Die Zukunft der polizeilichen Überwachung[1]

von RA und FA f. Strafrecht Dr. Ulrich Sommer, Köln

Bereits heute ist absehbar: Moderne Technologien werden die Veränderungen des alltäglichen Lebens dramatisch beschleunigen. Die Polizei wird die hierdurch zwangsläufig erzeugten zusätzlichen Datenmengen zur Aufklärung von Straftaten nutzen wollen. Der Gesetzgeber ist aufgerufen, die neue Qualität von Grundsrechtseingriffen zu erkennen und dem drohenden Verlust von freiheitlichen Handlungsräumen entgegenzusteuern.

Die Technik

hat in nur einer Dekade das Zusammenleben in der modernen Gesellschaft radikal verändert. Eine Teilhabe am sozialen Leben ohne individuellen Rückgriff auf den Computer ist kaum denkbar. Die Gewöhnung an das Tempo und die explodierende Informationsfülle verschüttet den Blick auf die revolutionären Auswirkungen der universellen Datenerfassung und deren individueller Verwendung. Das Tempo der technischen Weiterentwicklung wird ebenso beschleunigt wie ihre Auswirkungen auf das tägliche Leben. Die handschriftlich ausgefüllte Banküberweisung wird bald einer fernen Vergangenheit ebenso angehören wie zahlreiche andere Schriftstücke. Informationsgespräche und Buchlektüren werden nahezu vollständig dem dauerhaften Zugriff auf Milliarden von Internetseiten weichen.
Die Rationalisierung vieler Vorgänge des alltäglichen Lebens verspricht die Weiterentwicklung winziger Chips mit dem Namen **RFID** (Radio Frequency Identification). Stecknadelgroße stromlose Datenträger können demnächst bei Waren und Ausweiskarten umfassende Informationen speichern, die durch aktivierende Leseeinrichtungen abgerufen werden. Bar-Code und Magnetstreifen sind Technologien des vergangenen Jahrhunderts. Schon heute kann der mit einem Stapel entliehener Bücher durch eine schlichte Schranke tretende Benutzer das komplizierte Ausfüllen von Rückgabescheinen überflüssig werden lassen: Der winzige Chip in jedem einzelnen Buch dokumentiert, dass sich das Buch wieder in der Bibliothek befindet. Der Chip kann – wie in der Londoner U-Bahn – die simple Berechtigung zur Fahrt unter gleichzeitiger zeitlicher Erfassung ebenso dokumentieren wie die notwendigen Daten auf den Eintrittskarten zur Fußball-WM. Angereichert mit biometrischen Daten können Lesegeräte zahllose individuelle Angaben in dem neu herausgegebenen Pass ebenso ablesen wie Mautschranken bei durchfahrenden Kraftfahrzeugen. Die Logistik riesiger Warenbestände wird für Konzerne transparenter, wenn beispielsweise in jeder Jeans individualisierbare Produktionsdaten jederzeit ablesbar sind.
Die Verbesserung der Reichweite der Lesbarkeit ist ebenso prognostizierbar wie die Verbindung dieser Technik mit **GPS**. Wenn bereits heute als Diebstahlschutz mit Hilfe einer solchen elektronischen Erfassung der aktuelle Standort eines Fahrzeuges jederzeit feststellbar ist, ist der Weg nicht weit, jede wertvolle Armbanduhr oder Kaviardose mit ähnlichen Ortungsmöglichkeiten zu versehen.

[1] Der Vortrag wurde unter dem Titel „Offene und geheime Ermittlungsmethoden“ beim 57. Deutschen Anwaltstag am 25.05.2006 in Köln gehalten - einer Veranstaltung der Arbeitsgemeinschaft Informationstechnologie und der Arbeitsgemeinschaft Strafrecht im DAV; der Vortrag war frei gehalten, die schriftliche Fassung gibt die wesentlichen Gedanken wieder.

Der Chip taugt nicht nur für Waren. Er wird Tieren mit individualisierender Information eingepflanzt. Geschichten von herrenlosen Hunden lassen sich demnächst dem vergangenen Jahrhundert zu ordnen. Derart getestet haben sich diese Chips auch für Menschen als gesundheitsverträglich erwiesen. Mit Genehmigung ihrer Regierung hat eine amerikanische Firma begonnen, ihren Kunden Chips mit schnell ablesbaren persönlichen Merkmalen einzupflanzen, um ärztliche Hilfe im Falle eines Unfalls zu beschleunigen. Der Mensch mit blitzschnell erfassbarem **DNA**-Code ist keine Vision mehr.

