Mit der Eingrenzung der Online-Durchsuchung und dem Urteil gegen den "Großen Lauschangriff" hat das Bundesverfassungsgericht Schäubles Überwachungsmanie Grenzen gesetzt. Doch das grundgesetzliche Gebot unbedingter Achtung einer Sphäre der ausschließlich privaten – "höchstpersönlichen" – Entfaltung droht durch eine "europäische Sicherheitsarchitektur" umgangen und ausgehöhlt zu werden.
Christine Wicht gibt einen Überblick über die Vielzahl schon eingeführter und geplanter europaweiter Überwachungsmaßnahmen durch Datennetze und Ermittlungs- und Informationstechnologien.

Vom 28. bis 30. Januar fand in Berlin der 11. Europäische Polizeikongress statt. 1703 Teilnehmer aus rund 61 Nationen diskutierten über die europäische Sicherheitsarchitektur. Der diesjährige Kongress stand unter dem Motto "Europäische Sicherheitsarchitekturen – Informationstechnologie, Ermittlung, Einsatz". Das Komitee für Grundrechte und Demokratie rief gemeinsam mit anderen Gruppen zu einer Demonstration auf, weil der Europäische Polizeikongress eine Propagandaveranstaltung für die Überwachung der Bürger sei. Die Demonstration richtete sich unter anderem gegen Vorratsspeicherung von Telefon- und Internetdaten, Videoüberwachung und gegen das Aufweichen der Grenzen zwischen Polizeien und Geheimdiensten. Wenn die Vielzahl unterschiedlichster Überwachungsmaßnahmen europaweit erst einmal eingeführt ist, droht aus dem bisherigen Überwachungsmosaik eine umfassende Observationskonstruktion zu werden.

Sieht man einmal von der allgemeinen Bedrohung des jüngst vom Bundesverfassungsgericht definierten "Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" ab, so könnte es für die Bürger richtig gefährlich werden, wenn sich aufgrund unzureichend ausgereifter technischer Mittel oder Computerpannen Fehlerquoten häufen und Menschen in Verdacht geraten können, die unschuldig sind, aber ihre Unschuld nicht beweisen können, weil elektronische Daten, auch wenn sie falsch sind, gegen ihre Unschuld sprechen.

Nur etwa 400 Bürger haben vor dem Kongressgebäude gegen die zunehmende Überwachung und die damit einhergehende Bedrohung ihrer Grundrechte demonstriert. Das dürfte vor allem daran liegen, dass die europäische Sicherheitsarchitektur ein äußerst kompliziertes Netz verschiedenster Überwachungsmaßnahmen auf unterschiedlichsten Gebieten darstellt. Für den EU-Bürger, der künftig mit weiteren Bedrohungen seiner informationllen und Bewegungsfreiheit rechnen muss, wird das Überwachungsnetz zunehmend engmaschiger und vor allem immer ungreifbarer.

Veranlasst durch immer differenziertere hoheitliche Überwachungsmaßnahmen entwickelt sich für einschlägige Unternehmen das Thema „Sicherheit" zu einem äußerst lukrativen

Geschäftsfeld. Kein Wunder dass auf dem Polizeikongress geradezu eine Messe der Sicherheitsindustrie stattfand. Zahlreiche Firmen präsentierten ihr neue Technologien zur Datenübermittlung, biometrische Systeme zur Personenerkennung und Neuerungen über die Kontrolle von Internetdaten.

Teilnehmer des Polizeikongresses
Die Teilnehmer des Kongresses, die sich da bezeichnenderweise unter der Überschrift "axis of evil" (Achse des Bösen) versammelten, setzten sich zusammen aus Vertretern europäischer Länder und Gaststaaten. Eingeladen waren Vertreter von Kriminal- und Schutzpolizeien, Grenzpolizeien, Sicherheits- und Nachrichtendiensten sowie der Regierungen und Parlamente (Innenminister, Justizminister, Europaabgeordnete, Staatssekretäre, Behördenleiter, Polizei- und Grenzschutzbehörden) und Konzernvorstände aus 61 Ländern. (Teilnehmerliste).

