FORUM

GLÄSERNE BÜRGERINNEN

ODER: SIND WIR DENN ALLE TERRORIST/INNEN?

Innenminister Schäuble und andere InnenpolitikerInnen halten offensichtlich große Teile der Bevölkerung für Terrorverdächtige. Dieser Eindruck drängt sich jedenfalls auf, wenn man die sicherheitspolitischen Diskussionen in den letzten Wochen und Monaten verfolgt.

Die Kontroversen um Online-Durchsuchungen oder Präventivhaft für Terrorverdächtige sind allerdings nur Endpunkte einer jahrelangen Entwicklung, die zu einer erschreckenden Ausweitung von Überwachungs- und Erfassungsmethoden geführt hat.

Passfotos und biometrische Daten

Vor der Sommerpause haben Bundestag und Bundesrat weit reichende Änderungen des Passgesetzes beschlossen, die zum 1. November 2007 in Kraft getreten sind. Danach werden zusätzlich zum Passfoto (seit 2005) jetzt auch zwei Fingerabdrücke digital auf einem Chip im Pass gespeichert. Während die Fingerabdrücke (zunächst) nur auf dem Pass und nicht bei Sicherheits- oder Meldebehörden gespeichert werden, bleibt es bei der Hinterlegung der Passfotos in digitaler Form bei den kommunalen Meldebehörden. Eine zentrale bundesweite Datei mit biometrischen Daten gibt es weiterhin nicht. Neu ist allerdings, dass die regionalen Polizeibehörden online auf die Fotodateien zugreifen können, "wenn die Passbehörde nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährden würde".

Die zuletzt genannte Einschränkung stellt allerdings keine ernstzunehmende Grenze für den Zugriff der Polizei auf die gespeicherten Passfotos dar. Dies zeigt, wie Schritt für Schritt die Grenzen der Nutzung von Personendaten der BürgerInnen verschoben werden. In diesem Fall werden biometrische Daten, die zunächst nur der Erstellung des Passes dienen sollten, nun viel umfassender für die Zwecke der Sicherheitsbehörden verwendet. Die gleiche Entwicklung wie bei den Passfotos ist mittelfristig auch für die Fingerabdrücke zu befürchten: Sind erst einmal die Voraussetzungen für die Erhebung dieser biometrischen Daten geschaffen, ist es nur noch ein kleiner Federstrich im Gesetz bis zur dauerhaften Speicherung.

Die größte und auch berechtigte Sorge der DatenschützerInnen ist dabei, dass mit den Themen innere Sicherheit und Terrorbekämpfung schon in der Vergangenheit unbeschränkte Zugriffe der Ermittlungsbehörden auf Daten eingeräumt wurden, die dann später nicht zur Terrorfahndung, sondern tatsächlich zur Ausspähung "normaler" Lebensverhältnisse missbraucht wurden.

Schon bei der Einführung der Speicherung von Passfotos auf den Reisepässen sagte dazu die Landesbeauftragte für Datenschutz und Informationsfreiheit in Nordrhein-Westfalen, Bettina Sokol: "Eine wesentliche Gefahr besteht darin, dass es schon jetzt Wünsche gibt, die biometrischen Daten in einer zentralen Datei zu speichern. Eine Datei, die über kurz oder lang auch das Interesse der Strafverfolgungsbehörden wecken würde, denn was wäre schöner als alle an einem Tatort aufgefundenen Fingerabdrücke problemlos einzelnen Bürgern zuordnen zu können. Langfristig würde das eine Katalogisierung aller europäischen Bürger bedeuten."

Foto: claude05

Kontoabfrage

Ein weiteres Beispiel für den automatisierten Zugriff staatlicher Behörden auf Daten von BürgerInnen ist die Kontoabfrage. Dabei können u.a. Strafverfolgungsbehörden und Sozialbehörden über zentrale Schnittstellen bei allen Banken die sog. Kontostammdaten abrufen, sofern dies "zur Erfüllung ihrer Aufgaben erforderlich" ist. Darunter fallen z.B. Name, Geburtsdatum, Kontonummern und Depots. Kontostände und -bewegungen können auf diese Weise zunächst nicht abgefragt werden.

