Bettina Sokol (Hrsg.)

Total transparent -Zukunft der informationellen Selbstbestimmung?

Düsseldorf 2006

Herausgeberin:

Landesbeauftragte für
Datenschutz und Informationsfreiheit
Nordrhein-Westfalen
Bettina Sokol
Kavalleriestraße 2 - 4

40213 Düsseldorf

Tel.: 0211/38424-0
Fax: 0211/3842410
E-mail: poststelle@ldi.nrw.de

Diese Broschüre kann unter www.ldi.nrw.de abgerufen werden.

ISSN:
Druck:

Gedruckt auf chlorfrei gebleichtem Recyclingpapier

Vorwort

Am 03. November 2005 haben das Institut für Informations-, Telekommunikations- und Medienrecht der Westfälischen Wilhelms-Universität Münster und ich als Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen unser jährliches gemeinsames Symposium durchgeführt. Das Thema lautete diesmal "Total transparent - Zukunft der informationellen Selbstbestimmung?" Die auf dem Symposium gehaltenen Vorträge sind in dem vorliegenden Band dokumentiert. Den Vortragenden ebenso wie allen anderen Personen, die am erfolgreichen Tagungsverlauf und am Erstellen dieser Dokumentation mitgewirkt haben, danke ich ganz herzlich. Auch der freundlichen Unterstützung der Daimler-Chrysler AG gebührt besonderer Dank.

Düsseldorf 2006 *Bettina Sokol*

Inhaltsverzeichnis

Eröffnung

Bettina Sokol

Einen wunderschönen guten Tag, meine sehr verehrten Damen und Herren. Ich freue mich, Sie ganz herzlich zu unserem Symposium zur Zukunft der informationellen Selbstbestimmung begrüßen zu dürfen. Unser heutiges Thema ist zwar sozusagen ein Dauerbrenner, aber derzeit doch auch von besonderer Aktualität. Vor zwei Tagen ist nämlich in Deutschland der so genannte E-Pass eingeführt worden, der ein digitalisiertes Foto auf einem Funkchip, einem so genannten RFID enthält. In zwei Jahren sollen die Fingerabdrücke noch dazukommen. Ob die mit diesem Pass verbundenen Versprechungen eingelöst werden können, ist allerdings höchst fraglich. Die automatisierten Gesichtserkennungsverfahren der heutigen Zeit weisen noch erhebliche Fehlerquoten auf. Die so genannten zweidimensionalen Verfahren sind viel zu ungenau und die so genannten dreidimensionalen Verfahren stecken noch dermaßen in den Kinderschuhen, dass niemand ernsthaft erwägen kann, sie in der Praxis einzusetzen. Die Studien des Bundesamtes für die Sicherheit in der Informationstechnik, des BSI, weisen zudem auch alle das Ergebnis auf, dass sämtliche untersuchten Verfahren bislang noch verbesserungsbedürftig sind. Es ist also zu befürchten, dass Personen sowohl unberechtigterweise vom System akzeptiert werden als auch ungerechtfertigt nicht erkannt und zurückgewiesen werden. Wer an der Grenze in dieser Art und Weise aussortiert wird, gilt gerade wegen des besonders tiefen Glaubens an die Unfehlbarkeit dieser neuen Technik natürlich sogleich als verdächtig. Dies ist dann nicht nur besonders peinlich für die Betroffenen, sondern führt sicherlich auch zu Verzögerungen bei der Abfertigung.

