstweiligen Ruhestand. Hintergrund sind Berichte über geheime Personalakten über missliebige BeamtInnen und Vorwürfe der Manipulation in einem Strafverfahren gegen die Leiterin des hessischen Landeskriminalamtes (LKA) Sabine Thurau. Die Staatsanwaltschaft beschuldigt sie der Falschaussage gegen einen Polizisten, der eine Dienstreise nach Brasilien für einen privaten Abstecher genutzt haben soll. Am 8. November wird auch sie „auf eigenen Wunsch" von ihrem Amt entbunden und ins Innenministerium versetzt, wo sie eine „Konzeption zur Bekämpfung der organisierten Kriminalität" erarbeiten soll. In der Folge wird ein neuer polizeiinterner Ansprechpartner für Polizisten eingesetzt.

03.11.: **Razzia und Festnahmen bei Nazi-Radio:** BeamtInnen des BKA und der Länderpolizeien durchsuchen in zehn Bundesländern 22 Wohnungen von 23 Beschuldigten aus der rechtsextremen Szene. Die 17 Männer und sechs Frauen, die für das „Widerstandsradio" gearbeitet haben, werden der Volksverhetzung und Bildung einer kriminellen Vereinigung beschuldigt.
Castor-Proteste im Wendland: 50.000 Protestierenden stehen 16.000 PolizistInnen gegenüber. 1.316 Personen werden in Gewahrsam genommen. Gegen 172 laufen Ermittlungsverfahren. 117 Traktoren werden beschlagnahmt. 950 Demonstrierende und 131 PolizistInnen werden verletzt. Die Staatsanwaltschaft Lüneburg ermittelt gegen einen am Einsatz beteiligten französischen Polizisten. Am 1. Dezember teilt das Bundesinnenministerium auf Anfrage der Linken mit, dass 2.190 Dosen Pfefferspray versprüht worden sind (s. den Beitrag in diesem Heft, S. 71-79).

11.11.: **Sicherungsverwahrung:** In der Auseinandersetzung um die Konsequenzen aus der Entscheidung des EGMR von Ende 2009, wonach die nachträgliche Sicherungsverwahrung gegen die Europäische Menschenrechtskonvention verstößt, widerspricht der fünfte Senat des Bundesgerichtshofs (BGH) dem vierten. Er stoppt vorerst die Praxis einiger OLGs, welche die Betroffenen nach Ablauf der bis 1998 geltenden Höchstdauer ohne Prüfung einer weiteren Gefährlichkeit aus der Verwahrung entlassen haben. (Az.: 5 StR 394/10)

12.11.: **Ärztlicher Leiter straffrei:** Die Staatsanwaltschaft Bremen stellt das Ermittlungsverfahren gegen einen mutmaßlichen Mitverantwortlichen des tödlichen Brechmitteleinsatzes an einem Kleindealer 2004 wegen Verjährung ein. Dem Leiter des Ärztlichen Beweissicherungsdiens-

tes und Vorgesetzten des ausführenden Arztes könne keine Fahrlässigkeit nachgewiesen werden.

16.11.: **Schadenersatz für Blockade:** Das OLG Dresden verurteilt den Bund Deutscher Milchviehhalter für die Blockade der zum Müller-Milch-Konzern gehörenden Molkerei Sachsenmilch im Juni 2008 zu einer Schadenersatzleistung. Die Blockade habe wirtschaftlichen Druck beabsichtigt und sei daher nicht durch die Versammlungsfreiheit gedeckt.

17.11.: **Geldstrafe für prügelnde Polizistin:** Das AG Limburg verurteilt eine Polizistin wegen Körperverletzung zu einer Geldstrafe von 5.400 Euro. Die 27-Jährige hatte als Zuschauerin eines Fußballspiels auf zwei Spielerinnen eingeschlagen.

21.11.: **Peter Grottian verurteilt:** Das AG Lindau verurteilt den emeritierten Politikwissenschaftler Peter Grottian wegen Aufforderung zum Hausfriedensbruch zu einer Geldstrafe von 3.600 Euro. Er hatte bei einem Vortrag in Lindau zu einer „öffentlichen, gewaltlosen, gewissensbestimmten und gesetzwidrigen Bankbesetzung" aufgerufen. Betroffene Banken hatten keine Strafanzeige gestellt. Der Politikprofessor kündigte Widerspruch gegen den Strafbefehl an.