Ursprünglich als Mittel zur Bekämpfung von Geldwäsche terroristischer Gruppen eingeführt, wird die Abfrage der Kontostammdaten inzwischen für alles Mögliche, aber de facto nicht zur Terrorfahndung genutzt. Das belegen die nackten Zahlen: Im Jahr der Einführung (1. April 2003) des Gesetzes wurden gerade 1027 Kontoabfragen gestartet. Inzwischen ist diese Zahl nach Angaben des Bundesverbandes Deutscher Banken explosionsartig auf über 107.000 im Jahr 2006 gestiegen.

Das Bundesverfassungsgericht (BVerfG) hat inzwischen den automatisierten Abruf im Wesentlichen für verfassungsgemäß erklärt.[1] Damit kann sozusagen jedeR SachbearbeiterIn in den Finanz- oder

Sozialämtern und der Bundesagentur für Arbeit online abfragen lassen, welche Konten einE BürgerIn bei welchen Banken unterhält. Dazu bedarf es nicht einmal eines Gerichtsbeschlusses oder einer dezidierten Begründung gegenüber irgendeiner anderen Stelle.

Online-Ausforschung

An Dreistigkeit kaum noch zu überbieten ist die Online-Ausforschung privater Computer, die schon seit Ende 2006 Gegenstand heftiger Debatten ist. Innenminister Schily hatte bereits 2005 den ihm unterstehenden Behörden (Nachrichtendienste und Bundeskriminalamt) in einer Dienstanweisung ohne gesetzliche Grundlage gestattet, heimlich so genannte Trojaner auf die Computer von BürgerInnen zu schleusen. Diese Spionageprogramme, benannt nach dem mythischen trojanischen Pferd, spähen heimlich die PCs von BürgerInnen aus und versenden Daten über das Internet, so dass die Ermittlungsbehörden Zugriff auf alle persönlichen Daten haben, die sich auf dem Computer befinden.

Der Bundesgerichtshof (BGH) hat mit Beschluss vom 31. Januar 2007 dieses Durchstöbern privater Computer jedenfalls für den Bereich der Strafverfolgung ausdrücklich mangels gesetzlicher Grundlage in der Strafprozessordnung (StPO) untersagt.[2] Das hinderte unseren Bundesinnenminister aber perfiderweise nicht daran, den Geheimdiensten diese Schnüffelaktionen zunächst weiter zu gestatten, bis der öffentliche Druck zu groß wurde. Das Argument des Ministers: Die Fahndung nach TerroristInnen, die unser Land angeblich bedrohen, erfordere solche Maßnahmen und wer nichts zu verbergen habe, brauche auch nichts zu befürchten. Abgesehen davon, dass solche Schnüffelaktionen gegen die Grundrechte verstoßen, sind die Schlussfolgerungen wenig überzeugend. Ein Staat darf nicht einfach mit geschürter Terrorangst die elementaren Rechte seiner BürgerInnen verletzen, schon gar nicht ohne gesetzliche Grundlage. Was sollen die BürgerInnen von einem Minister halten, der Beschlüsse des obersten deutschen Strafgerichts schlichtweg ignoriert, nur weil es ihm nicht in den Kram passt?

Im Grundgesetz (GG) wurde der Unverletzlichkeit der Wohnung (Art. 13 GG) nicht umsonst ein hoher Stellenwert eingeräumt. Auch wenn vielfach versucht wird, dies wegzudiskutieren, müssen zu der "unverletzlichen Wohnung" auch die darin aufgestellten Computer gehören. Damit müssen auch für Online-Durchsuchungen mindestens die gleichen Beschränkungen gelten wie für den so genannten Großen Lauschangriff. Der "Kernbereich privater Lebensgestaltung" muss danach von Überwachungsmaßnahmen freigehalten werden.