Stark präsentiert waren darüber hinaus Unternehmen von Sicherheitstechnologien. Zahlreiche Interessenvertreter der Sicherheitsindustrie referierten zu sicherheitspolitischen Themen. Der Kongress wurde bezeichnenderweise unter anderem von der European Aeronautic Defense and Space Company (EADS) und dem Software-Konzern SAP finanziert. Außerdem nahmen Unternehmen, die im Sicherheits- oder Komminikationssektor oder in der IT-Branche tätig sind, am Kongress teil, wie beispielsweise: Motorola, Siemens, Giesecke & Devrient, IBM, IABG, 3M, das Logistikunternehmen empolis (gehört zu Bertelsmann) und die seit einigen Jahren privatisierte Bundesdruckerei.

Nun aber zu den auf dem Kongress thematisierten schon verwirklichten oder noch geplanten Überwachunssystemen:

Das Visainformationssystem (VIS)

Der Vizepräsident der Europäischen Kommission, Franco Frattini, zuständig für Justiz, Freiheit und Sicherheit, forderte auf dem Kongress, dass die Freiheit, die durch die Schengen-Erweiterung entstanden sei, mit einer Stärkung der Sicherheit im Innern wie nach außen einhergehen müsse. Frattini kündigte an, dass die EU-Kommission im Februar ein Mitteilungspaket mit drei Vorschlägen veröffentlichen werde, wie die EU- Außengrenzen besser gesichert werden sollen. (Dieses ist abzurufen unter [PDF – 524 KB]).

Es soll ein so genanntes „Entry-Exit-System" entwickelt werden, das Einreise-Informationen elektronisch speichert und vernetzt. Auf diese Weise sollen z.B. abgelaufene Visa sofort erkannt und ein automatischer Alarm bei Überschreitung der Visafrist ausgelöst werden. Der herkömmliche Reisepass mit Stempel und Foto ist somit nur noch ein Anachronismus.

Die Zukunft gehöre nach Überzeugung Frattinis der elektronischen Erfassung der Reisenden. So enthält beispielsweise das europäische Visainformationssystem (VIS) 70 Millionen Fingerabdrücke von Personen, die im Schengenraum einen Visaantrag gestellt haben. Ähnlich wie die USA will nun auch die EU-Kommission die Einführung elektronischer Reisegenehmigungen prüfen (Electronic Travel Authorisation = ETA). Das Visainformationssystem VIS steht in engem Zusammenhang mit dem Schengeninformationssystem SIS II.

Das Schengener Informationssystem (SIS)

Für Innenminister Wolfgang Schäuble (CDU) bedeutet die Schengen-Erweiterung ein Mehr an Freiheit und zugleich ein Mehr an Sicherheit. Der EU-Bürger sieht das Schengen-Abkommen in erster Linie als Erleichterung der Grenzüberquerung ohne zeitaufwändige Passkontrollen, doch das Schengeninformationssystem SIS II ist keine simple Datenbank mehr, sondern ein Informationssystem mit dem Schwerpunkt „Prävention und Erkennung von Bedrohungen der öffentlichen Ordnung und Sicherheit“.

Am 21. Dezember 2007 fielen die Grenzkontrollen für die Bürger der Länder Estland, Lettland, Litauen, Polen, Tschechien, Slowakei, Ungarn, Slowenien und Malta weg. Jedoch sind mit dem Schengenabkommen nicht bloß die Grenzkontrollen weggefallen, sondern es wird im Gegenzug auch die intensivere Zusammenarbeit und die Koordinierung zwischen den Polizeidiensten und Justizbehörden zur Bekämpfung des organisierten Verbrechens geregelt. Die umfangreiche Datenbank, das Schengener Informationssystem (SIS), wurde geschaffen, um Strafverfolgungs-, Justiz- und Konsularbehörden der EU-Mitgliedstaaten einen optimalen Datenzugang über bestimmte Personengruppen zu ermöglichen. Das SIS ist seit 1995 im Einsatz. Die Erweiterung der Datenbank, SIS II, mit deren Hilfe biometrische Daten, Fotos und Fingerabdrücke gespeichert werden, sollte Ende 2007 eingeführt werden. Die Einführung wurde offenbar aus technischen Gründen verschoben.

SIS und VIS wurden verknüpft, um Personen an den Außengrenzen der EU identifizieren und Abschiebungen vornehmen zu können. Deshalb sind SIS und VIS wiederum an FRONTEX und an die Fingerabdruckdatei EURODAC (in der die Daten aller Asylbewerber, die in den Schengenraum einreisen bzw. sich dort aufhalten, registriert werden) angeschlossen.