23.11.: **Videoüberwachung von Demos untersagt:** Das Oberverwaltungsgericht Münster erklärt die Videoaufnahmen auf einer Anti-AKW-Demonstration in Münster im Juni 2008 für rechtswidrig. Eine anlasslose Kameraüberwachung sei geeignet, BürgerInnen einzuschüchtern und in ihrem Demonstrationsrecht einzuschränken (Az.: 5 A 2288/09; s. den Beitrag auf S. 86 f. in diesem Heft).

26.11.: **Kennzeichnungspflicht:** Der Berliner Innensenator Erhardt Körting (SPD) kündigt eine Kennzeichnungspflicht für Berliner PolizistInnen ab dem 1. Januar 2011 an. Die BeamtInnen können sich entscheiden, ob sie ihren Namen oder eine fünf- bis sechsstellige Nummer tragen.

30.11.: **Telekom-Mitarbeiter verurteilt:** Das Landgericht (LG) Bonn verurteilt einen ehemaligen Abteilungsleiter der Telekom wegen Verletzung des Fernmeldegeheimnisses, Untreue und Betrugs zu dreieinhalb Jahren Haft. Der 60-Jährige hatte Verbindungsdaten von Aufsichtsräten und Journalisten überwacht und 230.000 Euro veruntreut.
„Pro Köln" wird weiter beobachtet: Das VG Berlin lehnt eine Klage der fremdenfeindlichen Gruppierung „Pro Köln" gegen ihre Nennung im Verfassungsschutzbericht des Bundesinnenministeriums ab.

Dezember 2010

03.12.: **Kein Schadenersatz für verletzten Demonstranten:** Das LG Rostock weist die Klage eines beim G8-Gipfel 2007 verletzten Demonstranten gegen das Land Mecklenburg-Vorpommern ab. Dem 39-Jährigen war bei einem Wasserwerfereinsatz die linke Augenhöhle zerstört worden. Mecklenburg-Vorpommern sei nicht zuständig, da die Wasserwerferbesatzung aus Nordrhein-Westfalen gekommen sei.

05.12.: **Innenministerium verlangt Staatstreue:** Das sächsische Innenministerium will eine Verfassungstreueerklärung und eine Absage an die Zusammenarbeit mit „Extremisten" zur Bedingung von Förderungen für Vereine und Initiativen machen.

06.12.: **Massenabschiebung in Berlin:** Die Bundespolizei schiebt 45 VietnamesInnen vom Berliner Flughafen Schönefeld ab. Gegen die ausführende Fluggesellschaft Aeroflot gab es zuvor Bombendrohungen.

07.12.: **El-Masri verliert Prozess:** Das VG Köln weist die Klage des CIA-Entführungsopfers Khaled El-Masri gegen die BRD ab. Die Entscheidung der Bundesregierung, trotz Vorliegens eines von einem deutschen Gericht ausgestellten Haftbefehls die USA nicht um die Auslieferung der der Entführung beschuldigten CIA-Agenten zu ersuchen, sei durch ihren weiten Ermessensspielraum gedeckt. (Az.: 5 K 7161/08)

09.12.: **Werthebach-Kommission:** Die im April 2010 von Bundesinnenminister Thomas de Maizière (CDU) eingesetzte und vom ehemaligen BfV-Chef Eckart Werthebach präsidierte Kommission zur „Evaluierung der Sicherheitsbehörden" empfiehlt in ihrem Abschlussbericht eine Zusammenlegung von BKA und Bundespolizei.

12.12.: **Vorwürfe gegen Polizisten werden überprüft:** Die Berliner Polizei ermittelt nach einer Kundgebung von 100 Personen vor der iranischen Botschaft in Berlin wegen Körperverletzung im Amt gegen mehrere eigene Beamte. Acht Demonstrierende waren verletzt worden.
Bankräuber sterben nach Schießerei: Nach einem Banküberfall kommt es in der Karlsruher Innenstadt zu einer Schießerei zwischen dem Räuberpaar und PolizistInnen. Bei der Flucht eröffnet der Mann das Feuer und trifft eine 28-jährige Polizistin in den Oberschenkel. Beim folgenden Schusswechsel wird er tödlich getroffen, worauf sich seine Begleiterin selbst erschießt. 21 Überfälle werden dem Paar zugeschrieben.

14.12.: **Razzia bei Islamisten:** PolizistInnen durchsuchen in Nordrhein-Westfalen, Niedersachsen und Bremen 23 Vereins- und Privathäuser der Vereine „Einladung zum Paradies“ und „Islamisches Kulturzentrum Bremen“.