Videoüberwachung

Auch bei der Videoüberwachung haben die letzten Jahre eine erhebliche quantitative Ausweitung gebracht. Wie auch andere Landesgesetze ermächtigt das Polizeigesetz in Nordrhein-Westfalen (PolG) die Polizei, an öffentlich zugänglichen Orten, die Kriminalitätsschwerpunkte sind bzw. an denen "die Beschaffenheit" des Ortes die Begehung von Straftaten begünstigt, eine Videoüberwachung zu installieren und die Aufnahmen aufzuzeichnen und zu archivieren (§ 15 PolG).

Abgesehen davon, dass der Nutzen der Videoüberwachung für die Kriminalitätsbekämpfung höchst zweifelhaft ist und vielmehr der Durchsetzung einer Verhaltenssteuerung im Sinne eines bürgerlich-konservativen Begriffs von öffentlicher Ordnung dient, zeigt sich das wahre Potential, wenn man sie mit anderen Maßnahmen verknüpft: Es laufen bereits die entsprechenden Modellversuche, um die in Innenstädten, Bahnhöfen, S- und U-Bahnstationen und allen möglichen anderen Orten installierte Kameraerfassung mit einer automatisierten digitalen Gesichtserkennung zu verknüpfen. Noch ist die entsprechende Software bei sich schnell bewegenden Menschen nicht ausgereift. Bei weniger Bewegung, wie beispielsweise an den Passschaltern in den Flughäfen hingegen, funktioniert die Gesichtsfelderkennung bereits. Dass wird vermutlich dazu führen, dass die auf der Grundlage des Passgesetzes gespeicherten Bilddaten für die automatisierte Fahndung oder die Erstellung von Bewegungsprofilen herangezogen werden.

Eine willkommene Ergänzung dazu sind auch die Daten der Firma Toll-Collect (elektronische Autobahnmaut). Ein Zugriff auf die Mautdaten unter Berufung auf § 100g StPO (Auskunft über Telekommunikations-Verbindungsdaten) wird inzwischen ernsthaft diskutiert und wurde trotz entgegenstehender gesetzlicher Regelung in mehreren Fällen gerichtlich zugelassen.[3] Damit ließe sich dann - theoretisch - ein vollständiges Bewegungsprofil jedes Fahrzeuges erstellen. Auch hier wurde bei der Einführung ausdrücklich versichert, dass die elektronische Erfassung von Fahrzeugdaten ausschließlich für die Erhebung der Autobahnmaut verwendet wird und ermittlungstechnische Zugriffe ausgeschlossen seien. Vor diesem Hintergrund wird jetzt auch klar, warum die Bundesregierung so großen Wert darauf gelegt hat, dass das so teure und technisch unausgereifte System der Telekom zum Einsatz kommen musste: Mit der viel einfacheren und zuverlässigeren österreichischen Methode kann man nur Maut erheben; für Fahndungszwecke ist es ungeeignet.

Überwachung der Telekommunikation

Die Überwachung der Telekommunikation, zu der auch Email-Verkehr, Gespräche über Mobiltelefone und alle Verbindungsdaten gehören, ist in den §§ 100a ff. StPO geregelt. Die neuen Kommunikationsformen haben immer wieder für Diskussionsstoff gesorgt. Umstritten ist beispielsweise, inwieweit das Fernmeldegeheimnis (Art. 10 GG) vor der Erstellung von Bewegungsprofilen mit Hilfe von Handys im Stand-by-Betrieb schützt. Dies ist zum Beispiel entscheidend beim Einsatz des so genannten IMSI-Catchers (§ 100i StPO). Dieses Gerät simuliert gegenüber allen Mobiltelefonen in seiner Reichweite das Vorhandensein einer Basisstation, woraufhin sich jedes eingeschaltete Handy bei dem Gerät einbucht und dabei gewisse Daten übermittelt. So lassen sich dann alle ein- und ausgehenden Telefonate dieser Handys überwachen; es bedarf dafür nicht einmal einer Schnittstelle bei dem Netzanbieter.