Für Deutschland konnte zwar durchgesetzt werden, dass die Speicherung der neuen Daten nur auf dem Pass und nicht extern erfol-

gen darf, insbesondere nicht in einer zentralen Datei. Aber ob es sichergestellt ist, dass nicht in anderen Staaten dieser Welt, die ja nicht alle demokratisch und rechtsstaatlich verfasst sind, möglicherweise Speicherungen dieser Daten vorgenommen werden, dürfte ebenfalls fraglich sein. Das Missbrauchsrisiko ist also durchaus nicht ganz gering. Immer wieder hat außerdem die Bundesdruckerei betont, dass unsere heutigen Ausweispapiere bereits in einem hohen Maße fälschungssicher sind. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher auch seit 2001 - seit die Einführung solcher Ausweispapiere diskutiert wird - die Notwendigkeit solcher Pässe hinterfragt. Nun sind Fakten geschaffen. Unter Beteiligung der Bundesregierung sind auf europäischer Ebene Festlegungen getroffen worden, die gleichwohl noch einen zeitlichen Spielraum geboten hätten und nicht zu solcher Eile genötigt hätten. Vor diesem Hintergrund ist die Eile der Einführung der neuen Pässe besonders unverständlich. Hier wird ein Großversuch an der deutschen Bevölkerung gestartet. Dem zweifelhaften Sicherheitsgewinn stehen mit Sicherheit erhöhte Risiken für unsere Freiheitsrechte gegenüber.

Doch damit nicht genug. Seit Jahren wird ebenfalls von interessierter Seite die Vorratsdatenspeicherung diskutiert. Das heißt, sämtliche Spuren, die in der Telefonie und im Internet hinterlassen werden, sollen für bestimmte Zeiträume gespeichert und für die so genannten Bedarfsträger vorgehalten werden, damit die Sicherheitsbehörden entsprechende Zugriffsmöglichkeiten bekommen können. Wenn wir uns die dann anfallenden Datenmengen einmal vorstellen wollen, ist ein Vergleich mit dem Offline-Leben vielleicht ganz hilfreich. Überlegen Sie sich, Sie würden morgens beim Verlassen des Hauses registriert, es würde festgehalten, wo Sie dann hingehen, welche Bücher Sie anschauen, was Sie wo essen, ob und welches Kreditinstitut Sie besuchen, was Sie in der Pause, am Arbeitsplatz oder nach dem Verlassen des Arbeitsplatzes unternehmen. Dies alles auf Jahre hin zu speichern, wäre etwa dem vergleichbar, was die Vorratsdatenspeicherung in der Telekommunikation und beim Internet bedeutet. Bisher ist dies aus guten Gründen, auch wegen eines gewissen Widerstands der Wirtschaft, die natürlich die Kosten zu tragen hätte, in Deutschland nicht durchsetzbar gewesen. Gerade aber auch wegen verfassungsrechtlicher Bedenken - insbesondere im Hinblick auf das Verhältnismäßigkeitsprinzip - hat sich auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder seit Jahren immer wieder gegen diese Pläne zur Wehr gesetzt. Gegen den ausdrücklichen Beschluss des Bundestages gegen eine solche Vorratsdatenspeiche-

rung gibt es nun auf Europäischer Ebene die Diskussionen und Versuche, diese Verpflichtung durchzusetzen. Ob dies nun durch einen Rahmenbeschluss oder eine Richtlinie geschehen wird, ist noch nicht klar, aber es gilt gerade in diesen Zeiten noch zu versuchen hier das Schlimmste zu verhüten.

Zudem ist die Vorratsdatenspeicherung ein weiteres Beispiel für staatliche Begehrlichkeiten betreffend die privatwirtschaftlich geführten Datenbestände. Das kennen wir schon aus der Rasterfahndung und auch aus den Vorfällen, in denen auf Bänder aus der Videoüberwachung zugegriffen wird. Wir hinterlassen Offline und Online täglich viele Spuren, die zunehmend an Aussagekraft gewinnen, zum Beispiel über unser Konsumverhalten und über unsere Aufenthaltsorte. Der in den USA bereits gebräuchliche implantierte Ortungschip im menschlichen Körper dürfte insoweit leider noch nicht der Schlusspunkt dieser Entwicklung sein. Auch Unternehmen in den USA - wie etwa ChoicePoint - besitzen Einzelangaben über mehr als 200 Millionen Menschen. Das geht von der Autoregistrierung über Zeitungsabos und andere Kaufgewohnheiten bis hin zu Vorstrafen. Solche Unternehmen werden sicher auch weiter wachsen. Allein ChoicePoint hatte 2004 einen Umsatz von fast einer Milliarde Dollar. Dort werden Profile und Dossiers erstellt, die auch wieder staatliche Begehrlichkeiten wecken.

