# Technik als Politik. Zur Transformation gegenwärtiger Grenzregimes der EU

**Stefan Kaufmann**

**SUMMARY**

The article focuses from a micro-political perspective on the fundamental change taking place within contemporary border regimes. It asks for the political dimensions of the technological upgrading of surveillance and control of the border. It will be demonstrated that the modes of producing security are in no way of homogeneous political nature. Firstly, there is a kind of military-style politics of radical exclusion and walling-off at work, which can be observed in the technology and the aligned institutional and tactical aspects of the SIVE-project. Secondly, border protection, e. g., on airports or at the Eurotunnel operates with step-by-step procedures and a machine-like mode of producing suspicion, seeming to produce a high degree of democratic and liberal legitimacy. Thirdly, with the combination of biometric identification and data bank management the mode of producing security tends to result in authoritarian surveillance and control. However, this in no way is the permanent operational mode of surveillance and control, but it is one control-level within a flexible regime, able to turn rapidly from liberal to authoritarian modes of political regulation.

Mit Blick auf die Grenzen der EU lassen sich mindestens drei Momente nennen, welche die gegenwärtige Transformation des Grenzregimes antreiben. Da ist zum einen die räumlich und institutionell neue Form von Staatlichkeit, wie sie sich mit der EU ausbildet. Das politisch-juridische Gebilde der klassischen Nationalstaaten und mithin die nationalen Grenzziehungen verlieren bekanntlich an sozialer Prägekraft. Wo einst der (National-)Staat als Handlungsrahmen, als Souverän, als alleiniger Akteur oder zentraler Bezugspunkt diente, treten jetzt inter- und transnationale oder auch regionale Relationen, Institutionen und Organisationen öffentlicher und privater Natur, auf. Dabei geht zumindest die Aufgabe der Grenzsicherung weitgehend auf die EU über. Zweitens wird

**Comparativ |** Zeitschrift für Globalgeschichte und vergleichende Gesellschaftsforschung 18 (2008) Heft 1, S. 42–57.

die Transformation des Grenzregimes durch ein neues Sicherheitsdenken vorangetrieben. Ein Sicherheitsdenken, das seit Ende der 80er Jahre und nochmals verschärft nach 9/11 seine Konturen gewann. Sicherheit wird seither nicht mehr vorrangig militärisch verstanden, sondern auf einem Kontinuum angesiedelt, das vom illegalen Immigranten über organisierte Kriminelle bis zum Terroristen reicht. Nicht mehr (nur) der äußere Feind, der politische Gegner, wird als essentielle Bedrohung der Sicherheit wahrgenommen, vielmehr werden ganz heterogene Formen von Bedrohung aufgerufen. Heterogene, sektorale Felder innerer Sicherheit geraten in den Kontext äußerer Bedrohung. Und gerade weil die Freiheit der Verkehrsflüsse, die Freiheit von Waren, von Kapital, von Dienstleistungen und Personen sich in das gleiche Programm einschreiben, welches das Feld der Sicherheit in neuer Weise strukturiert, verliert die Grenzsicherung im Kontext der neuen Sicherheitsarchitektur keineswegs an Bedeutung.[1] Das dritte Moment, das sich daran anschließt, ist der technologische Umbau der Grenzen. Grenzen funktionieren – so kann man sagen – als Selektionsmaschinen, welche die Unterscheidung „durchlassen – nicht durchlassen" prozessieren. Insofern existieren sie lediglich in actu als soziotechnische Arrangements, die regeln, welche Menschen und Sachen in ein Staatsgebiet hinein- oder aus ihm herausdürfen, welche herausmüssen und welche nicht.[2] Dabei ist das soziotechnische Arrangement selbst, die Technologien und damit verbundene Operationsweisen, mit denen Grenzen kontrolliert und Selektionen durchgeführt werden, keineswegs ein politisch neutrales Instrument. Dies ist offensichtlich: eine Grenze mit Selbstschussanlagen kann kein Sicherungsmittel eines liberalen Rechtsstaats sein, da sich mit ihrer Installation der Charakter eines solchen Staates verändern würde. Weniger offensichtlich aber ist die Antwort auf die Frage, welcher politische Gehalt sich hinter den eingesetzten Sachtechnologien und Operationsformen der im Umbruch befindlichen EU-Grenzsicherung verbirgt, welches Staatsverständnis, welche Machtkonfigurationen sich in diesen manifestieren.

Ich möchte im Folgenden drei Technologien, genauer: drei technische Projekte, skizzieren, mit denen sich heterogene Aspekte der Grenzsicherung beleuchten, unterschiedliche Taktiken und Strategien der Sicherheitsproduktion in den Blick rücken lassen. Mit diesen Technologien sind – wie sich zeigen lässt – jeweils unterschiedliche Modi politischer Regulation verknüpft. Modi politischer Regulation, die weit über die Grenzsicherung hinausreichen und denen möglicherweise ein paradigmatischer Charakter für die Sicherheitsproduktion in gegenwärtigen Gesellschaften zukommt. Es geht erstens um radikale Exklusions- und Abschottungsprojekte, für die etwa das SIVE-Projekt, die Überwachung der Südspanischen Küstenregion steht, zweitens um Formen der Durchleuchtung, wie

1 Vgl. ausführlich zu dieser Rekonfiguration des Sicherheitsverständnisses und dem damit verbundenen institutionellen und räumlichen Umbau des Grenzregimes: S. Kaufmann, Grenzregimes im Zeitalter globaler Netzwerke, in: H. Berking, (Hrsg.), Die Macht des Lokalen in einer Welt ohne Grenzen, Frankfurt a. M./New York 2006, S. 32-65.

2 Die Formulierungen in diesem Absatz gehen auf einen Aufsatz zurück, der zusammen mit Ulrich Bröckling und Eva Horn verfasst wurde; S. Kaufmann/U. Bröckling/E. Horn, Einleitung, in: Dies., (Hrsg.), Grenzverletzer. Figuren politischer Subversion, Berlin 2002, S. 7-22.

sie etwa an Flughäfen oder am Eurotunnel praktiziert werden und drittens um das Problem der Verknüpfung von Datenspeicherung und biometrischer Personenerkennung.