16.12.: **Polizeireform beschlossen:** Der brandenburgische Landtag verabschiedet ein Gesetz zur „Polizeistrukturreform 2020“. Danach werden 1.900 von 8.900 Stellen gestrichen und ein zentrales Landespolizeipräsidium in Potsdam wird geschaffen.
DHKP-C Mitglieder verurteilt: Das OLG Düsseldorf verurteilt drei Mitglieder der türkischen DHKP-C wegen Mitgliedschaft in einer terroristischen Vereinigung zu Haftstrafen zwischen drei Jahren und neun Monaten und sieben Jahren und neun Monaten.
Innenministeriumsneubau begonnen: Bundesinnenminister Thomas de Maizière tätigt den ersten Spatenstich für den 40.000 Quadratmeter großen Bau, der Platz für 1.600 Arbeitsplätze bieten und 2014 eingeweiht werden soll.

21.12.: **Überwachung rechtswidrig:** Das VG Köln gibt einer Klage des freien Journalisten Friedrich Burschel gegen seine Überwachung durch das BfV statt. Der Verfassungsschutz hatte eine Akkreditierung des Journalisten beim G8-Gipfel in Heiligendamm 2007 verhindert.
Razzia gegen Rechts: Ermittler durchsuchen in Baden-Württemberg, Rheinland-Pfalz, Brandenburg und Niedersachsen Wohnungen von Mitgliedern der Jungen Nationaldemokraten.

22.12.: **Verdeckter Ermittler entdeckt:** Mitglieder der Heidelberger Kritischen Initiative (KI) enttarnen einen Spitzel des LKA Baden-Württemberg, der seit 2009 verschiedene Projekte infiltriert und linke Gruppen bespitzelt hatte.

30.12.: **Polizeilicher Todesschuss:** Ein Polizist erschießt in München eine 49-Jährige in ihrer Wohnung. Die Polizei war durch den Leiter einer psychiatrischen Einrichtung verständigt worden, seine ehemalige Patientin drohe, ihre 24-jährige Tochter zu töten. Als ein Polizist über den Balkon in die Wohnung eindringt, greift die Frau ihn mit einem Messer an. Ein Pfeffersprayeinsatz bleibt wirkungslos, worauf der Beamte einen Schuss abgibt, der die Frau am Schlüsselbein trifft. Im Krankenhaus erliegt sie ihren Verletzungen. Die Tochter befand sich nicht in der Wohnung.

Literatur

Zum Schwerpunkt

Dass Private Strafverfolgung betreiben, dass die Übertretung allgemeinverbindlicher Gesetze nicht von staatlichen Organen verfolgt wird, dass es unterschiedliche Konstellationen der (Nicht-)Zusammenarbeit zwischen öffentlich-staatlichen und privatwirtschaftlich organisierten Einrichtungen gibt – über diese unübersehbaren Entwicklungen gibt es zumindest im deutschen Sprachraum nicht viel mehr als vage Vermutungen, die sich aus „Skandalen" und journalistischen Berichten nähren. Seriöse wissenschaftliche Veröffentlichungen sind so gut wie nicht vorhanden. Im Unterschied zu jenen privat-öffentlichen Polizeikooperationen, die sich auf Streifendienste, die Überwachung des Raumes etc. beziehen, findet die „private" Bearbeitung strafbaren Verhaltens ebenso wie die Arbeitsteilung mit der öffentlichen (Kriminal-)Polizei unter Ausschluss von Öffentlichkeit und Wissenschaft statt. Nur wenige Ausnahmen sind erwähnenswert.

Morath, Mona: *Private Strafermittlungen. Eine Studie unter besonderer Berücksichtigung der Problematik privater Straftatenaufklärung durch organisierte Sicherheitsdienste, Hamburg 1999*
Angesichts der (damals) erwarteten Steigerungen von Kriminalität und den begrenzten Ressourcen, die für den Ausbau der Polizeien zur Verfügung stünden, plädierte diese juristische Dissertation für ein „kooperierendes Miteinander" (S. 268) von Polizei und privaten Ermittlungsdiensten. Grundlegende rechtliche Probleme werden nicht gesehen. Die privaten Ermittler müssten besser ausgebildet, die Betriebe müssten konzessioniert werden. Die Tätigkeiten der Privaten seien durch Datenschutzbestimmungen, allgemeine Persönlichkeitsrechte, durch das Strafrecht und durch das Verbot verdeckter Methoden ausreichend begrenzt. Lediglich das Verbot bestimmter Vernehmungsmethoden müsste auf die Privaten ausdehnt werden. Unter diesen Bedingungen, so meint die Autorin, stellten „private Strafermittlungen" eine „sinnvolle Ergänzung" des staatlichen Strafverfolgungssystems dar.