Videoaufnahmen werden dank verbesserter Qualität und enorm gestiegener Speichermöglichkeiten alltägliches Leben bestimmen. Wer sein Haus, sein Auto oder andere wertvolle Dinge bewachen will, wird auf dieses Medium zurückgreifen. Vermietungsgesellschaften in manchen europäischen Ländern betreiben bereits Observationskameras, auf die jedermann über das Internet zurückgreifen und damit eigene Beobachtungen über Auffälligkeiten registrieren kann. Aktuell gibt es z.B. in Großbritannien weit mehr als 5 Millionen private Videoobservationen, Tendenz steigend.

Neben dem PC symbolisiert das **Mobiltelefon** die rasante Entwicklung vom Unvorstellbaren zum Unverzichtbaren. Neben ständiger Erreichbarkeit trotz steigender Mobilität ist das winzige Gerät in millionenfacher Auflage zu einem Teil der Individualität ihres Benutzers verschmolzen. Die Aufbewahrung und Nutzung persönlicher Bilder, Nachrichten oder Musikdateien geht einher mit einem breiten Spektrum permanent ausgestrahlter geographischer Daten zu einem aktuellen Standort. Die Informationen der jeweiligen Providerkarte (IMSI) gehört hierzu ebenso wie diejenigen zur Erkennung des verwandten Telefons (IMEI), der Zugangscode zum Verbindungschip (PUK) oder zur konkreten Identifizierung des Rechnersystems (dynamische IP).

Vorhersehbar ist, dass die Teilhabe am gesellschaftlichen Leben ohne Nutzung dieser neuen Technologien faktisch unmöglich sein wird. Vorhersehbar ist auch, dass gerade das derart gelebte Alltagsleben notwendigerweise massenhaft Daten produzieren wird. Vorhersehbar ist ebenfalls, dass angesichts sich entwickelnder Speicherkapazitäten solche Datenspuren nicht flüchtig bleiben werden.

Die Polizei

wird zusätzliche Aufklärungsmöglichkeiten aufgrund neuer Technologien nutzen müssen, will sie ihrer gesetzlichen Aufgabe der Strafverfolgung nachkommen. Observiert sie einen Tatverdächtigen, ist es ebenso legitim wie sinnvoll, sich jeweils modernster technischer Geräte zu versichern, um die Heimlichkeit der Maßnahme einerseits und die Qualität der Beobachtung andererseits abzusichern. Ermittlungsaktionen der Zukunft mit Hilfe von verdeckten Ermittlern sind vorstellbar, die mit phantasievollen technischen Accessoires ausgestattet sind, wie man sie heute nur in James Bond Filmen findet.

Vorhersehbar ist allerdings auch, dass diese Art der Ermittlung zur großen Ausnahme polizeilicher Aufklärungstätigkeit werden wird. Der dauerhaften Personalnot der Ermittlungsbehörden steht ein sich ständig erweiterndes Betätigungsfeld gegenüber: Kaum eine Woche vergeht, in der der Gesetzgeber nicht eine neue Strafnorm schafft und damit die Beschreibungen strafrechtlich relevanten Tuns in unserer Gesellschaft erweitert. Ohne dass klassische Kriminalität zunimmt, erweitert sich damit permanent der Bereich der aufzuklärenden Straftaten. Mit den traditionellen Mitteln der Zeugenvernehmungen und mobilen Ermittlungstätigkeit ist dies nicht zu bewältigen. Bleibt die Aufgabe von Ermittlungspersonen auch in der Zukunft die Rekonstruktion von Sachverhalten, müssen die elektronischen Datenspuren im Ermittlungsinteresse als unentbehrliches Hilfsmittel angesehen werden. Da-

tenspuren lassen sich schnell und zentral sammeln, zusammenfügen und auswerten. Gegenüber traditionellen Zeugenaussagen haben sie eine vielfach höhere Validität. Ermittelt ein Polizeibeamter beispielsweise im Rahmen eines vorgebrachten Alibis eines Tatverdächtigen, wird er es begrüßen, mehr an der Hand zu haben als einzelne fragwürdige Wahrnehmungen eines in seiner Glaubwürdigkeit zweifelhaften Zeugen. Die Fülle von im Alltagsleben erzeugter Daten wird ihm in Zukunft ein dichtes Netz vermitteln können, aus dem sich individuelle Bewegungs- und Verhaltsprofile ableiten lassen.