Bei der Telekommunikationsüberwachung im engeren Sinne, also dem Mithören oder Mitschneiden von Telefongesprächen, erscheint insbesondere die geringe praktische Wirksamkeit der einschränkenden Anordnungsvoraussetzungen problematisch. Die Überwachung der Telekommunikation bedarf gemäß § 100b StPO der richterlichen Anordnung; in der Praxis läuft sie allerdings häufig leer. Empirische Untersuchungen haben gezeigt, dass im Gerichtsalltag Fälle, in denen der Antrag der Staatsanwaltschaft auf Durchführung der Telekommunikationsüberwachung abgelehnt wird, nahezu

1 BVerfG, Beschluss vom 13.6.2007, Aktenzeichen: 1 BvR 1550/03 u.a., http://www.bverfg.de (alle Weblinks Stand August 2007).

2 BGH, *Neue juristische Wochenschrift (NJW)* 2007, 930.

3 S. z.B. AG Gummersbach, *NJW* 2004, 240.

nicht vorkommen. Welp[4] formulierte es schon 1994 so: "Der Richter vergibt Eintrittskarten, ohne die Vorstellung zu kennen, die gegeben wird." Das dürfte auch dazu geführt haben, dass allein in den Jahren 1990 (2494 Anordnungen) bis 2003 (21.651 Anordnungen) die Anzahl der Telekommunikationsüberwachungen um über 850 % angestiegen ist.

Der Katalog der Anlasstaten, also derjenigen Taten, zu deren strafrechtlicher Verfolgung die Überwachungsmaßnahmen zulässig sind, umfasst inzwischen über 80 Delikte und ist eine Rundreise durch das halbe Strafgesetzbuch und die Nebengesetze. Die Mehrheit der Überwachungsanordnungen (54 %) beruht dabei auf dem Verdacht einer Anlasstat aus dem Betäubungsmittelgesetz (BtMG). So reicht nach gegenwärtigem Recht bereits der Besitz einer nicht geringen Menge von Cannabis-Produkten als Anlasstat aus (§ 29a I Nr. 2 BtMG; also schon ab etwa 80 g Haschisch). Da sehr viele dieser Verfahren mit Freiheitsstrafen von unter zwei Jahren enden, stellt sich zwangsläufig die Frage nach der Verhältnismäßigkeit.

Immerhin hat das BVerfG 2005 einer noch weiteren Ausdehnung der Möglichkeiten der Telekommunikationsüberwachung in das Vorfeld eventueller zukünftiger Straftaten eine vorläufige Absage erteilt[5] und mit der Nichtigerklärung von Vorschriften des niedersächsischen Polizeigesetzes deutliche Grenzen dahingehend gesetzt, dass eine rein präventive Überwachung der Telekommunikation unzulässig ist.

Vorratsdatenspeicherung

Bedenklich erscheint auch der Zugriff der Ermittlungsbehörden auf die Verbindungsdaten (§ 100g StPO) der Telekommunikation. Dies gilt umso mehr, seit Anfang 2006 die Europäische Gemeinschaft eine Richtlinie erlassen hat,[6] nach der verdachtsunabhängig alle Telekommunikations-Verbindungsdaten zwischen sechs und 24 Monaten gespeichert werden sollen. Unter dem Begriff "Telekommunikationsdaten" sind so ziemlich alle Daten erfasst, die beim Internet-Surfen, Emailen, SMS versenden und Telefonieren über Festnetz und Handy entstehen. Darunter fallen auch die erfassbaren Verkehrsdaten (Standort- und Kennungsdaten des Handys). Das bedeutet im Klartext, dass von den rund 490 Millionen Menschen, die in Europa leben, sämtliche Spuren, die sie bei der Kommunikation hinterlassen, auf Vorrat gespeichert werden.