Bussmann, Kai-D.; Werle, Markus M.: *Addressing Crime in Companies. First Findings from a Global Survey of Economic Crime, in: British Journal of Criminology 2006, No. 6, pp. 1128-1144*
Im Jahr 2005 wurden rund 5.500 Unternehmen weltweit über ihre Erfahrungen mit und ihre Reaktionen auf Wirtschaftskriminalität befragt. Die Untersuchung erfolgte in Zusammenarbeit mit „Price Waterhouse Coopers International", einem der großen Anbieter auf dem globalen Sicherheitsmarkt zur Bekämpfung von Wirtschaftskriminalität. Interessant an den Befunden ist die insgesamt geringe Bedeutung, die die Unternehmen der staatlichen Polizei geben: Nur vier Prozent der Delikte seien von der Polizei entdeckt worden – wobei erhebliche regionale Unterschiede existieren. Die Bereitschaft, die öffentliche Strafverfolgung einzuschalten, sinke erheblich, wenn der Beschuldigte aus dem Unternehmen stamme. In 80 Prozent dieser Fälle komme es zu einer Entlassung, nur die Hälfte würden zur Anzeige gebracht. Weltweit, so die Autoren zusammenfassend, hätten Unternehmen „ein Set von Strategien zur Prävention und Kontrolle im Schatten des Systems der Kriminaljustiz" entwickelt.

Jaeger, Rolf Rainer: *Problematik privater Ermittlungsorganisationen in Unternehmen, in: der kriminalist 2008, H. 1, S. 19-24*
Aus polizeilicher Sicht benennt der stellvertretende Bundesvorsitzende des „Bundes Deutscher Kriminalbeamter" einige problematische Aspekte „privater Ermittlungsorganisationen" in Unternehmen. Die Bedeutung dieser „Firmenkripo" werde insgesamt erheblich unterschätzt. Für ihre Arbeit sei kennzeichnend, dass sie sowohl im Hinblick auf die verfolgten Ziele wie die eingesetzten Methoden an die Interessenlage der Unternehmen gebunden blieben. Schadensbegrenzung und -wiedergutmachung, einvernehmliche und „geräuschlose" interne Lösungen, Rückgriff auf die Polizei nur in besonderen Konstellationen – das seien die grundlegenden Merkmale dieses Gewerbes. Die Kosten für die Allgemeinheit (die Geltung des Strafrechts wird unterlaufen, kriminelle Beschäftigte und Kunden suchen sich neue Opfer) und für die Betroffenen (geringer Schutz gegen falsche Anschuldigungen und unerlaubte Ermittlungen; „Ermittlungen" und Strafe erfolgen durch das Unternehmen) sind offenkundig. Liest man Jaegers Kritik aufmerksam, kann man kaum für privat-polizeiliche Kooperationen plädieren. Wer es Ernst meint mit rechtsstaatlichen Garantien, mit dem Schutz von Beschuldigten, mit der Gewaltenteilung und mit der Gültigkeit eines allgemeinen Rechts, der muss „Firmenkripos" als undemokratische Einrichtungen ablehnen.

Schneider, Stephen: *Privatizing economic crime enforcement: Exploring the Role of Private Sector Investigative Agencies in Combating Money Laundering, in: Policing & Society 2006, No. 3, pp. 285-312*

Favarel-Garrigues, Gilles; Godefroy, Thierry; Lascoumes, Pierre: *Sentinels in the Banking Industry, in: British Journal of Criminology 2008, No. 1, pp. 1-19*

Die Bekämpfung der Geldwäsche ist eines der zentralen Felder, in denen die Interessen der Privatwirtschaft (Banken etc.), des Staates und einer spezialisierten Sicherheitsindustrie gleichförmig zusammenlaufen. Seit die Geldwäschebekämpfung zum strategischen Ansatzpunkt zur Schwächung von Drogenhandel, organisierter Kriminalität und Terrorismus geworden ist, genießen die Initiativen, „schmutziges" Geld aus dem sauberen Geldkreislauf fernzuhalten, politische Priorität. Die Fallstudien zu fünf englischsprachigen Ländern (Schneider) und zu Frankreich (Favarel-Garrigues u.a.) werfen ein Schlaglicht auf die entstehende Professionalisierung der „privaten" Geldwäschebekämpfer und ihre Zusammenarbeit mit staatlichen Instanzen. Während Schneider für eine stärkere Regulierung der privaten Aktivitäten plädiert, um sie in eine Partnerschaft mit dem Staat einzubinden, betonten die Autoren der französischen Studie bereits entstandene Kooperationen, die zu einer „joint intelligence production" geführt haben.