Zugriff auf SIS II haben darüber hinaus die Kraftfahrzeugzulassungsstellen, die europäische Justizbehörde Eurojust und die Europäische Polizeibehörde EUROPOL, die unter Einhaltung der jeweiligen Bestimmungen Daten auch an Dritte weitergeben kann. Des Weiteren können Justizbehörden der Mitgliedstaaten und Schengen-interne Sicherheitsdienste und

Geheimdienste die Daten abrufen. Vor allem der Zugriff von Geheimdiensten wird in Deutschland als problematisch angesehen. Die Linksfraktion im Bundestag hat bereits mehrfach versucht, den Zugriff von Geheimdiensten zu verhindern, jedoch ohne Erfolg (Quelle: www.rosalux.de [PDF – 372 KB]). Der Bundesbeauftragte für den Datenschutz, Peter Schaar sprach sich dagegen aus, das VIS für Geheimdienste zu öffnen, auch weil diese keine Strafverfolgungsbehörden im klassischen Sinne darstellen. Die Vernetzung von Polizei und Geheimdiensten ist insofern äußerst problematisch, als es in anderen EU-Ländern das Trennungsgebot zwischen Polizei und Geheimdiensten nicht gibt, wie es in Deutschland aufgrund der Erfahrung mit der Gestapo rechtlich verankert wurde.

In diesem Zusammenhang ist interessant, dass Schäuble noch in diesem Jahr den automatisierten Zugriff aller EU-Polizeibehörden auf bestimmte nationale Datenbanken anstrebt; dies wird von Schäuble als ein Quantensprung im Bereich des internationalen Datenaustausches gesehen.

Frattini propagierte überdies den grenzüberschreitenden Informationsaustausch der Vernetzung von Polizei-Datenbanken und war sich mit Schäuble über eine Kooperation der nationalen Sicherheitsbehörden und der Geheimdienste einig. Es ist wahrscheinlich nur eine Frage der Zeit bis diese Kontrollsysteme, die momentan zur Migrationskontrolle eingesetzt werden, kontinuierlich auf die gesamte EU-Bevölkerung ausgeweitet werden. Die Freiheit stirbt bekanntlich scheibchenweise.

Einreiseregister

Um Terroristen und illegale Einwanderer aufzuspüren, plant die EU-Kommission ein Ein- und Ausreiseregister, an das eine Datenbank mit biometrischen Merkmalen wie Fingerabdrücken und elektronisch lesbaren Gesichtsformen gekoppelt ist. An den Grenzen der EU werden jährlich rund 300 Millionen Ein- und Ausreisen registriert. Schätzungen gehen davon aus, dass 160 Millionen Grenzübertritte durch EU-Bürger erfolgen, 60 Millionen Reisende kommen aus Drittstaaten, die kein Visum benötigen (wie USA oder Kanada) und 80 Millionen Reisende aus Drittstaaten mit Visumspflicht.

Geplant ist nun, dass jeder, der in die EU einreisen will, seinen Fingerabdruck abgeben muss. Die EU-Bürger selbst erhalten in den nächsten Jahren Schritt für Schritt neue Ausweispapiere mit elektronisch gespeicherten, biometrischen Merkmalen. Die Erfassung der biometrischen Daten von Drittstaatsangehörigen, die für die Einreise in die EU ein Visum benötigen, ist in Vorbereitung. Aber auch wer als Drittstaatsangehöriger ohne Visum einreisen kann, wird zur Abgabe des Fingerabdrucks verpflichtet sein. Betroffen wären davon neben US-Bürgern und Kanadiern auch Japaner und Australier, die für einen

Kurzaufenthalt bis zu drei Monate kein Visum benötigen. Das geplante Register, das die Daten von den insgesamt 1792 Grenzkontrollstellen an den Außengrenzen und innerhalb der EU (darunter Flug- und Seehäfen) austauscht, soll die Möglichkeit des Visa-Missbrauchs reduzieren.

Für Reisende, die als „vertrauenswürdig“ gelten, soll es eine bevorzugte Grenzabfertigung geben, unabhängig davon, ob sie EU-Bürger sind oder aus Drittstaaten stammen. An Grenzübergängen und Flughäfen wird die Aufstellung von Lesegeräten angestrebt, die die biometrischen Daten im Reisepass mit denen des Passinhabers abgleichen sollen und dann automatisch eine Schranke öffnen, schlug Frattini vor. An einigen europäischen Flughäfen sind solche automatischen Grenzkontrollsysteme bereits im Einsatz. In Frankfurt läuft ein Modellprojekt, bei dem Passagiere mittels Iris-Scan identifiziert werden. Die Kosten für solche Systeme liegen laut Kommission bei rund 35.000 Euro je Gerät.