Er wird unter Umständen feststellen, dass der Verdächtige zum Tatzeitpunkt in einem Lebensmittelmarkt war, er wird blitzschnell die RFID–gestützten Daten zum Warenkorb abrufen und dabei einen Einblick in das Konsum- und Leseverhalten des Verdächtigen gewinnen. Er wird die Überwachungskamera des Supermarkts mit einer biometrischen Software auswerten und den nachfolgenden Weg des Einkäufers exakt anhand der GPS-Daten des Autos und der Standortdaten des Mobiltelefons bestimmen können. Er wird feststellen, dass der Verdächtige ein kurzes Gespräch mit seinem Büro und ein längeres mit einer stadtbekannten Prostituierten geführt hat, er wird sich dadurch die anschließend erfolgten Banküberweisungen und aufgerufene Internetseiten erklären und registrieren, dass die einstmals in San Francisco vor drei Jahren produzierte Jeans aus dem Kleiderschrank geholt und vom Verdächtigen zu einem Parkspaziergang angezogen wurde. Das Ergebnis einer einstündigen Rekonstruktion des Alltagslebens des Verdächtigen ist vielleicht strafprozessual entlastend, aber ebenso radikal durchleuchtend.

Der Unterschied dieser Version polizeilicher Arbeit zum aktuellen Zustand ist nicht nur hinsichtlich der Grundlage der Datenfülle gravierend. Eine entscheidende qualitative Änderung erfährt die Polizei dadurch, dass sie nicht selbst durch Observationsmaßnahmen Daten produziert, sondern auf **privat erzeugte Datenspuren** zurückgreift. Polizeiliche Aufklärung ändert sich nicht durch neue Observation, sondern durch Nutzung der schlichten Ergebnisse von sich dramatisch verändernder, elektronisch unterstützter Lebensführung. Nicht die präsente Überwachung von Tatverdächtigen wird im Mittelpunkt stehen, sondern die **retrospektive Observation**. Eine polizeiliche Strategie erscheint hiernach konsequent, sich im Hinblick auf das Ermittlungsinteresse des potentiellen Zugriffs auf alle derartige Daten zu versichern.

Das Gesetz

relativiert ein drängend vorgetragenes Erkenntnisinteresse der Exekutive. Rechtsstaatliches Ermitteln bedarf der ausreichenden gesetzlichen Beschreibung des Handlungs- und Eingriffsspielraums. Aktuell fehlen gesetzliche Regelungen zum beschriebenen Bild polizeilichen Arbeitens. Der Status quo vermittelt auch hier Anhaltspunkte für eine **Prognose legislatorischen Verhaltens**.

So lässt der Regelungswille des Gesetzgebers in der Vergangenheit darauf schließen, dass er auch neue technische Entwicklungen einer gesetzlichen Basis zuführen will. Soweit mit neuer Technik durch die Ermittlungsbehörden selbst Observationsdaten erzeugt werden sollten, hat das Parlament in der Vergangenheit einen Regelungswettlauf aufgenommen. Der Textaufwand im achten Abschnitt des ersten Buchs der StPO, der u.a. derartige Überwachungsmaßnahmen regeln soll, hat sich in den letzten Jahrzehnten vervielfacht. Die Überwachung von Telefongesprächen (§ 100a StPO) wurde ebenso detailliert geregelt wie beispielsweise der kleine und große Lauschangriff (§ 100c StPO), die langfristige Observation mittels technischer Geräte und Fotografien (§ 100f StPO) oder die Verwendung des IMSI-Catcher (§ 100i StPO) sowie damit verbunden die Verschaffung weiterer Anschluss- und Standortdaten von Mobiltelefonen (§ 100g StPO).

Formal signalisiert dies den parlamentarischen Willen, derartiger Observationsmaßnahmen an der Leitlinie hinreichend präzisierter gesetzlicher Beschreibungen auszurichten. Ob dieser gesetzgeberische Eifer verfassungsrechtlich notwendig ist, scheint allerdings in jüngster Zeit das Bundesverfassungsgericht zu bezweifeln, wenn eine überkommene gesetzliche Formulierung den Einsatz besonderer „für Observationszwecke bestimmte technische Mit-

tel“ erlaubt und hierdurch der Freibrief für die Verwendung aller neuen Technologien durch die Ermittlungsbehörde erteilt wird, sofern sie sich nur als in Flexibilität und Genauigkeit verbesserte Technik darstellt.[2]