Sind wir bereits total transparent? Ich möchte nicht behaupten, dass wir in einem Überwachungsstaat leben würden. Das wäre meines Erachtens eine unzulässige Verharmlosung dieses Begriffs. Besorgniserregend sind die bereits vorhandenen technischen Möglichkeiten und Infrastrukturen für eine umfassende Überwachung und Registrierung allerdings schon. Hier kommt es jetzt darauf an, was politisch und gesellschaftlich gewollt ist. Wie weit wir uns schon auf dem Weg in eine Rechts- und Gesellschaftsordnung befinden, in der viele Bürgerinnen und Bürger nicht nur den tatsächlichen Überblick darüber verloren haben, wo überall sich welche Daten zu ihrer Person befinden, sondern in der sie selbst mit kräftigstem Bemühen nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß - wie es das Bundesverfassungsgericht einmal ausgedrückt hat - das soll heute unser Thema sein. Meine Damen und Herren, ich wünsche uns einen erkenntnisreichen Tag mit anregenden Diskussionen, eine Streitkultur im allerbesten Sinne und bedanke mich für ihre Aufmerksamkeit.

Gesellschaftlicher Wandel und technologischer Fortschritt in der Verfassungsrechtsprechung zur Privatheit

Elke Gurlit

I. Einführung in die Problemstellung

Als das Bundesverfassungsgericht (BVerfG) in seinem Urteil vom 15.12.1983 zur Verfassungswidrigkeit des Volkszählungsgesetzes vom 25.03.1983 das Grundrecht auf informationelle Selbstbestimmung anerkannte,[1] wurde ein verfassungsgerichtliches Signal für die Verteidigung der persönlichen Integrität der Bürgerinnen und Bürger gesetzt. Staatliche Datenbeschaffung und Überwachung sollten grundrechtlich gebändigt werden. Die politischen, technischen und gesellschaftlichen Rahmenbedingungen, in die das informationelle Selbstbestimmungsrecht gestellt ist, sind aber gravierenden Änderungsprozessen unterworfen. Die verfassungs*gerichtlichen* Reaktionen auf die Wandlungsprozesse sind Gegenstand dieses Beitrags. Dazu sind in einem ersten Schritt die Ausfächerungen der Rechte auf Privatheit zu skizzieren. Das BVerfG hat überaus filigrane Abgrenzungen zwischen den verschiedenen Ausprägungen der Rechte auf Privatheit vorgenommen (II.). In einem zweiten Schritt wird es darum gehen, anhand ausgewählter Wandlungsfaktoren zu ermitteln, ob und wie die Grundrechtsrechtsprechung mit den Veränderungsprozessen Schritt hält. Neben den technologischen Wandlungsprozessen rücken vor allem ein geändertes Verständnis der Erfüllung staatlicher Sicherheitsaufgaben, aber auch die Internationalisierung von Kommunikationsbeziehungen und die Privatisierung ehemals staatlicher Formen der Leistungserbringung in den Blick (III.). Es zeigt sich, dass das BVerfG

[1] BVerfGE 65, 1, 43; siehe zuvor bereits BVerfGE 54, 148, 155; 27, 1, 6; 35, 202, 220.

grundrechtsübergreifende Antworten gefunden hat, die vor allem in der Entwicklung prozeduraler Sicherungsmechanismen bestehen (IV.).