Die Kosten für die Schaffung des Ein- und Ausreiseregisters und des Systems für registrierte Vielreisende beziffert die Kommission auf 20 Millionen Euro. Die Mitgliedstaaten müssten zusammen nochmals etwa 35 Millionen Euro für die automatisierten Kontrollpunkte ausgeben. (Quelle: ec.europa.eu [PDF – 524 KB]).

Wenn dieses System eingeführt wird, können alle in die EU Ein- und aus der EU Ausreisende kontrolliert werden, weil der elektronische Reisepass mit einem Funkchip ausgestattet ist, der eine Datenabfrage ohne persönlichen Kontakt ermöglicht. Auf die bei den Meldebehörden gesammelten biometrischen Daten haben im Übrigen auch Polizeivollzugsbehörden Zugriff. Wenn man bedenkt, welche Diskussion die Meldung der Fluggastdaten an die USA bei uns ausgelöst hat, dann ist es bemerkenswert, dass dieser weitere, elementare Baustein im Überwachungsmosaik bisher weitgehend ohne öffentliche Aufmerksamkeit blieb.

Seinerzeit wurde trotz des Widerstands des EU-Parlaments die Datenweitergabe an die USA durchgesetzt, erst der Europäische Gerichtshof kippte das Abkommen. Der Bundesdatenschutzbeauftragte Peter Schaar kritisierte 2007 an der Vereinbarung mit den USA, dass sie, gemessen an den Vorgaben des europäischen Datenschutzrechts, unzureichend sei. Schäuble verteidigte jedoch die Vereinbarung und kündigte im letzten Jahr an, in der Europäischen Union ein vergleichbares System aufbauen zu wollen. Dieser Zeitpunkt scheint nun gekommen zu sein. Auf dem Polizeikongress löste die Forderung des EU-Kommissars Frattini, dass Fluggesellschaften künftig den nationalen Stellen, die für Risikobewertung, Strafverfolgung und Terrorabwehr zuständig sind, PNR-Daten über Flüge in die EU und aus der EU zur Verfügung stellen sollen, immerhin noch eine kontroverse Debatte aus.

Fluggastdatenspeicherung

Die Bundesministerin für Justiz, Brigitte Zypries (SPD), kritisierte den Rahmenbeschluss der EU zur Erhebung der Passagierdaten (PNR-Daten), der beinhaltet, dass bei jeder Flugreise in oder aus der EU insgesamt 19 verschiedene Daten jedes Reisenden erfasst werden. Die Justizministerin verwies darauf, dass die Weitergabekriterien „relativ großzügig" seien und dass ohne richterlichen Beschluss auf die Daten zugegriffen werden könne. Schäuble verteidigte das Vorhaben als zusätzliches Sicherheitsinstrument, räumte jedoch ein, dass die Vorschläge dem Abkommen mit den USA zur Weitergabe von Fluggastdaten ähnlich seien, und diese habe schließlich der Bundestag ohne verfassungsrechtliche Bedenken gebilligt. **Zypries warnte auf der Tagung hingegen, dass die Vorschläge zu einer europäischen Fluggastdatei mit dem deutschem Verfassungsrecht nicht vereinbar seien und wies darauf hin, dass die verdachtsunabhängige Sammlung und langjährige Speicherung von persönlichen Daten ein wesentlich schärferer Grundrechtseingriff sei als die bereits beschlossene Vorratsspeicherung von Telefon- und Internetdaten**. Zypries wies diese Pläne zurück, da sie ein weiterer Schritt in Richtung Präventionsstaat seien.

Zur Erinnerung: Das Bundeskabinett hat am 19. September 2007 dem Entwurf des Gesetzes über ein Fluggastdaten-Abkommen zwischen der EU und den USA zugestimmt. In dem Gesetz ist die Übermittlung der Fluggastdaten bei Passagierflügen in die oder aus den Vereinigten Staaten von Amerika und die dortige Datenverwendung geregelt. Die Daten werden insgesamt 15 Jahre gespeichert. Der Vertrag wird momentan im Rahmen des nationalen Rechts vorläufig angewendet und wird erst in Kraft treten, wenn in allen EU-Mitgliedstaaten die innerstaatlichen Verfahren abgeschlossen sind. Der Vertrag ist auf sieben Jahre geschlossen (und kann abgerufen werden unter: www.bmi.bund.de [PDF – 64 KB]).