Gill, Martin; Hart, Jerry: *Policing as a business: The organisation and structure of private investigation, in: Policing & Society 1997, No. 2, pp. 117-141*

Nur als Illustration, was anderswo schon lange möglich war, in Deutschland niemanden zu interessieren scheint: Gill und Hart fertigen Mitte der 90er Jahre eine empirische Bestandsaufnahme des privaten Ermittlungsgewerbes in England an. Im Ergebnis liefern sie vier idealtypische Modelle, in denen „private investigators" tätig werden: 1. der allein arbeitende Ermittler, 2. kleinere Firmen mit wenig Beschäftigten, die in der Regel für Rechtsanwälte tätig werden, 3. Firmen mit mehr Beschäftigten, größerem Umsatz und regionaler oder nationaler Reichweite und 4. „prestige companies", die sich auf wirtschaftskriminalistische Ermittlungen spezialisiert haben. Durch formelle und informelle Netzwerke seien die unterschiedlichen Akteure miteinander verbunden.

Aus dem Netz

www.bdd.de

Wenig erfährt man auf der Hompage des „Bundesverbandes Deutscher Detektive e.V." über die Ermittlungstätigkeiten seiner Mitglieder (die nur ca. 10 Prozent der Detekteien Deutschlands ausmachen). Immerhin lässt sich den jährlichen Kurzberichten entnehmen, dass 2009 mehr als die Hälfte der Aufträge aus „Wirtschaft/Industrie/Handwerk" kamen. Dabei stellten Banken, Kreditinstitute und Versicherungen nur 16 Prozent der Auftraggeber. In 52 Prozent der Fälle hätten die „detektivischen Ermittlungsergebnisse" zu einer „privaten oder innerbetrieblichen Regelung" geführt; in 30 Prozent sei es zu einer Anzeige/einem Prozess gekommen.

www.bdws.de

Der „Bundesverband Deutscher Wach- und Sicherheitsunternehmen e.V." ist der Spitzenverband der privaten Sicherheitsbranche. In seinem Focus stehen die klassischen Bewachungs- und Sicherungstätigkeiten. In welchem Ausmaß seine 828 Mitgliedsfirmen – darunter die Großen der Branche – auch kriminalistisch tätig werden, lässt sich der Homepage nicht entnehmen.

www.asw-online.de

In der „Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V." (ASW) sind faktisch die Sicherheitsabteilungen der großen Unternehmen zusammengeschlossen. Mitglieder sind neben acht Landesverbänden u.a. die Spitzenverbände der deutschen Wirtschaft (DIHK, BDI, BDA) sowie der BDWS und der BDD. Nach ihren „Leitsätzen" vertritt die ASW „die Sicherheitsinteressen der Wirtschaft gegenüber Politik, Staat und Gesellschaft". Der Verband propagiert ein „Sicherheitsmanagement" als „kontinuierliche(n) Prozess der frühzeitigen Identifizierung und Abwehr aller Risiken und Gefahren unter Berücksichtigung der Unternehmensstrategie und Geschäftsziele". Die Zusammenarbeit mit dem Staat müsse intensiviert werden; ein „nationaler Sicherheitsrat" sei denkbar. Und auch die „Errichtung integrierter gemeinsamer Frühwarnstrukturen" sei möglich.
(alle: Norbert Pütter)

Sonstige Neuerscheinungen

Hoogenboom, Bob: *The Governance of Policing and Security. Ironies, Myths and Paradoxes, Houndmills, Basingstoke (Palgrave Macmillan) 2010, 236 S., EUR 71,–*