## Fortifikation als Modus der Grenzregulation – militärische Operationsformen

Fortifikation ist eine archaische Technologie der Grenzsicherung. Ihre Mittel reichen von Holzpalisaden, Steinmauern und Wachtürmen bis zu Stacheldrahtverhauen, Betonwällen, Minenfeldern und Selbstschussanlagen. Fortifikation bedeutet, die Grenze als physisches Hindernis zu etablieren, das unkontrollierte Überschreitung verhindert. Die Grenze wird zur hermetisch abgeriegelten Linie. Sie kennt nicht allein Kontrollpunkte an Verkehrsübergängen, sondern die Absperrung auch „grüner" und „blauer" Übergangszonen. Fortifikationen betonen die militärische Funktion der Grenze. Sie finden sich dort, wo die Grenze vor allem eines ist: eine zur Demarkationslinie geronnene Frontlinie, eine Scheidelinie zwischen Freund und Feind. Inzwischen allerdings werden Fortifikationen genau dort eingerichtet, wo das Wohlstandsgefälle zwischen EU-Staaten und Nachbarländern am ausgeprägtesten ist.[3] War bereits der Eiserne Vorhang nicht nur eine nationale, sondern eine Systemgrenze, so wirken die neuen Mauern als Wohlstandsgrenzen – und mehr noch: sie markieren Kulturgrenzen. Der Ortswechsel der Fortifikationsbauten ist Ausdruck eines Bedeutungswandels des Sicherheitsregimes: Wenn gegenwärtig von der Festung Europa die Rede ist, ist damit nicht die Abschottung vor Feinden im traditionellen Sinn, sondern die Ausgrenzung von Migranten gemeint. Seinen sinnfälligsten Ausdruck findet diese Fortifikation denn auch in den doppelreihigen, acht bzw. zehn Kilometer langen stacheldrahtbewehrten Zäunen, Kontrolltürmen, Kamera- und Sensorenüberwachungen, welche 1995 und 1996 um die Landgrenzen von Ceuta und Melilla, den spanischen Enklaven auf afrikanischem Boden, gezogen wurden.

Die Abschleifung der Differenz zwischen militärischen und anderen Grenzfunktionen zeigt sich mehr noch in einem der technologisch avanciertesten EU-Projekte zur Grenzsicherung: dem „Sistema Integrado de Vigilancia Exterior" (SIVE). Das SIVE-Projekt ist ein System der Küstenüberwachung zur „Entdeckung, Identifikation, Verfolgung und Unterbindung"[4] von jeder Form illegalen Eindringens auf spanisches Territorium. Zunächst im Streifen der Meeresenge von Gibraltar installiert, wird das System sukzessive ausgedehnt. Es operiert inzwischen auch auf den Kanarischen Inseln, den Küsten der Provinzen Malaga und Granada und im Laufe des Jahres 2008 soll der Ausbau für die gesamte Spanische Südküste von Huelva bis Almería abgeschlossen werden. Mit diesem Projekt werden technische und organisatorische Formen militärischer Aufklärung in den Bereich der Grenzüberwachung übersetzt. Es geht um Aufklärung im Vorfeld der

3 Darauf weist sogar eine Veröffentlichung der Guardia Civil zur Grenzkontrolle hin; F.G. Maroto, Control de fronteras, in: Publicaciones de la Universidad Nacional de Educacion a Distancia, 2005, S. 1; zit. nach: http://www.uned.es/investigacion/publicaciones/Cuadernillo_junio200503.pdf (16.01.2008).

4 Ebd., S. 4.

Grenze. SIVE soll sämtliche Bewegungen und Annäherungen an die Grenze bzw. die Küste sichtbar machen. In der Meeresenge von Gibraltar arbeitet das System mit drei fest installierten Überwachungsanlagen, die durch sieben mobile, auf Schiffen und Fahrzeugen installierten Aufklärungseinheiten ergänzt werden. Die Stationen verfügen über eine Aufklärungseinheit aus einem Hochleistungsradar sowie Infrarot- und Videokamera mit Restlichtverstärker und einer Kommunikationseinheit zur Übermittlung von Daten, Bild und Stimme. Den veröffentlichten Daten gemäß können Flüchtlingsboote ab einer Größe von circa zwei Metern in einer Reichweite von bis zu zehn Kilometern entdeckt werden. Ab einer Entfernung von fünf Kilometern können die Objekte genauer identifiziert und Personen – als weiße Leuchtpunkte auf Schwarz-Weiß-Bildschirmen – sichtbar gemacht werden. Die Daten werden in einer zentralen Kommandostelle gesammelt, interpretiert sowie Richtungen und Geschwindigkeiten der Objekte berechnet. Entsprechend wird dann auch vom Bildschirmarbeitsplatz die nächstgelegene Einheit der Guardia Civil informiert und zu einem ermittelten Abfangpunkt dirigiert. SIVE wird zudem an ein im Aufbau befindliches digitales Fernmeldesystem zur verschlüsselten Übertragung von Sprechfunk und Daten angeschlossen. An zahlreichen, teils auch mobilen, Endausgabestellen wird dadurch unter anderem der Zugang zum Schengener Informationssystem (SIS) ermöglicht.[5] Die Erweiterung dieses und ähnlicher Systeme durch die Aufklärung von „fliegenden Drohnen", wie sie etwa zur Überwachung der Adriaküste bereits eingesetzt wurden, steht seit längerem zur Diskussion.[6]

Was für die blaue Grenze gilt, soll auch für die grüne Grenze gelten: jede Form der Überschreitung soll registriert werden. An Polens Grenzen zu Belarus und zu Russland wurden, schon längst bevor die deutsch-polnische Grenzkontrolle fiel, Versuche durchgeführt, optotronische Flächenüberwachung, wie sie mit dem SIVE installiert ist, mit aktiven Zäunen, unterirdischen Schrittmeldern und Thermokameras für fokussierte Erfassungen zu kombinieren. Dabei können die unterirdischen Schrittmelder, mit GPS ausgestattet, Veränderungen im elektrostatischen Umfeld exakt lokalisieren. Ins System integrierte Wärmebildkameras fokussieren dann das entsprechende Raumsegment, um die Meldungen zu verifizieren.[7] Mit der Kombination von stationären Einrichtungen und mobilen Einsatzkräften, mit der Verlagerung der Aufklärung ins Vorfeld und ins Hinterland der Grenze wird das Grenzregime auf eine neue operative Basis gestellt. Dazu gehören auch Pläne, die Grenzbeamten selbst in das Überwachungsnetz einzubinden, indem ihr Aufenthaltsort durch automatisierte Positionsmeldungen per GPS permanent

5 Vgl. G. Piper, Spaniens elektronische Mauer. Immigration zwischen Vertuschung und Kriminalisierung, in: Bürgerrechte & Polizei 69 (2) 2001, S. 55-62; Maroto, Fronteras (Anm. 3), S. 4 f.; und die Animation unter: http://www.iesparquedelisboa.org/comenius2/Inmigracion/multimedia/sive.html (16.01.2008)

6 Proceedings of the Workshop on Research and technological challenges in the field of border control in the EU-25. 18-20 October. Ljubljana, Slovenia 2004, S. 12, 51; zit. nach: http://europa.eu.int/comm/enterprise/security/doc/proceedings_en.pdf (16.01.2008)