Die Fluggesellschaften übermitteln jetzt die Daten direkt an das Heimatschutzministerium, (Department of Homeland Security, DHS). Die gemeldeten Daten umfassen u.a. Reiseverlauf, Reisebüro, Sachbearbeiter des Reisebüros, Informationen über Buchung, Reisestatus des Fluggastes, Bonus-Daten, Gratisflüge, sämtliche Informationen zum Gepäck, Sitzplatznummer. Es ist bis heute nicht geklärt, ob ein Betroffener von der Eintragung erfährt, wenn ihm die Einreise in die USA verwehrt wird, und ob ein Betroffener rechtlich darauf einwirken kann, dass seine Daten gelöscht werden.

EUROSUR – EU-Überwachung auf See, aus der Luft und via Satelliten

Über die genannten Sicherheitssysteme hinaus stellte Frattini eine Roadmap zur Errichtung

eines integrierten Grenzüberwachtungssystems der südlichen und östlichen Grenzen der Europäischen Union vor. Dieses soll den Namen EUROSUR (European Border Surveillance System) tragen. Durch ein lückenloses Überwachungsnetz soll künftig erkannt werden, wo illegale Flüchtlinge unterwegs sind. Laut Frattini gibt es in Europa rund 50 nationale Behörden, die sich um Grenzüberwachung und Grenzkontrolle kümmern. Deren Systeme will die EU-Kommission nunmehr vernetzen, darüber hinaus soll EUROSUR mittels Satelliten und Überwachungskameras in Flugzeugen und Drohnen Daten erfassen und weiterleiten. „Satelliten bieten die Möglichkeit, große Flächen zu überwachen, auch das offene Meer und die Küsten von Drittstaaten“, schreibt dazu die Kommission.

Schäuble sprach sich außerdem dafür aus, die Europäische Grenzschutzagentur FRONTEX und die Europäische Polizeibehörde EUROPOL weiter zu stärken. Von Kritikern wird die Kompetenzerweiterung von EUROPOL als eindeutiges Indiz für die Schaffung eines europäischen Polizeiamtes gesehen.

FRONTEX – zur Verteidigung der Festung Europa

Auf Initiative Deutschlands wurde mittels einer Verordnung des Rates der Europäischen Union im Oktober 2004 die EU-Grenzschutzagentur FRONTEX (Europäische Agentur für die operative Zusammenarbeit an den Außengrenzen der Mitgliedstaaten der Europäischen Union) mit Sitz in Warschau eingerichtet. Der Europäische Rat vom Dezember 2005 beauftragte FRONTEX, ein System zur lückenlosen Überwachung des Mittelmeerraumes sowie ein Netzwerk für die Effektivierung nationalstaatlicher Seekontrollen zu entwickeln. Die Agentur verfügt über 116 Schiffe, 23 Flugzeuge, 27 Hubschrauber, 23 Fahrzeuge, Überwachungsgeräte wie 56 Thermal- und Infrarotkameras, 33 mobile CO2-Detektoren, acht Herzschlag-Detektoren, einen passiven Bildgeber für Millimeterwellen und gut ausgerüstete Polizeieinheiten und agiert mit einem Budget von 42 Millionen Euro. Für 2008 sind 70 Millionen Euro geplant.

Das Europäische Parlament stimmte im April 2007 gegen diesen Ausbau von FRONTEX und damit gegen die gesetzliche Grundlage für die so genannten schnellen Einsatzkräfte für den Grenzschutz, RAPIDS (Rapid Border Intervention Teams). Was aus diesem Beschluss folgt ist unklar.
Diese Einsatzkräfte sollen künftig in Ausnahmesituationen für einen begrenzten Zeitraum eingesetzt werden können. Die benötigte technische Ausrüstung wird im Bedarfsfall über einen extra hierfür geschaffenen Ausrüstungskatalog (Centralised Record of Available Technical Equipment – CRATE) bereitgestellt. In der Datenbank CRATE wird das von den Mitgliedsstaaten zur Verfügung gestellte Material zur Grenzsicherung erfasst und verwaltet (Quelle: http://frontex.antira.info/glossar). FRONTEX soll längerfristig eine eigene,

uniformierte Grenzsicherungstruppe stellen, die möglicherweise von Malta aus im Mittelmeer operieren kann. Hauptaufgabe bleibt der Kampf gegen illegale Einwanderung, aber das Aufgabengebiet soll auf Terrorbekämpfung ausgeweitet werden. Mit FRONTEX soll auch die kaum bekannte "Europäische Gendarmerietruppe" (EGF) zusammenarbeiten. (Mehr Informationen über FRONTEX [PDF – 716 KB])