Zwölf Kapitel Altpapier, eine zu harte Bewertung? Hoogenboom ist es nicht gelungen, einen einzigen neuen Gedanken zu entwickeln, von den Redundanzen einmal abgesehen, auch wenn er in der Einleitung (S. 9) behauptet, er werde die Leser mit seinem Buch noch sensibler machen für Entwicklungen in der Kriminalpolitik „by pinpointing new themes and new research questions". Um es wenigstens anzudeuten, im zweiten Kapitel heißt es etwa, es sei zwischen „fictional" and „factual policing" zu unterscheiden (S. 17-38), also: nicht alles, was zu Veränderungen in Polizeitaktiken und -strategien von Politik, Polizei und Sozialwissenschaft behauptet wird, findet tatsächlich statt. Chapeau! Den Vorwurf, seine Kolleginnen und Kollegen aus der Kriminologie würden sich nicht oder zu wenig um die Empirie kümmern – „factual policing is a ‚neglected' subject" (S. 20) –, erhärtet er nicht. Im dritten Kapitel, das sich mit „neuen" Kooperationsformen zwischen Polizei, Militär, Geheimdiensten und der Bedeutung neuer Technologien für die Polizeiarbeit auseinandersetzt, behauptet er zum Ende apodiktisch, all das sei „under-researched and … in fact sometimes not studied at all" (S. 56). Nun, dass es immer noch mehr Forschungsbedarf geben kann, geschenkt, aber es wäre dann doch schön gewesen, Hoogenboom hätte sich die Mühe gemacht, aktuelle Literatur zu den von ihm vermeintlich identifizierten Forschungslücken zur Kenntnis zu nehmen – die Studien von Wakefield (2003) und Button (2007) zur Zusammenarbeit von Polizei und kommerziellen Sicherheitsdiensten tauchen in der Literatur nicht auf, auch nicht die Arbeiten von Coaffee et al. (2009) und Aas et al. (2009) zur Bedeutung von Überwachungstechnologien – Stephen Graham (2004, 2009) scheint ihm gar kein Begriff; die Liste ließe sich fortsetzen. Selbst die (berechtigte) Kritik am Konzept des „nodal policing"-Ansatzes von Shearing, Stenning, Wood und anderen – noch dazu unter dem Motto „was sich liebt, das neckt sich" (S. 200, deutsch im Original) – verbleibt an der Oberfläche. Der Verlag hatte das Buch stets als Koproduktion mit Maurice Punch angekündigt, und Hoogenboom erwähnt in einer Endnote, „we disentangeled ourselves from this book and chose different avenues" (S. 216). Vielleicht hätte Hoogenboom besser an der Seite von Punch bleiben sollen – ein ärgerliches und überflüssiges Buch.

Deflem, Mathieu (ed.): *Surveillance and Governance: Crime Control and Beyond, Bingley (Emerald Publishing) 2008, 378 S., EUR 77,–*
Der vom Soziologen Mathieu Deflem herausgegebene Band umfasst 16 Beiträge, die, in vier Unterkapitel gegliedert, sich der Foucaultschen Gouvernementalitätstheorie verpflichtet fühlen. Im ersten Teil, *Boundaries and Spaces*, wird die (soziale Konstruktion der) Grenze und der überwachte Raum so in den Blick genommen, dass deutlich wird, Überwachung ist heute Bürgerpflicht (James Walsh), aber auch hoch umstritten – Videoüberwachung anlässlich der Winter-Olympiade 2010 in Vancouver und Whistler (Kevin Haggerty, Laura Huey, Richard Ericson) – und sehr variabel einsetzbar – Überwachung am Flughafen Orly und im ‚Problemquartier' Dammarie-Les-Lys. Im zweiten Abschnitt, *Technologies and Strategies*, wird Hausarrest als Teil neoliberaler Regierungsform gelesen (William Staples, Stephanie Decker), dem FBI in Universitäten und Bibliotheken nachgespürt (Scott White), staatliche Überwachung in sozialen Bewegungen analysiert (David Cunningham, John Noakes) und werden kommerzielle Sicherheitsdienste als Verlängerung des staatlichen Gewaltmonopols identifiziert (Michael McCahill). Unter der Überschrift *Objectives and Counter Objectives* wird u.a. gezeigt, wie ‚der Bürger' in Australien, Großbritannien, Kanada und den USA (freiwillig) zum Koproduzenten von Sicherheit wird – solange er weiß ist (Janet Chan). Die Doppelrolle des Internet als Ort politischen Widerstands (Benoit Dupont) und effektiverer staatlicher Kontrolle (Kevin Stevenson) wird ebenso beleuchtet, wie – im letzten Abschnitt, *Beyond Crime Control* – der Einsatz von Überwachungstechnologien im Schulwesen, die Ausgrenzung verstärken (John Gilliom), aber zumindest auch sichtbar machen kann (Nathan Harris, Jennifer Wood). Auch für diejenigen, denen Foucault nicht als Richtschnur gilt, ein fundierter und empirisch satter Band.