7 Vgl. Ebd., S. 49.

überprüft wird. Die Grenzpolizei wartet nicht mehr an den Schlagbäumen auf mögliche Grenzverletzer, sie geht zu flexibleren militärischen Taktiken der Frontsicherung über.[8] Symptomatisch für die Reorganisation der Grenzkontrolle ist denn auch die zunehmende Aufrüstung mit Militärtechnologie und militärtechnischen Know-How. In zahlreichen europäischen Ländern wurde die Grenzpolizei, wie etwa der deutsche Bundesgrenzschutz, in den 1990er Jahren erstmals mit Hubschraubern, geländegängigen Fahrzeugen, Schnellbooten, Nachtsichtgeräten und ähnlichem Material ausgestattet, das meist aus militärischen (Rest-)beständen stammt. Im Kontext von SIVE werden nun High-End-Geräte militärischer Technologie unter der Leitung des spanischen Elektronikhersteller Amper Sistemas in ein speziell ausgelegtes Aufklärungssystem der Grenzpolizei integriert. Und die 2005 gegründete europäische Grenzschutzagentur hat die Aufgabe, auch die Entwicklung von Aufklärungsmitteln voranzutreiben. Generell ist die informations- und kommunikationstechnische Aufrüstung der Grenze ein zentrales Projekt der Harmonisierung der europäischen Grenzregime. Die insgesamt auf etwa 240 Mio. € veranschlagten Kosten des SIVE-Projekts werden zum Teil aus EU-Programmen finanziert. Mit EU-Geldern des PHARE-Programms zur Osterweiterung hat Estland einen Vertrag mit dem spanischen Elektronikherstellers Amper Systemas zur Installierung von SIVE an der Grenze zu Russland abgeschlossen. Im Rahmen des Umbaus des polnischen Grenzregimes, der unter anderem die personelle Aufstockung, den Aufbau von Datenbanken und die Grenzüberwachung betrifft, ist eines der teuersten Projekte die Anschaffung von fünf Hubschraubern zur Luftüberwachung (à 5 Mio. €), von 60 mobilen Überwachungsgeräten (à 413.000 €) und 236 tragbaren Wärmebildkameras (à 49.000 €).[9]

Zu beobachten ist überdies gerade im Spanischen Fall ein signifikantes institutionelles Moment: Mit der Guardia Civil kommt hier eine Organisation mit paramilitärischem Charakter zum Einsatz, die bis in die 1990er Jahre überhaupt nicht mit Grenzschutzaufgaben betraut war. Die Operationsweise, das erforderliche technische Know-How, der Umgang mit schwerer Bewaffnung und Ausrüstung scheint am ehesten in solchen Organisationen verankert, die als Zwischenform zwischen Armee und Polizei traditionell im Ruf einer institutionellen Anomalie standen. Kräfte, die nicht in routinierter Passkontrolle geschult sind, sondern für Spezialeinsätze in kleinen Einheiten, mit dem Ziel der Bekämpfung von Infiltration, militantem Widerstand und inneren Unruhen. Seit Ende der 1980er Jahre verzeichnen in nicht wenigen europäischen Staaten gerade diese Kräfte, die institutionell oft zwischen Verteidigungs- und Innenministerium angesiedelt sind, einen enormen Wachstumsschub.[10]

8 Vgl. Ebd., S. 9, 51.

9 The new border regime at Bug River, Statewatch Bulletin 13(1).2003 (Ref.6672).; zit nach: http://database.statewatch.org/protected/article.asp?aid=6672.

10 D. Lutterbeck, Between Police and Military. The New Security Agenda and the Rise of Gendarmeries, in: Journal of the Nordic International Studies Association (39) 2004, S. 45-68.

Nicht umsonst wird diese Form der Fortifikation häufig als Errichtung einer „elektronischen Mauer“[11] bezeichnet. Der technologische Übergang von Steinen und Beton zur virtuellen Mauer elektronischer Überwachung ist zugleich Ausdruck wie Bedingung der Möglichkeit einer räumlichen Flexibilisierung der Grenzregimes in Europa. Fortifizierung ist nicht mehr an die Errichtung statischer Mauern und linearer Grenzverläufe gekoppelt. Die mikropolitische Transformation des Grenzraums ließe sich in den juridischen Bestimmungen weiter verfolgen, Grenzkontrollen ins Hinterland zu verlagern, in der grenzpolizeilichen Diplomatie transnationalen Austauschs und noch bis in die diplomatischen Bestimmungen von Rückführungsabkommen. Technologien und Operationsweisen sollen sich den wandelnden Wegen und Techniken möglicher Grenzverletzer anpassen. Es geht um Kräfteverlagerung, um Positionswechsel, um die Anpassung an den fluktuierenden Verlauf der Pfade der Grenzverletzer. Die mikropolitische Verlagerung steht im Kontext einer Rekonfiguration eines Grenzregimes, das nicht mehr in punktueller, statischer Kontrolle, sondern in Kategorien eines Managements von großräumigen Bewegungen denkt. Die Grenzpolizei stellt operativ auf die Überwachung und Kontrolle von grenzüberschreitenden Strömen um. Im Kern aber operiert dieses Management, und das ist der politisch-juridische Hintergrund des technischen Programms, mit einer radikalen Exklusionsoption, die sich gegen Migranten richtet.[12]

## Zur liberalen und demokratischen Ökonomie maschinisierter Kontrolle

Freilich greift es bereits am Beispiel der Operationsform von SIVE zu kurz, allein in Begriffen und Metaphern wie Fortifikation, Mauern und militarisierter Abwehr zu denken. Einen Gutteil seiner Legitimität zieht SIVE aus dem Faktum seiner Virtualität: die Handelsströme, die lokale Fischerei und vor allem die Touristenströme werden davon nicht tangiert. SIVE funktioniert als eine Form von Grenze, die nicht vor, sondern erst nach einer Verdachtsschöpfung in Erscheinung tritt. Insofern ist der Fortifikationsmodus an eine außerordentlich subtile politische Ökonomie der Kontrolle gekoppelt. Das fortifikatorisch-exkludierende Moment, das mit SIVE errichtet wird, geht mit einer ostentativen Liberalität einher, sich für unverdächtiges Verhalten nicht zu interessieren. Der Grenzraum wird permanent überwacht, bei Grenzannäherungen und -übertritten aber wird nur im Verdachtsfall kontrolliert oder interveniert. Mit SIVE ist eine weitgehend

11 Piper, Elektronische Mauer (wie Anm. 5).

12 D. Bigo, When two become one. Internal and external securitisations in Europe, in: K. Morten/M.C. Williams, (Hrsg.), International Relations Theory and the Politics of European Integration. Power, security and community. London, New York 2000, 171-204, hier S. 184f., 190; Kaufmann, Grenzregimes (Anm. 1). Aufschlussreich zur Verknüpfung von allgemeiner Sicherheit und Wohlstand in Verbindung mit der Steuerung gewünschter Migration und der Migrationsabwehr an der Grenze – also zu den biopolitischen Optionen des Grenzregimes – ist das Dokument der britischen Regierung „Secure Borders, Safe Havens“, mit dem der Rahmen der technisch avanciertesten Grenzkontrolle in Europa bestimmt wird; Vgl. zur britischen Grenzkontrolle: UK-Home Office, Secure Borders, Safe Haven. Integration with Diversity in Modern Britain, Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty, February 2002.

immaterielle Grenze installiert, das System basiert auf einem verdeckten Monitoring des Grenzraums. Erst im konkreten Verdachtsfall setzen sich die Grenzbewacher überhaupt in Szene. Da zumindest Flüchtlingsboote relativ leicht aus der Masse des Verkehrs herauszufiltern sind, ist die Grenze durch ihren virtuellen Charakter bestimmt. Keine massierten Bauten sind zu sehen, keine Frontlinie ist markiert, eine Art „fleet in beeing" operiert jenseits der allgemeinen Sinnfälligkeit.