Die "Europäische Gendarmerietruppe" (EGF)

Die "Europäische Gendarmerietruppe" (EGF) (http://www.eurogendfor.eu/) geht auf eine Initiative der französischen Verteidigungsministerin Michelle Alliot-Marie zurück. Die fünf EU-Mitgliedstaaten Italien, Spanien, Frankreich, Portugal und die Niederlande haben im September 2004 einen Vertrag zur Gründung einer "Europäischen Gendarmerietruppe" (EGF) geschlossen. Beheimatet ist die Gendamerietruppe im italienischen Vicenza. Sie besteht im Kern aus ca. 900 Mitgliedern, die kurzfristig auf 3000 Mann aufgestockt werden kann. Aufgabe dieser europäischen Polizeitruppe ist die Aufstandsbekämpfung in Krisenregionen inner- und außerhalb der Europäischen Union. Die EGF soll aber auch mit der Grenzschutzagentur FRONTEX zusammenarbeiten, beispielsweise mit den italienischen Carabinieri, mit Küstenschutzbooten, Hubschraubern und Flugzeugen zur "Migrationsabwehr". Eine dazugehörige Akademie in Vicenza wird von den G8-Staaten finanziert. Die deutsche Polizei ist zwar der EGF noch nicht beigetreten, arbeitet aber mit polizeilichen und militärischen Einheiten anderer Länder z.B. schon im Kosovo und Afghanistan zusammen. FRONTEX wiederum arbeitet mit dem Europäischen Polizeiamt EUROPOL zusammen, wie in Artikel 13 der Verordnung des Rates 2007/2004, mit der FRONTEX geschaffen wurde, festgehalten wird:

> Die Agentur kann mit Europol und den internationalen Organisationen, die für die von dieser Verordnung erfassten Bereiche zuständig sind, im Rahmen von mit diesen Stellen geschlossenen Arbeitsvereinbarungen im Einklang mit den einschlägigen Bestimmungen des Vertrags und den Bestimmungen über die Zuständigkeit dieser Stellen zusammenarbeiten.

EUROPOL – Ein europäisches Polizeiamt

Die europäische Polizeibehörde Europol mit Sitz in Den Haag koordiniert bisher allein die Arbeit nationaler Polizeibehörden im Bereich der grenzüberschreitenden Kriminalität und soll den Informationsaustausch zwischen den nationalen Polizeibehörden fördern. Die Behörde verfügt über knapp 600 Mitarbeiter und ein Budget von etwa 65 Mio. Euro. Die

Arbeitsbereiche von Europol erstrecken sich von Terrorismusbekämpfung über Bekämpfung des Waffenhandels bis hin zu Drogenhandel, Geldwäsche und Kinderpornographie. Rechtliche Grundlage des Europol-Übereinkommens ist ein völkerrechtlich bindender Vertrag. Europol besitzt keine Vollstreckungsbefugnisse wie die Polizeibehörden der Mitgliedstaaten und darf mithin weder Personen festnehmen noch Hausdurchsuchungen vornehmen (Quelle).

In die Kritik geraten ist Europol wegen der Führung einer Verdächtigen-Datei und der Führung einer Arbeitsdatei zu Analysezwecken, weil die Gefahr besteht, dass durch solche Dateien das Prinzip der Unschuldsvermutung umgekehrt wird. Eine demokratische Kontrolle über Europol ist kaum möglich, so kann etwa das Europäische Parlament noch nicht einmal einen jährlichen Tätigkeitsbericht verlangen.

Über die Europol-Daten hinaus soll jedoch die Vernetzung verschiedener Polizeien künftig mit Hilfe eines Ad-hoc-Netzes vereinfacht werden.