Inzwischen hat die Bundesregierung den "Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG" in das parlamentarische Verfahren eingebracht, der eine sechsmonatige Vorratsdatenspeicherung vorsieht.[7] Durch die verdachtsunabhängige Speicherung von Verbindungsdaten werden künftig riesige Datenbestände über jedeN BürgerIn angelegt, ohne dass es dafür einen konkreten Anlass, z.B. den Verdacht einer Straftat gibt. Was als präventive Terrorismusbekämpfung verkauft wird, entpuppt sich bei näherem Hinsehen als nichts anderes als die vollständige Überwachung unserer Kommunikation.

Der große Lauschangriff

Die Befugnis zum heimlichen Abhören von Gesprächen in einer Wohnung (§ 100c Abs. 1 Nr. 3 StPO) zählt als klassische Geheimdienstmethode zu den umstrittensten Eingriffen, die die StPO kennt. Ob dieser Lauschangriff (Wohnraumüberwachung, Art. 13 Abs. 3 GG) im Hinblick auf Art. 79 Abs. 3, 1 Abs. 1 GG (Schutz der Menschenwürde) überhaupt verfassungskonform geregelt werden kann, ist heftig umstritten. In einer Entscheidung vom 3. März 2004 hat das BVerfG die Frage bejaht,[8] allerdings mit einer gewissen Begrenzung der Eingriffsmöglichkeiten. Danach darf der Staat nicht durch Überwachungsmaßnahmen in einen "absolut geschützten Kernbereich privater Lebensgestaltung" eingreifen. Problematisch ist an dieser Begrenzung, dass es dabei auf den Inhalt der mitzuhörenden Gespräche ankommt. Ob es sich um einen solchen absolut geschützten Inhalt handelt, stellt sich aber in der Regel erst während der Überwachung oder Aufzeichnung heraus. Der Schutzmaßstab des BVerfG ist also praktisch kaum umsetzbar.

In der Folge der Entscheidung des BVerfG hat aber der 1. Strafsenat des BGH eine Verurteilung wegen Mordes aufgehoben, die sich im Wesentlichen auf ein Selbstgespräch stützte, das der Angeklagte in seinem Krankenhauszimmer geführt hat. Der BGH stellte fest, dass ein solches (Selbst-)Gespräch dem Kernbereich privater Lebensgestaltung angehört und einem Beweisverwertungsverbot unterliegt.[9]

Die Bundesregierung hat, nachdem das BVerfG die Ausführungsregelungen des § 100c Abs. 1 Nr. 3 StPO für verfassungswidrig erklärt hatte, mit Wirkung zum 01.07.2005 die §§ 100c bis 100f StPO neu geregelt. Ob es damit gelungen ist, die Anwendung des Großen Lauschangriffs verfassungskonform zu regeln, ist aufgrund der genannten Probleme zu bezweifeln. Eine entsprechende Verfassungsbeschwerde wurde allerdings vom BVerfG wegen mangelnder Erfolgsaussichten nicht zur Entscheidung angenommen.[10]

Rasterfahndung

Als Rasterfahndung (§ 98a StPO) wird der Abgleich von Informationen bezeichnet, die aus mindestens zwei unterschiedlichen Datenquellen herrühren. Die Grundrechtsrelevanz dieser Maßnahme im Hinblick auf das Grundrecht auf informationelle Selbstbestimmung liegt vor allem in ihrer außergewöhnlich hohen Breitenwirkung: Von

der Rasterfahndung können die Daten beliebig vieler - unverdächtiger - Personen (im Extremfall der gesamten Bevölkerung) betroffen sein. So wurden etwa im Rahmen der Rasterfahndung nach dem 11. September 2001 allein in Nordrhein-Westfalen die Daten von 5 Millionen Männern gerastert; in 11.000 Fällen trafen mehrere der überaus allgemein gehaltenen Rasterkriterien zu, so dass diese Daten als "Recherchefälle" an das BKA übermittelt wurden.