Inhaltlich lassen sich insbesondere aus Verteidigersicht die umfassenden **Gesetzesänderungen** unter dem Schlagwort zusammenfassen: **„in dubio pro Ermittlung“** . Eingriffsschwellen wurden permanent gesenkt, Eingriffsanlässe beständig ausgeweitet. Weiche Gesetzesformulierungen („Straftat von erheblicher Bedeutung“) täuschen in ihrer großzügigen Auslegungsmöglichkeit Beschränkungen allenfalls vor, andere („wenn die Erforschung des Sachverhalts auf anderer Weise erschwert wäre“) werden von der Praxis ignoriert. Der Richtervorbehalt hat sich als wenig effektiver Rechtsschutz herausgestellt. Änderungen der Gesetzgebungsstrategien sind nicht in Sicht.

Die Prognose eines gesetzgeberischen Verhaltens zur Verwertung privat erzeugter Dateien muss eine weitere aktuelle Tendenz berücksichtigen: Ohne die Besonderheit eines Eingriffs in Freiheitsrechte zu analysieren, ist der Gesetzgeber bereits schleichend dazu übergegangen, sich diese potentielle Informationsquelle zu sichern. Der Zugriff auf strafprozessual relevante Daten wird angestrebt, ohne dass der strafprozessual relevante Anfangsverdacht einer Straftat auch nur in Sicht ist. Sprachlich getarnt wird diese Vorbereitung nur hypothetisch denkbarer Ermittlungstätigkeit als **„Vorfeldermittlung“**.

Diese Tendenz geht einher mit der vom Parlament entdeckten Methode, Bürger und private Organisationen gesetzlich zur Hilfestellung bei dieser neuartigen Überwachungsmethode zu verpflichten. Markanter Anfangspunkt dieser Entwicklung war das **Geldwäschegesetz**. Banken haben ihre Kunden zu überwachen und – bar jeder konkreten strafprozessualen Kenntnis – Verdachtsfälle zu melden. Faktisch ist diese **private Observationspflicht** zwischenzeitlich auf nahezu alle am Geschäftsleben beteiligten – einschließlich der Rechtsanwälte – ausgedehnt worden. Was im Hinblick auf die Aufklärung von Straftaten funktioniert, soll nach Idee des Gesetzgebers beim sog. **Kontenabruf** (§ 93 Abs.7, 8 AO) auch für steuerlich erhebliche Sachverhalte gelten. Banken wurden zur Schaffung einer Kontenevidenzzentrale verpflichtet, in der nunmehr Behörden herumstöbern können – ohne Wissen der Bank, ohne Wissen des betroffenen Bürgers, ohne die Möglichkeit eines Rechtsbehelfs. Dem Gesundheitswesen stehen vergleichbare Überwachungsinstrumentarien ins Haus.

Das **Telekommunikationsgesetz** hat die Verpflichtung zur **Speicherung von Bestands- und Verkehrsdaten** gegenüber allen privaten Anbietern gesetzlich fixiert. § 100g StPO regelt die Möglichkeit des strafprozessual bedingten Datenabrufs. Der – konsequente – aktuelle Höhepunkte dieser Entwicklung ist die **EU-Richtlinie zur Vorratsspeicherung** von Daten vom 15.03.2006. Spätestens bis zum 15.09.2007 ist die Richtlinie in nationales Gesetz umzusetzen. Sämtliche Internetprovider oder Anbieter von Festnetz- oder Mobilfunkanschlüssen sollen danach verpflichtet werden, faktisch alle erreichbaren Daten von Kommunikationsprozessen für einen Zeitraum von mindestens sechs Monaten bis möglicherweise zwei Jahren zu speichern. Ausgenommen ist lediglich der Inhalt eines geführten Gesprächs oder einer E-Mail. Ansonsten sind die Nummern, Namen und Anschriften aller am Kommunikationsprozess Beteiligten, ihre Benutzerkennungen, die exakten Zeitdaten, IMSI und E-Mail, alle Standortkennungen (Cell-ID) und andere verfügbaren Daten zur geografischen Ortung von Mobiltelefonen zu sichern. Die Absicht der Totalüberwachung ist evident. Folgt der deutsche Gesetzgeber in vollem Umfang dem Brüsseler Anliegen, dürfte der Weg zum Umgang mit den Daten zukünftiger Technologien eingeschlagen sein.

---

[2] So im sogenannten GPS-Urteil des BVerfG NJW 2005, 1338 ff.