Das Ideal eines liberalen Modus der Grenzkontrolle besteht denn auch darin, illegale Grenzüberschreitungen zu verhindern, ohne legale zu belästigen. Anders ausgedrückt: Aus dem Strom der Güter, Fahrzeuge und Personen sollen sie diejenigen herausfiltern, welche unerwünscht oder gefährlich sind – dies aber, ohne den Strom erlaubter Grenzübertritte lahm zu legen oder zu behindern. Gegenwärtig wird an den Grenzstationen der EU denn auch mit zahlreichen neuen technischen Mitteln daran gearbeitet, diesem paradoxen Imperativ, den Durchsatz der Kontrolle zu erhöhen, ohne in den Verkehrsfluss einzugreifen, gerecht zu werden. In politische Kodierungen übersetzt, lässt sich möglicherweise davon sprechen, dass mit spezifischen Automatisierungsprozessen nicht allein ein liberaler, sondern möglicherweise auch ein demokratischer Formwandel der Grenzkontrolle einhergeht.[13]

Der erste Schritt einer solchen demokratischen Ökonomie der Kontrolle besteht darin, dass Maschinen einen Verdacht, das ist ja ihr Wesen, automatisch streuen. Automatische Streuung der Kontrolle heißt, an Häfen, Flughäfen und Landübergängen von punktueller Durchsuchung von Containern, Lastwagen, Fahrzeugen oder auch Gepäckstücken auf deren generelles Durchleuchten umzustellen. Überwachungs- und Zeitökonomie sollen auf einen Nenner gebracht werden, indem nicht mehr Dinge durchsucht, sondern automatisch durchleuchtet werden. Spuren von Personen, Drogen, Währung, Waffen, Sprengstoffen, chemischen, biologischen, radiologischen und nuklearen Gütern oder Stoffen sollen ausfindig gemacht werden. Forcierte Technisierungsstrategien lassen die Grenzkontrolle mit Röntgengeräten operieren, die nicht mehr nur Gepäckstücke durchleuchten, sondern von ihrer Durchdringungskraft und Größe geeignet sind, PKWs, LKWs und Container innerhalb von wenigen Minuten zu durchleuchten. Röntgenuntersuchungen bringen die Umrisse aller möglichen Dinge, Waren, Behältnisse, Personen auf den Bildschirm, können aber geschickte Tarnungen unter Umständen nicht entdecken. Andere technologische Entwicklungen werden hingegen zur Entdeckung bestimmter Schmuggelwaren eingesetzt. An den Ostgrenzen der EU etwa werden Schleusen und mobile Geräte zur Messung von Gammastrahlung, also zur Entdeckung von Kernelementen und nuklearem Material, eingesetzt. An den polnischen Grenzen etwa waren bereits 2004 176 fest installierte Geräte im Einsatz, durch die der Grenzverkehr der Fahrzeuge und Personen geschleust wird. Diese werden durch Handgeräte ergänzt,

13 Im Folgenden übernehme ich die Überlegungen zu einer möglichen Demokratisierung qua Automatisierung, die Dominique Linhardt in seiner glänzenden ethnomethodologischen Untersuchung von Flughafenkontrollen ausgearbeitet hat; vgl. D. Linhardt, Demokratische Maschinen? Die Vorrichtung zur Terrorismusbekämpfung in einem französischen Großflughafen (Paris-Orly), in: Kriminologisches Journal (32) 2000, S. 82-107.

um bei Alarm mögliches Strahlenmaterial zu lokalisieren und auch die Dosen zu bemessen.[14]

Stärker noch scheint diese High-Tech-Strategie der Kontrolle bei der Suche nach blinden Passagieren durchzuschlagen. Am weitesten gerüstet ist aber die britische Regierung, die 2001 in Dover ein „Centre of Excellence" mit einer „Mobile Detection Unit" eingerichtet hat. Diese arbeitet mit „cutting edge technology" – vor allem um blinde Passagiere zu entdecken. Die Einheit kann von anderen EU-Staaten angefordert werden, um an den Hauptrouten illegaler Immigration Kontrollen durchzuführen und Hilfeleistung bei der Einrichtung neuer Technologien und Verfahren zu geben. Als eines der ersten Ergebnisse dieser Arbeit wurde im Januar 2006 am Eurotunnel ein neues reguläres Kontrollverfahren eingeführt. Dort passieren planenbezogene LKWs mit einer Geschwindigkeit von bis zu 16 km / h Vorrichtungen, die mit Bildgebungsverfahren auf der Basis von Millimeterwellenfrequenzen versteckte Personen aufspüren sollen. Empfindlicher als diese Geräte sind Herzschlagdetektoren, welche auch bei mit Containern beladenen LKWs die vom Herzschlag ausgehenden akustischen Schwingungen aufzeichnen können. Während Herzschlagdetektoren nur bei Behältnissen funktionieren, die über eine Aufhängung verfügen, kann mit Geräten, die $CO_2$ aufspüren, durch die Messung an kleinsten Öffnungen die Veränderung des Sauerstoffgehalts der Luft durch versteckte Personen nachgewiesen werden.[15] Bei all diesen Verfahren jedenfalls wird der Verdacht, nukleares Material, Sprengstoff, Waffen oder Personen zu schmuggeln, automatisch gestreut. Er ist nicht abhängig von möglicherweise voreingenommenen Staatsvertretern oder konkreten Ereignissen. Die Funktionalität der Verdachtsschöpfung besteht gerade darin, sie als geregeltes Verfahren unabhängig von konkreten Ereignissen einzurichten. Mehr noch aber wird von der Person des Kontrollierten abgesehen und die Kontrolle von der subjektiven Erfahrung, den möglichen Voreingenommenheiten oder Launen der Kontrolleure unabhängig gemacht. Vielmehr operiert eine Maschine im Namen des Staates, die – so lässt sich versuchsweise sagen: in demokratischer Weise – alle in gleicher Weise einer Kontrolle unterzieht. Überdies erlangen maschinelle Verfahren ihre Legitimität nicht zuletzt durch den Anschein eines unabänderlichen Sachzwangs.[16]

Als zweites Moment kommt hinzu, dass die Effizienz der Kontrolle darauf beruht, den

14 Vgl. Proceedings (wie Anm. 6), S. 50, 56.

15 Soweit dies aus den sehr verstreuten Mitteilungen, die es dazu gibt, ersichtlich ist, ist der Einsatz der Apparaturen und auch die Verfahrensweisen keineswegs fehlerfrei oder problemlos. Herzschlagdetektoren schlagen bei Erschütterungen durch Wind oder vorbeifahrende Fahrzeuge an, Gammastrahlenmessungen reagieren unter anderem auch auf die Kaliumkonzentration in Bananen, wenn mehrspuriger Verkehr mit transportablen Geräten überprüft wird, ist unklar, aus welcher Reihe der Alarm stammt usw. Vgl. zur britischen Grenzkontrolle: UK-Home Office, Safe Haven (wie Anm. 12), S. 91-99; EU: UK setting up "Mobile Detection Unit" for external border controls. Statewatch News Online, September 2002 (Ref. 6472); zit. nach: http://database.statewatch.org/protected/article.asp?aid=6472 (16.01.2008); Eurotunnel: Safety and Security; zit. nach: http://www.eurotunnel.com/ukcP3Main/ukcFreight/ukcsafetysecurity/ukpsinfo.htm (16.01.2008).