Mobile Datenübertragung mit hoher Bandbreitre (HiMoNN)

Eine sichere, mobile Übertragung von Daten mit hoher Bandbreite, HiMoNN (Highly Mobile Network Node), wurde von dem Unternehmen IABG auf dem Berliner Polizeikongress vorgestellt. HiMoNN ist ein von der IABG realisiertes, mobiles Ad-hoc-Netz. Innerhalb dieses Netzes können mobile Geräte sofort eine Verbindung zueinander aufbauen, ohne dass eine übergeordnete Infrastruktur nötig ist. Darüber hinaus integrieren sich Sensoren wie Überwachungskameras und Bewegungsmelder selbständig in das Netz. Eigenen Angaben zufolge will die IABG das selbst entwickelte mobile Ad-hoc Kommunikationssystem HiMoNN mit den Galileo-PRS-Signalen koppeln und damit den Sicherheitskräften neben einem breitbandigen, sicheren Sprach- und Datenübertragungssystem eine verlässliche Georeferenz bieten. Das System wurde ursprünglich als rein militärische Entwicklung konzipiert, heute ist HiMoNN auch für Einsätze von Polizei, Grenzschutz, Feuerwehr, Rettungsdienste und Katastrophenschutz von Interesse und bereits in Hessen und Brandenburg zum Einsatz gekommen. Nach Angaben des Herstellers biete HiMoNN aufgrund seiner Leistungsfähigkeit immer dann Vorteile, wenn eine hohe Konzentration verschiedener Einsatzkräfte erforderlich sei, wie etwa bei lokalen Großereignissen (z. B. Fußballländerspiele und Demonstrationen, Quelle: www.iabg.de

Ein Vertreter des Fraunhofer Instituts stellte auf dem Kongress ein Forschungsprojekt vor, nach welchem unter Einsatz von einer Vielzahl von Sensoren z.B. 3D-Rekonstruktionen von Szenarien möglich sei. Aber auch die Verfolgung und Wiedererkennung von Personen, auch

über mehrere Kameras hinweg, sei Ziel des Projektes. Dafür befindet sich gerade das Center for Advanced Security Research Darmstadt (CASED) in Gründung.

POLIZEI-ONLINE für europäische Polizeien

Uwe Seidel, Polizeioberrat im Innenministerium Baden-Württemberg, lobte die Zusammenarbeit mit dem privaten Partner Deutsche Telekom beim PPP-Konzept POLIZEI-ONLINE, einer seit 1998 bestehenden Integrationsplattform für die polizeilichen Anwendungen sowie das Bildungs- und Informationssystem des Landes Baden-Württemberg. Über ein landesweites Portal stehen den an über 700 Standorten verteilten über 30.000 Bediensteten rund um die Uhr u.a. aktuelle Informationen, Handlungsanleitungen, Rechtsvorschriften und gerichtliche Entscheidungen zur Verfügung. Durchgeführt wird das Projekt im Rahmen einer Public Private Partnership (PPP) mit der Deutschen Telekom AG.

Die Entwicklungen in POLIZEI-ONLINE stoßen zunehmend auf internationales Interesse, weshalb die Nutzung und Weiterentwicklung des Systems auch im Rahmen internationaler polizeilicher Kooperationen erfolgen soll. Ziel ist es, ein Referenzprojekt für die europäischen Polizeien zu schaffen. In diesem Zusammenhang baut die Polizei Baden-Württemberg gemeinsam mit dem Projektpartner Deutsche Telekom AG ein vergleichbares System für die mitteleuropäische Polizeiakademie (MEPA-Mitglieder sind Polen, Ungarn, Tschechien, Slowakei, Slowenien, Österreich, Schweiz und Deutschland) auf, um die Fortbildungsmaßnahmen der MEPA zu unterstützen und die internationale Zusammenarbeit von Polizeiexperten zu fördern.

Das Projekt ist nach Ansicht der EU-Kommission geradezu maßgeschneidert für die Struktur und die Ziele der MEPA, da die Bekämpfung international operierender Tätergruppierungen ein über die Grenzen hinweg koordiniertes polizeiliches Handeln erfordere, dessen Vorbereitung, Durchführung und Erfolg nur von entsprechend qualifizierten Polizeibeamten gewährleistet werden könne. Ziel müsse es daher sein, sich alle verfügbaren Informationen rund um die Uhr erschließen zu können, organisations- und grenzübergreifende Netzwerke zu bilden und das individuelle Wissen aktuell und schnell für alle verfügbar zu machen (Quelle: www.mepa.net)

Alle nationalen Datenbanken sollen allen Mitgliedstaaten offen stehen

Bereits im deutschen EU-Ratspräsidentschaftsprogramm „Europa gelingt“ wurde eine Verbesserung und Effizienz der europäischen Datenbanken in den Bereichen Justiz und Inneres, eine Steigerung der Interoperabilität und die Eingliederung eines