Das offenbar unstillbare **Kontrollbedürfnis** entspricht dem allgemeinen Zeitgeist. Eine rationale Rechtfertigung für die extreme Erweiterung von Überwachungen lässt sich nur schwer formulieren. Die Zahlen der Kriminalstatistik gehen zurück. Um so eher ist die Politik bemüht, mit Schlagworten wie der organisierten Kriminalität oder dem internationalen Terrorismus in der Öffentlichkeit Bedrohungsszenarien aufzubauen, die sie dann anschließend mit ihren Gesetzesinitiativen bedienen können. Die gesetzgeberische Phantasie der Einflussnahme auf gesellschaftliche Verhältnisse wirkt demgegenüber reduziert. Statt an der Verbesserung der Bedingungen gesellschaftlichen Zusammenlebens zu arbeiten, konzentrieren sich Gesetze häufig auf die Formulierung neuer Verbote und der Effektivierung ihrer Überwachung.

Freiheitsrechte

geraten bei dieser Interessenlage aus dem Blickfeld. Dass sie überhaupt bei dieser Totalüberwachung tangiert sein können, wird zum Teil bezweifelt. Es wird auf die Freiwilligkeit der Datenerzeugung hingewiesen, die ihr bereits jeden geheimhaltungsbedürftigen Charakter nehmen könne. Daten sind zwangsläufig für andere einsehbar und verwertbar. Ein gesteigertes Schutzbedürfnis wird von der Politik gern negiert. Schließlich erscheint die Retrospektive einer Zusammensetzung der Daten aus Anlass einer konkreten Strafverfolgung weit entfernt von der drohenden Präsenz eines Kontrollstaats Orwell´scher Prägung.
Die Idee vom Schutz eines anonymen Privatlebens als Ausfluss verfassungsrechtlichen Freiheitsverständnisses ist beim Gesetzgeber aktuell nicht hoch im Kurs. Dass dem schnöden Observationsdrang durch Datenspeicherung mit der simplen Argumentation „es tut ja nicht weh“ auch auf der Ebene verfassungsgerichtlicher Argumentation beigetreten werden könnte, zeigt die abweichende Meinung der Richterin Haas im Beschluss vom 04.04.06 zur polizeilichen Rasterfahndung. Eine erhebliche Eingriffsintensität polizeilichen Datenabgleichs wird schon deswegen negiert, weil diese Daten „ohnehin für jedermann offen zutage liegen“ und ihre allgemeine Zugänglichkeit auf verschiedenen Wege denkbar ist. Vergeblich fahndet die Verfassungsrichterin angesichts der Alltäglichkeit der Daten nach einem schweren Eingriff in ein Persönlichkeitsrecht und kritisiert die Ansicht der Senatsmehrheit, dass das fehlende Wissen des Betroffenen um den Datenabgleich die Eingriffsintensität steigere. Wird darüber hinaus das Primat der Gewährleistung der bürgerlichen Sicherheit durch den Staat gegenüber dem Grundrecht auf Freiheit institutionalisiert, wäre das verfassungsrechtliche Fundament für jegliche Totalobservation gelegt, falls es sich nur auf die politische Einschätzung einer staatlichen Bedrohung wie die durch den Terrorismus stützen könnte. (Noch) wird im höchsten deutschen Gericht so nur eine Mindermeinung formuliert.
Ob und in welchem Ausmaß die ins Haus stehende Totalerfassung von Daten den Bereich unserer grundrechtlich geschützten **Handlungsfreiheit (Art. 1 Abs.1, 2 Abs. 1 GG)** berührt, darf aktuell als ungesichert gelten. Als die Begriffe der Freiheit und Menschenwürde im Grundgesetz formuliert wurden, ahnte niemand etwas von IMSI-Daten oder RFID-Chips. Die dynamische Auslegung erfordert eine neue Justierung des auch im Alltagsleben abgewetzten Freiheitsbegriffs.
Dass ein nicht ausformuliertes Gefühl von Freiheit in unserer Gesellschaft durch Überwachungsstrategien tangiert sein können, verrät die Diskussion über die Aktivitäten von BND-Spitzeln im Journalistenbereich. Auch wenn von Spitzeln erlangte Informationen nicht genuin geheim sind, entspricht es unserem Verständnis gesellschaftlichen Zusammenlebens und staatlicher Organisation, in einem garantierten von jeder staatlichen Überwachung

freien Raum handeln zu können. Dass Handlungen öffentlich vorgenommen werden, dass Daten freiwillig produziert werden, ändert nichts daran, dass staatliche Intervention stets anlassbezogen sein muss. Die **unzulässige Rundumüberwachung** als Konsequenz dieser Ideen taucht explizit mehrfach in der Rechtssprechung des Bundesverfassungsgerichts auf.[3] Eine konkretisierende Ausprägung hat dieser Ausfluss des Freiheitsrechts allerdings noch nicht erhalten.