16 Ob Legitimität allein auf Verfahren beruhen kann, ist dennoch fraglich. Auch wenn die Verfahren der Gepäckkontrolle am Flughafen zur Abwehr von Anschlägen und Entführungen in ähnlicher Weise funktionieren wie die Kontrollen, um blinde Passagiere zu entdecken, ist zu vermuten, dass Terrorabwehr und Migrationsabwehr nicht in gleichem Maße Legitimität zugesprochen wird.

Eingriff zu minimalisieren. Der zeitliche Aufwand ist gering. Zudem wird mit einer fein gesteuerten Ökonomie des Verdachts operiert, die keine totale Kontrolle erlaubt, sondern Schritt für Schritt Indizien erhebt und nach Spuren forscht – sei es von verbotenen und gefährlichen Substanzen oder von blinden Passagieren. Die Maschinen nehmen, im Gegensatz zu einem menschlichen Kontrolleur, nicht in den Blick, was alles im Gepäck oder Container mitgeführt wird, zumindest nehmen sie dies in geringerem Maße auf. Gesucht wird lediglich nach Spuren, die auf Verstöße hindeuten. Am Eurotunnel etwa wird das Fahrzeug nur dann, wenn die Durchleuchtung Anzeichen auf eine verborgene Person ergibt, einer $CO_2$-Untersuchung unterzogen. Ergibt die $CO_2$-Untersuchung ein negatives Ergebnis wird der Verdacht fallen gelassen. Lediglich wenn sie den Verdacht bestätigt, wird das Fahrzeug – im Einverständnis mit dem Fahrer – geöffnet und manuell untersucht. Verweigert der Fahrer die Untersuchung, wird ihm die Beförderung verweigert. Den Fahrern wird nicht Menschenschmuggel unterstellt, es wird lediglich geprüft, ob sich blinde Passagiere in der Ladung versteckt halten. Das Verfahren funktioniert in einer Weise, dass es ein hohes Maß an Legitimität erzeugen kann: Der Staat hat die Aufgabe, eine bestimmte Gefahr abzuwehren und Sicherheit zu gewährleisten, reduziert aber die dafür notwendigen Eingriffe, die Überprüfung der Fahrer bzw. der Fahrzeuge, auf ein Minimum.[17]

Ein weiteres Moment das weniger in Richtung demokratischer, denn liberaler Kontrollform läuft, ist die Aufforderung zur freiwilligen und, wie man etwas salopp sagen könnte – zur Do-it-Yourself Kontrolle. Eurotunnel etwa appelliert an die Sicherheit der Fahrer und ihre Sorge für möglicherweise gefährdete blinde Passagiere, um diese freiwillig zur etwas aufwändigeren $CO^2$-Untersuchung zu bewegen. Auf der britischen Seite locken die Behörden mit Straferlass, falls sich trotz freiwilliger Untersuchung am Eingang, später auf der britischen Seite des Tunnels doch ein blinder Passagier im Fahrzeug befindet. Solche Formen der Do-it-Yourself-Kontrolle haben sich auch in anderen Zusammenhängen entwickelt: Am Frankfurter Flughafen und am Amsterdamer Schiphol Airport etwa wird Vielfliegern angeboten, sich in ein spezielles Programm einzuschreiben, um Kontrollen an den üblichen Warteschlagen vorbei automatisch zu passieren. Interessenten werden zunächst einer eingehenden Sicherheitsprüfung unterzogen, können dann einen mit biometrischen Kennziffern versehenen Ausweis für die automatische Kontrolle erstehen. Das Prinzip, Daten gegen Privilegien zu tauschen, zieht somit auch in den staatlich regulierten Sicherheitsbereich ein.

Jedenfalls zielen die High-Tech-Strategien der Grenzkontrolle darauf, ein hohes Maß an Legitimität zu erzeugen: Kontrolle wird gleichförmig gestreut, sie wird auf sehr spezifische Momente begrenzt, sie wird mit dem Appell an die eigene Sicherheit, auch an die Sicherheit blinder Passagiere – ein Appell, der auch bei der Legitimation von SIVE

17 Um dies präziser zu fassen, müsste auf die unterschiedlichen Reichweiten und Aufgaben von staatlichem Grenzschutz und nicht-staatlichen Infrastrukturbetreibern eingegangen werden, was in diesem Rahmen nicht zu leisten ist.

eine Rolle spielt – verknüpft und sie ist zum Teil mit Momenten der Freiwilligkeit verbunden.

## Biometrie: Zur mikropolitischen Entdifferenzierung rechtsstaatlich etablierter Verfahren der Personenkontrolle

Personenkontrollen an der Grenze stellen fest, wer eine Person ist und ob diese Person zum Grenzübertritt berechtigt ist. Personen präsentieren sich in aller Regel in doppelter Weise an der Grenze: körperlich und in Form eines Papiers, eines Personalausweises, eines Reisepasses, eventuell eines Visums. An der Grenze repräsentiert das Papier die Person: Sie wird durchgelassen, wenn sich das Papier als echt und die darauf verbürgte Identität der Person als durchgangsberechtigt erweisen. Die Kontrolle besteht folglich aus zwei Teilen: dem Prozess der Verifizierung, in dem festgestellt wird, ob der Pass echt ist und ob eine Person tatsächlich mit der im Pass beschriebenen übereinstimmt und dem Prozess der Identifikation, in dem festgestellt wird, ob die Person zur Kategorie derjenigen gehört, welche die Grenze überschreiten dürfen oder eben nicht.
Das Zeitalter, in dem schlicht der Blick auf den Pass und das Blättern im Fahndungsbuch hinreichten, ist schon lange vorbei. Die Echtheit des Passes wird schon längst maschinell geprüft. Im Dezember 2004 beschloss der EU-Rat, mit der Begründung, to „render the travel document more secure and establish a more reliable link between the holder and the passport and the travel document as an important contribution to ensuring that it is protected against fraudulent use",[18] dass sämtliche Mitgliedstaaten maschinenlesbare Pässe mit biometrischen Daten einführen sollen. Mit dieser anstehenden biometrischen Aufzeichnung und einem eventuell mit elektronischen Daten generierten Archiv verschiebt sich allerdings das mikropolitische Gefüge grenzpolizeilicher Kontrollmöglichkeiten – und nicht allein dieser – in erheblichem Maße.
Biometrische Authentifizierungen basieren auf vier Schritten: Zunächst werden Personenmerkmale, die zur Identifizierung herangezogen werden, in biometrischer Form aufgenommen. Dann werden diese Aufnahmen gespeichert – dies kann in einer zentralen Datenbank oder auf dezentralen Trägern geschehen. Drittens muss zur Verifizierung, etwa an einem Grenzübergang, die Aufnahme wiederholt werden: etwa das Gesicht erneut präsentiert, oder erneut Fingerabdrücke abgegeben werden. Schließlich findet ein Abgleich der aktuellen mit der gespeicherten Aufnahme statt.[19] Die biometrische Aufzeichnung erlaubt zunächst, den Verifikationsprozess zu automatisieren. Ob die Daten im Pass – in der Regel Photo, Augenfarbe, Körpergröße – mit der Person übereinstimmten, die sich an der Grenze präsentierte, blieb den hermeneutischen Künsten der Grenzbeamten überlassen. Die biometrische Aufzeichnung übersetzt nun das kon-