Tsoukala, Anastassia: *Football Hooliganism in Europe. Security and Civil Liberties in the Balance, Houndmills, Basingstoke (Palgrave Macmillan) 2010, 179 S., EUR 48,–*
Bach, Stefanie: *Die Zusammenarbeit von privaten Sicherheitsunternehmen, Polizei und Ordnungsbehörden im Rahmen einer neuen Sicherheitsarchitektur der Bundesrepublik Deutschland. Beobachtungen und Analysen im Zusammenhang mit der FIFA WM 2006, Holzkirchen/Obb. (Felix Verlag) 2008, 237 S., EUR 39,–*
Tsoukala, Professorin für Kriminologie in Paris, zeichnet in ihrer Arbeit die Geschichte der Kriminalisierung so genannter ‚Hooligans' und deren

(nachträgliche) Legalisierung durch national- und europarechtliche Regulierungen nach. Sie kann zeigen, dass und wie es seit Mitte der 80er Jahre im Zuge der Kommerzialisierung des europäischen Fußballs zur Erfindung ‚des Anderen' gekommen ist: des ‚Hooligan'. Das Drama im Heysel-Stadion „merely accelarated a change that was already underway" (S. 26). Zwischen Mitte der 80er Jahre und 1997 setzt sich diese Linie durch, und auch die Polizeistrategien vereinheitlichen sich auf europäischer Ebene. Seitdem „combating football hooliganism was no longer simply an area into which policing methods were being imported from other domains, but had now become a method for testing and importing new internal security methods" (S. 118). Über die Figur des ‚Hooligan', wie Tsoukala u.a. anhand der Etablierung von Videosystemen, Reisebeschränkungen und Stadionverboten nachweist, „the breaching of civil liberties has become invisible to society because legal abnormality is now accepted as normal" (S. 134).

Einen anderen Fokus wählt Bach in ihrer Dissertation und konzentriert sich auf die Fußballweltmeisterschaft 2006 in Deutschland. Aus dem reichhaltigen Material – allein 21 Vertreter des kommerziellen Wach- und Sicherheitsgewerbes wurden interviewt – sollen lediglich drei Aspekte hervorgehoben werden: Erstens ist beeindruckend, wie sehr die interviewten Geschäftsführer von Sicherheitsunternehmen ihre Beschäftigten offensichtlich für ‚Vollidioten' halten (S. 54); zweitens kann Bach zeigen, wie die vielgerühmten *Volunteers* – immerhin 12.000 freiwillige, nicht entlohnte Helfer – in die Sicherheitsstrukturen unter dem Kommando kommerzieller Sicherheitsdienste in die Kontrollstrategien während der FIFA Weltmeisterschaft eingebunden wurden (S. 153 ff.); drittens, und zu dieser Schlussfolgerung sind die politisch Verantwortlichen für den Einsatz kommerzieller Sicherheitsdienste selbst nach dem Desaster der ‚Love Parade' im Juli 2010 mit 21 Toten bisher nicht gelangt, betont Bach mit Blick auf die Fußball-WM, „kann nur ein einziges Fazit gezogen werden: die Gewerbeaufsicht im Bereich des Sicherheits- und Bewachungsgewerbes muss intensiver und effektiver ausgeübt werden" (S. 206). Die Arbeit ist an manchen Stellen ungenau und vermischt Planungen der FIFA mit der tatsächlichen Umsetzung von Maßnahmen (etwa beim Einsatz von RFID), aber sie setzt gleichwohl Maßstäbe für ‚events to come'.
(alle: Volker Eick)

Summaries

Thematic focus: Private prosecutors

Private and state investigators – an introduction
by Norbert Pütter

The private security market is not restricted to patrol and watch services. In the context of increasing industry interest in security, the focus has turned to investigative activities executed either by in-house security departments and/or external service providers. The private contractor thereby decides the cause of the "investigation" and decides whether its results lead to charges being filed. There is, however, no contradiction in the relation between private and state security. Rather, different forms of cooperation and information exchange exist, which are sometimes legally fixed and at other times result from informal connections. The area of "grey policing", whereby industry and state interest overlap, represents a serious threat.

The data scandal at the Deutsche Bahn AG
by Albrecht Maurer

In order to uncover possible corruption, the German national railway Deutsche Bahn started screenings of more than 100.000 employees and matching their data with that of partner firms on a regular basis since the end of 1990s – without the knowledge of the workers' council or its data protection officer. The company contracted private investigators to spy on employees and controlled their e-mail traffic to identify internal critics. This huge scandal faded after top personnel were exchanged. The basic problem, namely, that a privatised company engages in internal investigations largely according to its own rules, remains.

Public Private Partnership in video surveillance
by Eric Töpfer

Although direct video surveillance by the police is limited in Germany, opaque surveillance webs are emerging as the police are seeking access

to other systems. The Football World Cup in 2006 was a catalyst for the technical networking of non-police CCTV systems with police command centres. But as this kind of networking proves to be expensive and inflexible in face of various police demands, informal cooperation is practised in which officers visit CCTV control rooms to exploit their surveillance capacities. These public private partnerships are not without conflicts; the key problem, however, is that they are unaccountable to those under surveillance.