In seinem Volkszählungsurteil hat das Bundesverfassungsgericht schon auf die unserem Gesellschaftsbild widersprechenden Effekte der Zusammenführung und Auswertung massenhafter persönlicher Daten hingewiesen. Allein das Bewusstsein der – auch nachträglichen – Totalüberwachung muss alltägliche Befangenheiten fördern. Ihre Institutionalisierung geht zwangsläufig mit **Einschüchterungseffekten** einher.[4] Sie provoziert die individuelle Lebensstrategie, nicht in der Gesellschaft auffällig zu werden. Statt Kreativität und Individualität fördert sie **Konformität**. Sie erhöht das allgemeine Lebensrisiko eines jeden Bürgers, Objekt staatlicher Ermittlungsmaßnahmen zu werden und sich einem unberechtigten Verdacht auszusetzen.[5] Das unsere Rechtsordnung tragende **Prinzip der Unschuldsvermutung** muss ins Wanken kommen, wenn in der erklärten staatlichen Absicht, zukünftige strafprozessuale Ermittlungen zu tätigen, der Datenbestand der gesamten Bevölkerung ohne jeden Verdachtsanlass erfasst wird.

Das **Recht auf informationelle Selbstbestimmung** ist durch die langjährige Rechtsprechung des Bundesverfassungsgerichts zwischenzeitlich als grundrechtsähnlich etabliert. Abgeleitet ist dieses Recht aus dem Gedanken der Selbstbestimmung des Einzelnen, wonach er grundsätzlich selbst zu entscheiden hat, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.[6] Liegt diesem Konzept der Ausprägung des Freiheitsgedanken die Vorstellung von der Beherrschung eigener Datenspuren zugrunde, ist dies von der Alltagstechnik längst hinweggespült worden. Schon heute weiß kein durchschnittlicher Benutzer des Internets, welche Daten er mit einem harmlosen Surfen gegenüber jedermann offenbart. Welche Fundgrube an Informationen das eigene Navigationsgerät im PKW bereit hält, hat sich längst dem Wahrnehmungsbereich des Autofahrers entzogen. Sind unbeherrschbare Datenspuren Gegenstand rechtlicher Betrachtung, erscheint die Beherrschbarkeit als Ausgangspunkt von Begrenzungsüberlegungen jeglichen Wert verloren zu haben.

Mit der **Achtung des Privatlebens** gegenüber nicht legitimierten staatlichen Interventionen hält **Art. 8** der Europäischen Menschenrechtskonvention einen Ansatzpunkt bereit, der der Lösung der Problematik näher kommt. Das Recht auf Privatheit in einer demokratischen Gesellschaft gilt es im Hinblick auf die drohenden Einschränkungen weiter zu entwickeln. Basierend auf diesen Überlegungen sollte es gesetzgeberisches Ziel in der Zukunft sein, den Dschungel massenhafter Datenspuren nicht als Offerte zur Selbstbedienung für staatliche Observation aufzufassen, sondern gerade angesichts der Quantitäten neue Formen für ein bürgerliches **Recht auf Anonymität** zu suchen.

Das Bundesverfassungsgericht

hat bislang nicht deutlich erkennen lassen, welche verfassungsrechtlichen Vorgaben eine gesetzliche Regelung zu beachten haben wird. Zum einen zeichnet sich die Einschränkung

[3] BVerfGE 65, 1, 42 f; BVerfG NJW 2005, 1338, 1341.
[4] BVerfGE 65, 1ff.
[5] BVerfG, Urt. v. 02.03.06 Rasterfahndung.
[6] BVerfGE 65, 1 Volkszählungsurteil.

der grundrechtsgeschützten Freiheitsrechte durch eine flächendeckende Auswertung privat erzeugter Datenspuren erst allmählich ab. Zum anderen lässt der Argumentationsansatz in vielen aktuellen Entscheidungen für die Praxis effektive Bindungswirkungen vermissen.