18 Council Regulation No 2252/2004, 13. Dezember 2004.
19 Vgl. European Commission, Institute for Prospective Technological Studies, Biometrics at the Frontiers: Assessing the Impact on Society. For the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), Technical Report Series 2005, S. 11, 31.

tinuierliche Erscheinungsbild in diskontinuierliche Daten, in Zahlenwerte – sei es das Gesicht, die Iris, den Fingerabdruck. Zahlenwerte, die eben von Maschinen ausgelesen werden können. Verifizierung bedeutet, dass ein Automat eine aktuelle Aufzeichnung von der Person vornimmt, die sich vor ihm präsentiert, um die so ermittelten Daten mit den im Pass auf einem Chip gespeicherten Daten zu vergleichen .

Die Verfahren, mit denen biometrische Daten ermittelt werden – und dies ist die erste Form der Entdifferenzierung – gleichen denen erkennungsdienstlicher Behandlungen: Exakt definierte Haltungen müssen eingenommen, Blickrichtungen und Abstände zu den Aufnahmegeräten präzise eingehalten werden usw. Während die bisherigen Verfahren, persönliche Spuren in Ausweise aufzunehmen, in der Regel Photo und Unterschrift, durchaus Spielräume in der Ausführung ließen, erfordert die digitale Aufnahme weitaus präzisere Standards. Der interpretativ zu füllende Raum zwischen einer Person und ihrem Ausweis soll geschlossen werden, „as if the identity card were glued to your body".[20]

Die Rede von „glued", der Verweis auf eine Stigmatisierung, hat seine Berechtigung: Die Verfahren verallgemeinern eine Behandlung, die in bisherigen rechtsstaatlichen Traditionen den Verdacht eines schweren Verbrechens voraussetzte. Dies trifft vor allem auf die Abnahme von Fingerabdrücken zu. Während die verallgemeinerte Verdachtsschöpfung bei der Warenkontrolle an der Grenzen sich auf eine bestimmte Situation richtet und offengelegten, präzise definierten Regeln folgt, wird hier ein unspezifischer Verdacht an die Person geheftet. Prophylaktisch werden von ihr in gleicher Weise Daten aufgenommen, wie bei einem Verbrecher.[21]

Die Differenz in der Behandlung zwischen polizeilich verdächtigen bzw. gesuchten und unverdächtigen Bürgern lässt sich in der Datenspeicherung wieder einführen. Die Gretchenfrage ist dabei: Werden die Daten lediglich auf einem Chip gespeichert, der in ein Dokument (Ausweis, Pass) eingefügt wird, oder werden sie in einer zentralen Datenbank vorgehalten. Während das Passgesetz in Deutschland, das als erstes EU-Land Pässe mit biometrischen Daten eingeführt hat, eine zentrale Datenspeicherung verbietet, war von EU-Seite ursprünglich eine Speicherung der Daten in einem zentralisierten „European Passport Register" vorgesehen. Diesen Plänen folgte als erstes die e-Pass Regelung in Großbritannien, die eine zentrale Speicherung der Daten vorsieht.[22] Dies würde bedeuten, eine – zumindest unter rechtsstaatlichen Prinzipien – ganz neue Art von Archiv einzurichten. Die zweite Form der Entdifferenzierung bestünde darin, an der Stelle,

20 I. van der Ploeg, The illegal body: ‚Eurodac' and the politics of biometric identification, in: Ethics and Information Technology (1) 1999, S. 295-302.

21 Dass dies dennoch kaum als Erschütterung genereller rechtsstaatlicher Prinzipien wahrgenommen wird, dürfte mit einem radikalen politisch-kulturellen Wandel in Bezug auf die Preisgabe persönlicher Daten zusammenhängen. In diesem Kontext zieht biometrische Erkennung in zahlreichen Ebenen ein: sei es bei den „do-it-yourself-Kontrollen" an Flughäfen, auf die schon verwiesen wurde, oder auch in den Zahlungsverkehr etwa an Supermarktkassen, an denen man per Fingerabdruck bezahlen kann.

22 Vgl. The road to „1984" Part 2 - EU: Everyone will have to have their fingerprints taken to get a passport. Statewatch Bulletin, Febr. 2004 (Ref. 25427); zit. nach: http://database.statewatch.org/protected/article.asp?aid=25427; UK: e-border plan to tackle "threats", Statewatch Bulletin, May/June 2005 (Ref. 26671); zit. nach: http://database.statewatch.org/protected/article.asp?aid=26671.

an der bisher lediglich ein Fahndungsbuch zur Verfügung stand, das inzwischen durch das Schengener Informationssystem (SIS), durch Interpol- und nationale Polizeidatenbanken abgelöst ist, ein Archiv mit den Daten aller Bürger – zumindest aller, die einen Pass beantragen – zu errichten, in dem sich in gleicher Weise gesuchte und unverdächtige Personen befinden.

Mit dem Abgleich in einem zentralen Register fallen auch die Kontrollschritte der Verifikation und der Identifikation zusammen, da die Überprüfung des Konnex' zwischen Person und Pass zugleich mit der Anfrage im Datenregister verbunden ist, das Auskunft über seine Person gibt.[23] Eine ganz spezifische Form, Körper und Datenbank zu verschalten, ist mit EURODAC installiert. Seit 2003 werden in der EU von Asylbewerbern und illegal eingereisten Personen die Fingerabdrücke genommen und in einer zentralen Datenbank, eben EURODAC, gespeichert. Bei Kontrollen an Grenzstationen oder durch nationale Polizeien, die über mobile Eingabegeräte verfügen, werden die Fingerabdrücke von Asylbewerbern und Migranten – oder diejenigen, die man dafür hält – überprüft. Die Daten werden dabei nicht über den Umweg von Pässen abgeglichen, vielmehr werden die Körper selbst zum Ausweis. Das System soll feststellen, ob ein Asylbewerber – möglicherweise unter anderer Identität – bereits anderweitig ein Gesuch gestellt hat oder auch ob eine Person sich außerhalb einer erlaubten Aufenthaltszone bewegt. Technisch handelt es sich hier um einen Abgleich von 1 : n, um einen Abgleich mit der Datenbank, in dem festgestellt werden soll, wer er ist und zu welcher Kategorie der Kontrollierte zählt. Die biometrische Kennzeichnung der Person ist das komplementäre technologische Moment zur juridischen Restriktion, dass die Ablehnung eines Antrags auf Asyl in einem Land für die ganze EU gilt. Bereits im ersten Jahr wurden über 250.000 Eingaben gemacht und über 17.000 Versuche abgelehnter Bewerber, woanders erneut einen Asylantrag zu stellen, sollen damit aufgedeckt worden sein. Die juridische und technische Verdichtung der Grenze gehen Hand in Hand.[24]

Auch mit dem gegenwärtigen Aufbau und Ausbau von Datenbanken verbindet sich eine weitere Form der Entdifferenzierung ehemals getrennter Bereiche staatlichen Zugriffs. Seit 2007 wird am Schengener Informationssystems (SIS II) gearbeitet. Mit SIS II verändert sich das Konzept dessen, was einst ein Fahndungsbuch war – im Fall von SIS eines für grenzpolizeiliche Zwecke – in erheblicher Weise. Auch wenn die technische Umsetzbarkeit, die legislative Absicherung und die operative Handhabung in vielerlei Hinsicht noch unklar sind,[25] knüpfen sich an die neue Datenbank sehr weitreichende

23 Auch ohne zentrales Register ist bei den Nutzern der Iris-Scanner-Erkennung an Flughäfen die Verifikation bereits an die Identifikation gekoppelt, da automatisch eine Anfrage im SIS gestartet wird.