Open Source Intelligence in a see-through world

by Ben Hayes

The internet has created new possibilities for the collection and analysis of intelligence. The border between open and undercover sources increasingly dissolves. At the same time a process of outsourcing can be observed: Open Source Intelligence is an increasingly profitable business of private enterprises, which are scarcely bound by regulations. They can, however, count on the support and interest of EU security institutions and EU Members States.

Business and the state as "security partners"

by Randalf Neubert

In March 2006, the Federal Criminal Authority (*Bundeskriminalamt*) started its "Global Player Initiative" and exchanging information with security departments of big corporations. The Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*) also cooperates in cases of economic espionage. Similar partnerships exist at the regional level. What really happens in these networks of state security and private industry is not known to the public.

Privatised security in the global context

by Norbert Pütter

New transnational actors start appearing in the security market: policing for profit encompasses security consultancies, who draft risk assessment reports for large corporations but also engage in private investigations, as well as forensic accountants and military service providers. Their transnational nature increases the problems: lack of transparency for the public, lack of legal and political control, dependency on contractors and

– in varying constellations – working with, beside or against state security apparatuses.

Non-thematic articles

Review: "The road towards the security society"

by Wolf-Dieter Narr

Criminal law professor Peter Alexis Albrecht has published a volume containing 49 essays reflecting his own political and scientific biography as well as the history of criminal law, prosecution and punishment in the Federal Republic from 1970 until the present. They address the criminal law of the welfare state and the unfulfilled hope to implement human rights also in the penal system; the change towards the state of prevention in the 1980s and 1990s and finally the shift towards a security society in which democratic legal definitions are increasingly blurred. Albrecht helplessly advises "absolutist regulations that are critical of the state" against these developments.

Protests against nuclear waste

by Elke Steven

In November 2010, shortly after the federal government extended the run-time of Germany's nuclear power stations, a new transport of highly radioactive waste from the reprocessing plant in France to the intermediate disposal facility in Gorleben took place. The Committee for Fundamental Rights and Democracy (Komitee für Grundrechte und Demokratie) followed the protests against the transport and monitored police conduct.

DNA database network with some constructional flaws

by Eric Töpfer

According to the Prüm Decision passed by the Justice and Home Affairs Council, the linking of national DNA databases of all 27 EU Member States should be finalised by 26 August 2011. This project, however, is facing a series of administrative, legal and particularly technical barriers. It is time to draw a critical balance regarding the breath-taking extension of globalised biometric control.

MitarbeiterInnen dieser Ausgabe

Heiner Busch, Bern, Redakteur von Bürgerrechte & Polizei/CILIP, Vorstandsmitglied des Komitees für Grundrechte und Demokratie

Volker Eick, Berlin, Politikwissenschaftler an der Freien Universität Berlin, John F. Kennedy Institut, Abteilung Politik

Angela Furmaniak, Freiburg/Lörrach, Rechtsanwältin und Mitglied des Republikanischen Anwältinnen- und Anwältevereins

Ben Hayes, London, Mitarbeiter von Statewatch

Mark Holzberger, Berlin, Referent für Migrations- und Integrationspolitik der Bundestagsfraktion von Bündnis 90/Die Grünen und Mitglied der Redaktion von Bürgerrechte & Polizei/CILIP

Martina Kant, Berlin, Redakteurin von Bürgerrechte & Polizei/CILIP und Bundesgeschäftsführerin der Humanistischen Union

Albrecht Maurer, Berlin, innenpolitischer Referent der Bundestagsfraktion Die Linke und Mitglied der Redaktion von Bürgerrechte & Polizei/CILIP

Katrin McGauran, Amsterdam, Mitarbeiterin von Statewatch

Matthias Monroy, Berlin, freier Journalist

Wolf-Dieter Narr, Berlin, Professor für Politikwissenschaft an der FU Berlin und Mitherausgeber von Bürgerrechte & Polizei/CILIP

Randalf Neubert, Berlin, Mitarbeiter des Instituts für Bürgerrechte & öffentliche Sicherheit

Norbert Pütter, Berlin, Redakteur von Bürgerrechte & Polizei/CILIP

Elke Steven, Köln, Sekretärin des Komitees für Grundrechte und Demokratie

Eric Töpfer, Berlin, Politikwissenschaftler am Zentrum Technik und Gesellschaft der TU Berlin, Redakteur von Bürgerrechte & Polizei/CILIP

Jan Wörlein, Berlin, Doktorand an der FU Berlin, Redakteur von Bürgerrechte & Polizei/CILIP