Die Strafverteidiger haben in den letzten Jahren Erfreuliches aus Karlsruhe konstatieren können. Grundrechtseingriffe von Ermittlungsbehörden wurden beim großen Lauschangriff ebenso für verfassungswidrig erklärt[7] wie in Einzelfällen die komplette Beschlagnahme von Mandantenunterlagen einer Anwaltskanzlei[8] oder – angesichts des geringen Gewichts des Tatverdachts – die Durchsuchung und Beschlagnahme eines Mobiltelefons bei einer beschuldigten Richterin.[9] Allen Entscheidungen ist zu eigen, dass mit deutlichen Worten der Gehalt der geschützten Rechtsgüter – sei es die Wohnung, sei es das Fernmeldegeheimnis oder das Recht auf informationelle Selbstbestimmung – definiert wird, bis hin zur Behauptung eines unantastbaren privaten Kernbereichs. Faktisch gelingt es dem Verfassungsgericht allerdings an keiner Stelle, die Bereiche der absoluten Unantastbarkeit mit der Forderung nach absoluten gesetzgeberischen Grenzen zu verknüpfen. Selbst bei der Entscheidung zum großen Lauschangriff dürfte sich der den Mangel reparierende Gesetzgeber auf der sicheren Seite wähnen, wenn er von der Überwachung nur dann absieht, wenn zu prognostizieren ist, dass hierdurch Äußerungen erfasst werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind. Diese Prognosesituation wird es in der Praxis nie geben. Gerade in Situationen, in denen tataufklärende Gespräche in einer Wohnung konkret erwartet werden können, bleibt die Abhörmaßnahme zulässig und die zwangsläufige Aufnahme von privaten Gesprächen vorhersehbar.

Wie auch in anderen Situationen verlagert letztendlich die Rechtsprechung des Bundesverfassungsgerichts den Grundrechtsschutz auf die Art und Weise der Durchführung der eingreifenden Maßnahme. Die Abwägung von Rechtsgütern und der **Verhältnismäßigkeitsgrundsatz** sind die Schlüsselworte dieses Grundkonzepts. Der ermittelnde Beamte soll „vor Ort" Abhörmaßnahmen unverzüglich unterbrechen, wenn ihm die stets präsente Grundrechtsabwägung die Erkenntnis vermittelt, dass ein abgehörtes Gespräch inhaltlich die Intimität des Kernbereichs privater Lebensführung überschreitet. Er hat Lauschangriffe wie Telefongespräche sofort abzubrechen, wenn er ein Mandantengespräch mit einem Anwalt erkennt. Er hat die Sichtung von Mandantendaten im PC einer durchsuchten Anwaltskanzlei zu unterlassen, wenn diese erkennbar keinen Verfahrensbezug haben. Er hat ein während der Durchsuchung vor ihm liegendes Handy einer Beschuldigten und die darin schlummernden Informationsquellen souverän zu ignorieren, wenn er den Eingriff in das Recht auf informationelle Selbstbestimmung gewichtet und angesichts der Überschaubarkeit des Ermittlungsvorwurfs für unverhältnismäßig erachtet.

Ein **Schutzkonzept**, das allein auf die derart beschriebene Einsicht des nach Informationen drängenden Ermittlungsbeamten setzt, **muss scheitern**. Es ist bar jeder praktischen Erfahrung, die insbesondere Strafverteidiger in ihrer täglichen Arbeit machen. Die – auch richterliche – Anordnung einer Maßnahme wird oft genug als pauschale Eintrittskarte verstanden, um ohne jede weitere gerichtliche oder staatsanwaltschaftliche Kontrolle den polizeilichen Informationsbedarf auch in grundrechtlich geschützten Bereichen zu befriedigen. Es mutet nahezu naiv an anzunehmen, dass ein von jeder konkreten Aufsicht befreiter Poli-

[7] BVerfGE 109, 279 = NJW 2004, 999.
[8] BVerfGE 113, 29; BVerfG NVwZ 2005, 1304.
[9] BVerfG NJW 2006, 976.