24 Vgl. The road to „1984", (Anm. 20). Die Funktionalität und auch die Fälschungssicherheit solcher Technologien nicht überschätzen. Fingerabdrücke z.B. sind bei ca. 5% der Bevölkerung gar nicht verwertbar, im Falle einer Schnittwunde können sie vorübergehend unbrauchbar sein und Fingerabdrücke wurden auch schon durch recht einfache Silikonfälschungen imitiert; vgl. European Commission, Biometrics at the Frontiers, (Anm. 19), S. 50-53.

25 So scheint man in vielen Bereichen noch weit von einer Harmonisierung und Standardisierung der Technologien und Verfahren entfernt. Die Zollbehörden etwa verfügen noch nicht einmal über kompatible Funksysteme und auch in Bereichen, wo wie mit dem SIS einheitliche Systeme existieren, ist die Handhabung in zahlreichen

Erwartungen auf zwei Ebenen. Es geht zum einen darum, dass die Grenzkontrolle, vor allem in der Funktionsweise und Handhabung ihrer Informationssysteme, nicht mehr allein auf konkrete Gefahrenabwehr, sondern auf Prävention abstellt, zum anderen darum, dass sie, wie andere Informationssysteme, insbesondere das Europol-Informationssystem sowie SIS II, „in naher Zukunft neben einem reinen Informationssystem auch ein Ermittlungssystem sein könnte".[26]

Zum Präventionssystem wird die Grenzkontrolle durch eine datentechnisch ermöglichte Flexibilisierung der Selektionskategorien. SIS war auf sechs Formen von Einträgen festgelegt – Personen, die zur Verhaftung oder Auslieferung ausgeschrieben sind; Personen, denen die Einreise ins Schengengebiet zu verweigern ist; vermisste und gefährliche Personen; Personen, die vor Gericht erscheinen sollten; Personen, die unter Aufsicht zu stellen sind; verlorene und gestohlene Sachen. SIS II soll hingegen von der Datenbankstruktur her progressiv ausgelegt werden. Das heißt, es können je nach Lagewandel neue Kategorien hinzugefügt werden – konkret etwa „violent troublemakers", die sowohl „hooligans" wie auch „protesters" umfassen können. Waren die Datenkategorien, welche die erfassten Personen beschreiben, bisher auf neun beschränkt, so können nun beliebig viele hinzugefügt werden – etwa biometrische Daten, die Erfassung von Adressen, von Sprachkenntnissen usw. SIS II erlaubt überdies, Verbindungen zwischen einzelnen Datenkategorien herzustellen, etwa Verbindungen zwischen verschiedenen registrierten Personen einzugeben. Mit seinem datentechnisch klar eingegrenzten Setting war das ursprüngliche SIS nichts anderes als ein gedrucktes Fahndungsbuch. Es enthielt lediglich spezifische, für den Umgang mit einer Person an der Grenze relevante Informationen (Durchlassen, Nicht-Durchlassen, verschärfter Kontrolle unterziehen) und die einzigen Differenz zum Buch bestand darin, dass es, eben weil es elektronisch vorlag, stets in aktueller Fassung abrufbar war. SIS bietet nun Möglichkeiten, Daten zu gruppieren, zu analysieren und zu kombinieren. Es erlaubt eine erweiterte Profilbildung, beliebige Kategorisierungen und die Bildung von Risikoprofilen. Das Erfassungssystem ist nicht mehr darauf eingestellt, bestimmte mit einzelnen Personen verbundene Gefahren abzuwehren, sondern sich auf ad hoc entstehende Problemlagen einzurichten. In präventiver Absicht lassen sich aus den Daten Kategorisierungen bilden, die einer spezifischen Behandlung unterzogen werden.[27]

Die Optionen, die sich damit ergeben, hat die britische Regierung mit ihrem „e-border programme" offen zum Ausdruck gebracht.[28] Sie verknüpft die seit April 2004 geltende Verpflichtung für Transportunternehmen, Namenslisten der Passagiere im Voraus zu

Details nicht standardisiert: für eine Datenbank ist ein „VW-Golf" eben kein „VW 17", „blue metallic" etwas anderes als „light blue" und „Mikhail Khodorkovsky" ist nicht „Michail Chodorkovskij"; vgl. Proceedings, (Anm. 6) S. 88.

26 EU-Tätigkeitsberichte: Zusammenfassung der Gesetzgebung: Schengener Informationssystem (SIS II), letzte Änderung 03.11.2006; zit. nach: http://europa.eu.int/scadplus/leg/en/lvb/l33183.htm (16.08.2008).

27 Siehe EU: Schengen Information System II - fait accompli? Statewatch Bulletin Jan./Febr. 2005 (Ref. 26448); zit. nach: http://database.statewatch.org/protected/article.asp?aid=26448.

28 UK ist zwar nicht dem Schengener Abkommen beigetreten, partizipiert aber am SIS II. Vgl. zum e-border Programm: UK: e-border plan, (Anm. 22).

übermitteln, mit den neuen Datenbankoptionen. Passagiere werden bereits im Vorfeld in Kategorien klassifiziert , die mit unterschiedlicher Kontrollintensität verbunden sind, mögliche Sicherheitsrisiken sollen so schon vor der Ankunft der Passagiere abgeklärt werden und die Grenzbehörden letztlich die „ability to deny travel" erhalten. Die Grenze ist damit an den Abreiseort verschoben. Und mehr noch: Zumindest die britische Regierung sieht vor, die Daten über längere Dauer zu speichern. Nicht das einmalige Aufsuchen von Personen, sondern ein routinemäßiges Überwachen des Reiseverhaltens ist beabsichtigt. Dies korreliert mit den Erweiterungen, wie sie SIS II vorsieht: Prävention besteht darin, Daten zusammenzuführen, um nicht nur wie die traditionelle Kontrolle einzelne Reisende abweisen oder durchlassen zu können, sondern um Risikoprofile zu erstellen, nach denen Reisende vorab kategorisiert werden.