II. Die Auffächerung privatheitsbezogenen Grundrechtsschutzes in der Rechtsprechung des BVerfG

1. Das allgemeine Persönlichkeitsrecht und seine Ausprägungen

Kern des Rechts auf Privatheit ist immer noch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz (GG). Das *informationelle Selbstbestimmungsrecht* als Element des grundrechtlichen allgemeinen Persönlichkeitsrechts[2] hat nach seiner Prägung im Volkszählungsurteil vielfache Bestätigung in der Judikatur des BVerfG gefunden.[3] Als Datenschutzgrundrecht schützt es den "Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten".[4] Allerdings sind auch die weiteren Ausdifferenzierungen des allgemeinen Persönlichkeitsrechts für den Schutz der Privatheit bedeutsam. Hierzu rechnet das *Recht auf Schutz der Privatsphäre*, das Handlungen und Äußerungen im privaten Bereich schützt. Das BVerfG hält an der Schutzabstufung zwischen Intim- und Privatsphäre fest und gewährt nur für erstere einen absoluten Schutz.[5] Der Bereich des Privaten ist nicht nur thematisch, sondern auch räumlich bestimmt. Schutz gebührt dem Aufenthalt an Orten, an denen sich der Betroffene in räumlicher Abgeschiedenheit wähnen darf.[6] Äußerungen unterfallen dann nicht dem Schutz der Privatsphäre, sondern dem *Recht am eigenen Wort*, wenn es nicht um den (privaten) Inhalt, sondern um die unmittelbare Zugänglichkeit der Kommunikation ungeachtet ihres

---

2 BVerfGE 54, 148 ff.; zu den zivilrechtlichen Wurzeln: BGHZ 13, 334, 337; 26, 349 ff.

3 Siehe aus jüngerer Zeit BVerfGE 103, 21, 32 - DNA-Analyse; BVerfG-K RDV 2005, 214 ff. - Drogenscreening; BVerfG NJW 2005, 1338 ff. - Datenerhebung durch GPS; BVerfG-K RDV 2005, 213 ff. - Beweiserhebung über die sexuelle Orientierung einer Asylbewerberin; eine Vollzugsaussetzung des Gesetzes zur Förderung der Steuerehrlichkeit mit seinen Regelungen zum "gläsernen Bankkunden" hat das BVerfG abgelehnt, s. BVerfG-K NJW 2005, 1179 ff.

4 BVerfGE 65, 1, 42; 67, 100, 143; 78, 77, 84; 103, 21, 33.

5 BVerfGE 80, 367, 373 f.; 103, 21, 31; BVerfG NJW 2000, 2189 f.

6 BVerfGE 101, 361, 382 f. - Caroline von Hannover.

Inhalts geht.[7] Das Recht gewährleistet die Selbstbestimmung über die eigene Darstellung in der Kommunikation mit anderen und gibt die Befugnis, selbst zu entscheiden, wem ein Kommunikationsinhalt zugänglich sein soll.[8] Das *Recht am eigenen Bild* ist ebenfalls nicht auf private Angelegenheiten beschränkt, sondern soll dem Einzelnen Einfluss- und Entscheidungsmöglichkeiten über die Anfertigung und Verwendung von Fotografien und anderen Aufzeichnungen geben.[9] Es schützt auch vor der Verbreitung eines technisch manipulierten Bildes, das den Anschein erweckt, ein authentisches Abbild einer Person zu sein.[10] Das allgemeine Persönlichkeitsrecht mit seinen Teilausprägungen tritt zurück, sofern spezifische Freiheitsverbürgungen grundrechtlichen Persönlichkeitsschutz gewährleisten.[11] Das BVerfG hat in den vergangenen Jahren vor allem Feinarbeit an diesen Ausdifferenzierungen geleistet.[12]

2. Die Kommunikationsgeheimnisse des Art. 10 GG

Vorrangig gegenüber Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG sind die Kommunikationsgeheimnisse des Art. 10 GG.[13] Sie gewährleisten die freie Entfaltung der Persönlichkeit durch einen vor der Öffentlichkeit verborgenen, privaten Kommunikationsaustausch.[14] Die größte Bedeutung in der Judikatur des BVerfG kommt seit einigen Jahren dem Fernmeldegeheimnis zu.[15] Es soll vor Gefährdungen schützen, die unmittelbar aus dem Übermittlungsvorgang resultieren.[16] Da es dem Fernmeldegeheimnis um