zeibeamter in Eigeninitiative abbrechende Maßnahmen ergreift, um sich selbst möglicherweise zur Aufklärung entscheidende Hinweise zu nehmen.
Will der Gesetzgeber zukünftig das Sammeln und Auswerten privater Datenspuren regeln, ist das schlichte Vertrauen auf eine abwägende Entscheidung des auswertenden Polizeibeamten erst recht grundrechtsgefährend. Wird der Eingriff erst durch die Massivität des Abgleichs deutlich, ist die individuelle Beurteilung von Quantität in Qualität für den Beamten häufig schwer erkennbar.
Das ursprüngliche Konzept der Strafprozessordnung war ein anderes: Noch in ausgeprägterem Maße als heute dürfte der Staat im 19. Jahrhundert den Wert der polizeilichen Arbeit geschätzt haben. Das hat den Gesetzgeber nicht davon abgehalten, Erkenntnisse über die Psyche des Ermittlers in die Regelung der Zulässigkeit von Beweismitteln einfließen zu lassen. So wird beispielsweise der Skepsis gegenüber der möglichen Einseitigkeit einer polizeilichen Zeugenvernehmung und deren fehlende Kontrollierbarkeit dadurch Rechnung getragen, dass – im Gegensatz zu einem richterlichen Protokoll – eine solche im Prozess selbst nicht verlesbar ist. Von dieser auch heute noch notwendigen Skepsis gegenüber der Qualität von Ermittlungsmaßnahmen ist der aktuelle Gesetzgeber weit entfernt.

Die Anwaltschaft

ist in der anstehenden Diskussion zu expliziter Stellungnahme aufgerufen. Lobbyisten für Bürgerechte sind aktuell rar. Dass der Schutz von Grundrechten im Ermittlungsverfahren und seinen Vorstadien in Ausschüssen und im Plenum des Bundestages gewichtige Fürsprecher hat, ist angesichts der gesetzgeberischen Aktivitäten der letzten Jahre zweifelhaft. Demokratisches Engagement ist daher gefragt, wozu auch Information und politische Stellungnahmen von Organisationen gegenüber dem Gesetzgeber gehören. Den deutschen Anwälten kommt aufgrund ihrer intimen Kenntnis der Praxis von Ermittlungsverfahren hierbei eine besondere Rolle zu. Es gilt auch von unserer Seite die beschriebenen Gefahren aufzuzeigen und an Vorschlägen mitzuarbeiten, wie wir angesichts der rasanten technischen Entwicklung **tradierte rechtsstaatliche Werte bewahren** können.
Es gilt, auch beim Gesetzgeber Sensibilitäten für den grundrechtseinschränkenden Charakter der Aufzeichnung sich massiv ausweitender Datenspuren zu wecken. Wird der Eingriff gerechtfertigt mit fundamentalen Sicherheitsbedürfnissen der gesamten gesellschaftlichen Organisation, sollte nichts dagegen sprechen, diesen Eingriff mit aller Deutlichkeit auf Fallkonstellation der konkreten terroristischen Bedrohung zu beschränken. Gerade angesichts der Weite der Eingriffsmöglichkeiten bedarf eine gesetzliche Regelung der besonderen Klarheit. Angesichts der Missbrauchsmöglichkeiten hat sich der Gesetzgeber an den traditionellen Gestaltungsmöglichkeit der **strengen Formalisierung** einerseits und der **Institutionalisierung von Kontrollmechanismen** andererseits zu orientieren. Nur so kann verhindert werden, dass die einmal erfolgte gesetzliche Fixierung der Speicherung und Auswertung von Daten zum Standardinstrument polizeilicher Arbeit verkommt.
Die Effektivierung des Grundrechtsschutzes bedarf der Sanktionierung im Fall des Verstoßes gegen gesetzliche Vorgaben. Das Minimum stellen klar zu formulierende **Beweisverwertungsverbote** dar. Hier gilt es die Tendenz des aktuellen Gesetzgebers wieder zu berichtigen, sich dieser Konsequenz unter undifferenziertem Hinweis auf die Aufrechterhaltung einer funktionsfähigen Strafrechtspflege und der angeblichen Gefahr materiell unrichtiger Urteile zu entziehen[10]. Ein gesetzgeberisches Konzept muss darüber hinaus konkrete Kon-

[10] s. hierzu z.B. die Begründung zum Gesetzesentwurf in der Drucksache des Bundesrats 163/04.

trollen und Verantwortlichkeiten institutionalisieren. **Transparenz nach Abschluss einer geheimen Maßnahme** ist hierfür unentbehrlich. Die Information des betroffenen Bürgers über die Datenauswertung einerseits sowie der nachvollziehbare Bericht des verantwortlichen Ermittelnden andererseits sollte gesetzgeberischer Standard werden.
Mussten wir in der Vergangenheit befürchten, dass unsere Freiheit durch gesetzgeberische Novitäten scheibchenweise stirbt, droht nun die Verschüttung durch einen unscheinbar daherkommenden Erdrutsch der Totalüberwachung. Vorhersehbar ist die Entwicklung gerade für uns Anwälte. Rechtspolitisch sollten wir uns zu mehr als bloßen Aufräumarbeiten nach dem Beben verpflichtet fühlen.