Das Kernproblem bei der Rasterfahndung ist, dass aufgrund der Kumulation von unbestimmten Rechtsbegriffen ("Straftat von erheblicher Bedeutung", "gewohnheitsmäßig", "in anderer Weise organisiert") Zweifel bestehen, ob sie geeignet sind, die Verhältnismäßigkeit der Eingriffe in das Grundrecht auf informationelle Selbstbestimmung zahlreicher unverdächtiger Personen hinreichend zu gewährleisten.

Auch bei der Rasterfahndung hat das BVerfG wenigstens im Bereich der präventiven Fahndung Grenzen gezogen.[11] Das Gericht sieht in der Rasterfahndung und der damit verbundenen Datenerhebung einen schweren Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), der mit einer nur allgemeinen Bedrohungslage nicht zu rechtfertigen ist. Das BVerfG fordert vielmehr eine konkrete Gefahr und das Vorliegen weiterer Tatsachen, aus denen auf die Vorbereitung oder Durchführung eines terroristischen Anschlags geschlossen werden kann. Angesichts dieser Vorgaben darf nun jedenfalls keine präventive Rasterfahndung mehr aufgrund einer - wirklichen oder herbei geredeten - bloßen allgemeinen Gefährdungslage durchgeführt werden.

DNA-Datenspeicherung

Im Rahmen der Fortschritte der Genom-Analyse hat sich die Identitätsfeststellung mittels genetischer Erkennungsmuster als effektive Ermittlungsmaßnahme erwiesen. Daher wurde mit § 81e StPO eine Rechtsgrundlage zur Durchführung der DNA-Analyse zum Zweck des Vergleichs von am Tatort aufgefundenen biologischen Spuren (Haare, Hautschuppen, Speichel, Sperma) mit der DNA des Beschuldigten geschaffen, sowie mit § 81g StPO eine Ermächtigungsgrundlage zur Feststellung und Speicherung des DNA-Identifizierungsmusters zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren. Hierbei ist die Gewinnung des Identifizierungsmusters - entgegen vielfach anders lautenden Aussagen - ausweislich der amtlichen Gesetzesbegründung nicht auf den sog. nicht-codierenden Bereich der DNA beschränkt. Damit werden solche Teile der DNA bezeichnet, von denen man annimmt, dass in ihnen keine Codierung von körperlichen Merkmalen, Krankheiten usw. enthalten ist. Da - auch angesichts der technischen Fortschritte auf diesem Gebiet - nicht absehbar ist, welche Rückschlüsse auf Krankheiten und Persönlichkeitsmerkmale künftig möglich sein werden, begründet die Maßnahme Missbrauchsgefahren, die mit denen eines herkömmlichen Fingerabdrucks nicht vergleichbar sind.

Zwar ist die Speicherung des DNA-Musters nur bei "Straftaten von erheblicher Bedeutung" zulässig, dazu zählt aber auch schon ein Diebstahl in einem besonders schweren Fall. Daher ist nicht verwunderlich, dass die sog. Trefferstatistik seit 1998 Erfolge in 617 Verfahren wegen Tötungsdelikten, in 1.349 Verfahren wegen Sexualdelikten, aber in 49.154 Diebstahlsverfahren ausweist.[12] Die DNA-Datenspeicherung hat ihren Charakter als besondere Eingriffsmaßnahme bei schwerer Kriminalität also trotz der bestehenden Missbrauchsmöglichkeiten schon weitgehend eingebüßt. Eine weitere Ausdehnung der Maßnahme auf sämtliche Delikte und ein Verzicht auf den