Informationsverbundes gefordert. Der deutsche Vorsitz maß der Verbesserung der Zusammenarbeit der nationalen Polizeien hohe Bedeutung bei und sprach sich dafür aus, allen betroffenen Polizei- und Sicherheitsbehörden zur Bekämpfung des Terrorismus und schwerer, grenzüberschreitender Kriminalität der Zugang zu den EU-Informationssystemen (SIS, VIS, EURODAC, Zollinformationssystem) zu ermöglichen. Deshalb sollten nationale Datenbanken allen Mitgliedstaaten und Europol sowie Eurojust im Rahmen des Erforderlichen zugänglich sein. Nach Ansicht der Deutschen Ratspräsidentschaft sei es unverzichtbar, dass die Polizei- und Sicherheitsbehörden der Mitgliedstaaten über umfassende und tagesaktuelle Informationen verfügen. Zu diesem Zweck solle der Europäische Informationsverbund ausgebaut werden. Zur Bekämpfung terroristischer Bedrohungen wird sich der Vorsitz für eine arbeitsteilige Form der Zusammenarbeit aller mit der Internetüberwachung befassten Sicherheitsbehörden der Mitgliedstaaten, unter Einbindung von Europol, einsetzen (Quelle [PDF – 308 KB]).

Aufhebung der Trennung von Polizei und Militär

Aussagen von Angela Merkel wie: *"Die alte Trennung zwischen innerer und äußerer Sicherheit ist von gestern"* oder die des BKA-Präsidenten Jörg Zierke: *"Die Trennung zwischen innerer und äußerer Sicherheit ist obsolet"* sind politische Aussagen, mit dem Ziel, die Trennung von Bundeswehr und Polizei aufzuheben. Derartige Äußerungen begünstigen die Verselbständigung militärischer Strukturen. Die von den Innenministern der europäischen Mitgliedstaaten geforderten und geplanten Überwachungsmaßnahmen gehen weit über die Orwellsche Phantasie eines umfassenden Überwachungsstaates hinaus. Mit der Argumentationskrücke „Terrorismusbekämpfung" wird die Erfassung, Speicherung von Fluggastdaten, Fahrzeugdaten, die Erstellung von Biometrischen Pässen und Fingerabdrücken und die Überwachung der Migrantenströme gerechtfertigt.

Sicherheit geht vor – nach den Ursachen von Migration und Terror fragt niemand

Die Ursachen des Terrorismus werden nicht einmal im Ansatz diskutiert, statt dessen wird seine Bekämpfung mit einem enormen technischen Aufwand betrieben. Dabei werden massive Eingriffen in die Privatsphäre und die persönliche Freiheit der Bürger als angeblich problemlos in Kauf genommen. **Der Bürger hat nicht mehr die Freiheit zu wählen, ob er seine biometrischen Daten oder Fingerabdrücke abgeben will, er muss und er hat keinen Einfluss über die Verwendung seiner persönlichen Daten**.
Der gleichen Logik folgt die Bekämpfung von Flüchtlingsströmen, die mit modernster Technologie und Milliardenaufwand eingedämmt werden sollen. Auch da werden nicht die Ursachen thematisiert, schließlich sind sie ja auch kein lukratives Geschäftsfeld.

Die aufgezählten Überwachungsmaßnahmen sind allerdings höchst fragwürdige Methoden zur Bekämpfung des Terrorismus, weil sie Unverdächtigte, ja weite Teile der Bevölkerung unter Generalverdacht stellen. Die Gefahr, dass unbescholtene Bürger unverschuldet in das Fadennetz der Terrorbekämpfung geraten, dürfte weitaus höher sein, als dass ein Terrorist gefangen wird.

Die Vorgehensweise der Sicherheitsstrategen lässt vermuten, dass verworrene Hintergründe und schwer durchschaubare Vertragswerke dazu führen, dass Bürger vor der Komplexität kapitulieren, politische Entscheidungsträger mit den Folgen und Hintergründen überfordert sind und somit immer weitere Sicherheitsmaßnahmen ohne nennenswerten Widerstand eingeführt werden können. Die High-Tech-Überwachung liest sich wie ein Science-Fiction-Roman, doch sie wird bald Realität sein, insbesondere auch deshalb, weil ein wachsendes wirtschaftliches Interesse hinter dem Ausbau der grenzenlosen und lückenlosen Überwachung steht.

(zum Vertiefen)