Die Erwartung, dass SIS II als Ermittlungssystem funktionieren kann, verknüpft sich mit der biometrischen Datenspeicherung. Alle Datenbanken, die biometrische Daten enthalten, also auch eine Passdatei aller Bürger, erlauben, das Informationssystem zum Ermittlungssystem zu transformieren. Momentane Systeme leisten dies zwar noch nicht, aber alle Erwartungen gehen dahin, dass zukünftig jeder eingegebene Datensatz, der von Photos, Videos, Fingerabdrücken eines Unbekannten stammt, sofern er biometrisch aufbereitet wird, mit den biometrischen Daten von Datenbanken, die personenbezogene Daten enthalten, abgeglichen werden kann.[29] Der Übergang von einem Informationssystem, das Daten zu gesuchten Personen enthält, zu einem Ermittlungssystem, das Zuordnungen von Vorkommnissen und Taten zu Personen etabliert, wird fließend. Die Einführung biometrischer Datenbanken unterläuft – zumindest in der Form, in der sie gegenwärtig konzipiert sind – rein technisch die Differenz von grenzpolizeilicher Kontrolle und polizeilicher Ermittlungsarbeit. Sofern biometrische Daten gespeichert werden, wie SIS II und das damit verbundene Informationssystem für Visa (VIS) dies vorsehen, lassen sich Ermittlungen in den Datenbanken durchführen, da wie in Verbrecherdateien Fingerabdrücke, digitalisierte Photos und eventuell weitere Daten zur automatischen Suche zur Verfügung stehen. Die Kombination von biometrischen Daten und Datenbanken erlaubt dann nicht allein die Verifizierung und Identifizierung einer Person, sondern auch das Screening: das Herausfiltern eines bestimmten personenbezogenen Datensatzes durch den Abgleich mit einem unter welchen Umständen auch immer entstandenen Datensatzes, der unabhängig von einer Zuordnungsmöglichkeit existiert.

Die technikpolitisch forcierte Entdifferenzierung rechtstaatlicher Verfahren der Grenzkontrolle ist ein wesentliches Element im Rahmen der Tendenz einer generellen institutionellen und räumlichen Diffusion des Grenzregimes und einer Vernetzung heterogener Instanzen und Konzepte der gesellschaftlichen Sicherheitsarchitektur. Um hier nur ein

29 Prinzipiell eignet sich die Gesichtserkennung, anders als der Fingerabdruck oder der Iris Scann, dazu, Personen aus einer Menge, etwa am Flughafen vor der eigentlichen Kontrolle herauszufiltern. Allerdings funktionieren solche Verfahren auf dem gegenwärtigen technischen Stand nur unter ganz spezifischen Bedingungen (etwa Lichtverhältnisse) und weisen eine sehr hohe Fehlerrate auf; vgl. European Commission, Biometrics at the Frontiers (wie Anm. 19), S. 48 f.

Beispiel dafür zu nennen, kann nochmals auf EURODAC verwiesen werden:[30] Die Datei war institutionell und räumlich im Wesentlichen auf Grenzkontrolle und für Asylbehörden bestimmt. Inzwischen ist aber auch die britische Polizei mit Fingerprint-Scannern und mobilen Ausgabestellen der Datenbank ausgerüstet, um verdächtige Ausländer überall im Land zu kontrollieren.[31]

## Schluss

Im Zeitalter der *Ströme* wird auch das Grenzregime, gestützt auf neue Technologien der Überwachung und Kontrolle netzwerkförmig rekonfiguriert. In räumlicher Hinsicht mit der Verdichtung, Verlagerung und Flexibilisierung der Raumüberwachung in institutioneller Hinsicht mit der Verflechtung der Operationsformen und Informationsbasen heterogener Institutionen, die nicht allein Visa-Abteilungen, Konsulate, nationale wie internationale Polizeibehörden integrieren, sondern auch private Transportunternehmen in das System einbinden. Dabei scheint die Kontrolle mit Technologien zu operieren, die sich politisch mit drei unterschiedlichen Codes verbinden.

Erstens hat man es mit einem sehr archaischen, quasi militärischen Modus der Abschottung und Abgrenzung zu tun. Daran machen sich ja auch die Metaphern der Kritik wie „Festung Europa", oder „Lagerkomplex" für Flüchtlinge fest. Technologisch und konzeptionell greift hier ein Denken in umfassender Aufklärung, räumlicher Abschottung, aber auch in flexiblen Taktiken, in räumlicher Streuung, Verlagerung, Schwerpunktbildung in die Grenzkonzeption über.

Zweitens schließt das, was versuchsweise als liberale und demokratische Formen der Kontrolle bezeichnet wurde, an einen Typus versicherungsförmiger Macht an. Die Kontrolle appelliert hier an die Einsicht und an das Eigeninteresse der Kontrollierten. Sie operiert mit einer vorsichtigen Ökonomie der Kontrolle, bei der sich die Formen der Datenerhebung und die Streuung von konkreten Verdachtsmomenten in einer kalkulierten und offenen Politik wechselseitig bedingen. Es handelt sich um Formen diskontinuierlicher, diskreter Kontrolle, wie sie gesellschaftlich weit gestreut, aber unverbunden nebeneinander stehen – so etwa, wenn Zollkontrolle und Flugsicherheit prinzipiell voneinander getrennt sind, oder wenn Gesundheitsbehörden und Banken ganz heterogene Daten zur Kundenverwaltung in heterogenen Kontexten und zu ganz unterschiedlichen Zwecken erheben. Dies lässt sich durchaus als eine Form liberalisierter Kontrolle und Steuerung verstehen.[32]

Drittens aber zeichnet sich in den Archiven eine Konfiguration ab, diskontinuierlich erhobene Daten zu kompilieren und miteinander zu verknüpfen. Kontrolle geht da-

30 Ausführlich dazu: Kaufmann, Grenzregimes (wie Anm. 1).

31 Vgl. The road to „1984" (wie Anm. 22).

32 Kevin Haggerty und Richard Ericson haben dafür den Begriff "surveillant assemblage" ins Spiel gebracht; K. D. Haggerty / R. V. Richard, The surveillant assemblage, in: British Journal of Sociology (51) 2000, S. 605-622.

bei eher in Form autoritärer Gewalt von einem zentralen, undurchsichtigen oder aber nur schwer durchsichtigen „Apparat" aus, der sich die Daten und Technologien der gestreuten Sammlungen aneignet.[33] Es entsteht ein Apparat, der Daten von nichtstaatlichen Stellen, wie etwa Reise- und Transportunternehmen, administrativer, polizeilicher, grenzpolizeilicher, oder geheimdienstlicher Natur zusammenführt. Die Operationsweise eines solchen Apparates hat man nach 9/11 am Werk gesehen, als Schalterbeamte mit einem Blick in den Computer Bürgern, die aus für sie selbst nicht nachvollziehbaren und juristisch nicht überprüfbaren Gründen auf *no-flight*-Listen geführt werden, die Beförderung verweigerten.
Charakteristisch für gegenwärtige Grenzregimes jedenfalls ist weder der eine oder andere Modus des Regierens, sondern eher die Fähigkeit, je nach Lage flexibel von einem Modus in den anderen umschwenken zu können.

33 Einen solchen "apparatus" sieht David Lyon vor allem in der Folge von 9/11 aufziehen; D. Lyon, Technology vs. 'Terrorism': Circuits of City Surveillance since September 11th, in: International Journal of Urban and Regional Research (27) 2003, 666-678, hier S. 674.