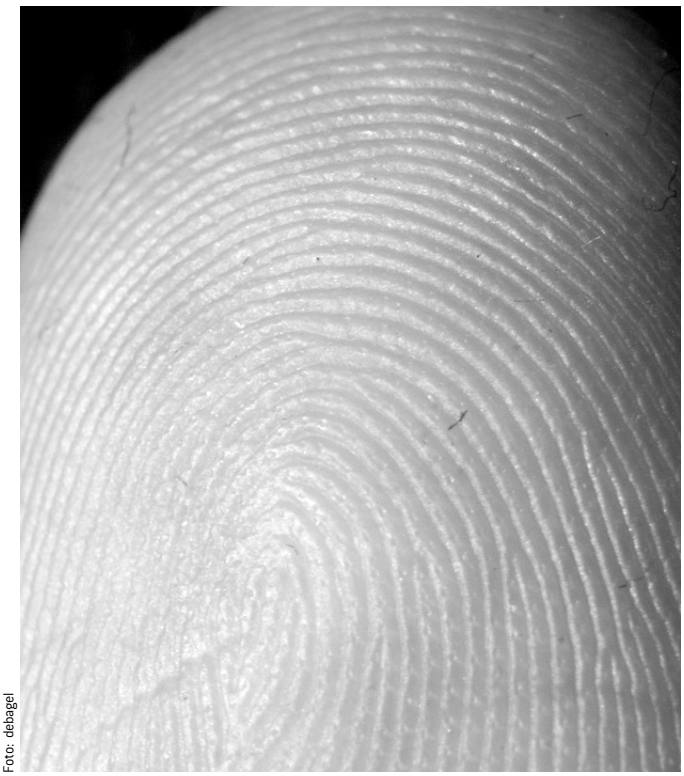

Foto: debagel

Richtervorbehalt, wie es von der Union immer wieder gefordert wird, erscheinen vor diesem Hintergrund als unverhältnismäßig.

Ausufernde Sicherheit

Das angeblich gestiegene Sicherheitsbedürfnis der Bevölkerung angesichts der (vermeintlichen?) Terrorgefahr wird von HardlinerInnen wie Schäuble, Beckstein, Schily & Co dazu benutzt, in den letzten Jahren immer mehr Überwachungsmaßnahmen einzuführen und noch weitergehende einführen zu wollen. Die Befugnisse der Nachrichtendienste und Strafverfolgungsbehörden werden erweitert, die materiellen Anordnungsvoraussetzungen abgesenkt und die Kontrolle der Maßnahmen durch RichterInnen zurückgefahren. Auch die jüngsten Vorhaben Schäubles (gezielte Tötungen, Internierung Verdächtiger, Internet- und Handyverbot für GefährderInnen) sind mit rechtsstaatlichen Standards unvereinbar. Gerade mit Blick hierauf sollte der Gesetzgeber zu einer Orientierung an den Freiheitsverbürgungen des Grundgesetzes zurückkehren, weitere Eingriffe in das Recht auf informationelle Selbstbestimmung unterlassen und zumindest die wenigen Kontrollmechanismen wie den Richtervorbehalt mit größerer Wirksamkeit ausstatten.

Joachim Hackbarth studiert Jura an der Fernuni Hagen.

4 Welp, Jürgen, Der SPD-Entwurf eines Zweiten Gesetzes zur Bekämpfung der organisierten Kriminalität, *Strafverteidiger (StV)* 1994, 161.

5 BVerfG, NJW 2005, 2603, siehe auch: Backes, Otto / Gusy, Christoph, Wer kontrolliert die Telefonüberwachung?, *StV* 2003, 249.

6 Richtlinie 2006/24/EG vom 15.03.2006.

7 Vgl. Bundestags-Drucksache 16/5846 vom 27.6.2007, http://dip.bundestag.de.

8 BVerfG, *NJW* 2004, 999.

9 BGH, *NJW* 2005, 3295.

10 BVerfG, Beschluss vom 11.05.2007, Aktenzeichen: 2 BvR 543/06, http://www.bverfg.de.

11 BVerfG, *NJW* 2006, 1939.

12 S. http://www.bka.de/profil/faq/dna02.html.