---

7 BVerfGE 106, 28, 41.

8 BVerfGE 106, 28, 39; zur Anerkennung des Rechts am eigenen Wort s. BVerfGE 34, 238, 246 f.; 54, 148, 155.

9 BVerfGE 101, 361, 381.

10 BVerfG NJW 2005, 3271, 3272 - Ron Sommer.

11 BVerfGE 54, 148, 153; 99, 185, 193; 101, 361, 380.

12 Der Überblick beschränkt sich auf Art. 10 und 13 GG; informatorische Eingriffe können indessen auch weitere Grundrechte wie etwa die Meinungs- und Pressefreiheit (Art. 5 Abs. 1 GG) oder die Grundrechte des Art. 6 GG berühren.

13 BVerfG NJW 2005, 2603, 2604; BVerfGE 110, 33, 53; 100, 313, 358; 67, 157, 171; anders noch BVerfGE 57, 170, 177 ff., in der das Gericht die Kontrolle von Gefangenenpost an Art. 2 Abs. 1 GG maß.

14 BVerfGE 67, 157, 171; 110, 33, 53.

15 Siehe nur BVerfGE 67, 157 ff.; 85, 386 ff.; 100, 313 ff.; 106, 28 ff.

16 BVerfGE 106, 28, 36; 85, 386, 396; zur Grundrechtsberechtigung juristischer Personen: BVerfGE 106, 28, 43; zum Grundrechtsschutz öffentlich-rechtlicher Rundfunkanstalten: BVerfGE 107, 289, 312 f.

die Vertraulichkeit des Kommunikationsmediums geht, soll das Grundrecht nicht berührt sein, wenn einer der Gesprächspartnerinnen oder -partner durch Aktivierung einer Lautsprechervorrichtung die Teilhabe Dritter ermöglicht. Hier geht es um Risiken, die nicht die Übermittlungstechnik schafft,[17] sondern das Handeln einer der Gesprächspartnerinnen oder -partner. Insoweit liegt aber eine Berührung des Rechts am eigenen Wort vor.[18] Andererseits soll Art. 10 GG und nicht die Eigentumsgarantie maßstäblich sein, wenn ein Mobiltelefon zwecks Auslesens der gespeicherten Daten beschlagnahmt wird.[19]

3. Der Schutz der Wohnung nach Art. 13 GG

Art. 13 Abs. 1 GG gewährt einen räumlich geschützten Bereich der Privatsphäre, in dem jedermann das Recht hat, in Ruhe gelassen zu werden.[20] Den gegenständlichen Schutzbereich der Unverletzlichkeit der Wohnung hat das BVerfG weit gezogen, indem es auch Betriebs- und Geschäftsräume einbezieht.[21] Die Wohnung bedarf nicht nur des Schutzes gegen physisches Eindringen, sondern vor allem auch gegenüber Maßnahmen der optischen und akustischen Observation.[22] Die Regelung des "Großen Lauschangriffs" in Art. 13 Abs. 3 GG hat zwar die verfassungsgerichtliche Prüfung überstanden; das BVerfG hat aber die geschriebene Schranke des Art. 13 Abs. 3 GG um weitere Vorgaben angereichert, denen mehrere

---

17 Ein übermittlungsspezifisches Risiko liegt aber in der vom TK-Betreiber errichteten Fangschaltung, BVerfGE 85, 386, 397.

18 BVerfGE 106, 28, 39 ff.

19 BVerfG NJW 2005, 1637, 1639.

20 BVerfGE 51, 97, 107; 103, 142, 150 f.; 109, 279, 313 f.; BVerfG-K NJW 2005, 1637, 1638; zum Vorrang gegenüber Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG: BVerfGE 109, 279, 325 f.; für Personen, die von Überwachungsmaßnahmen in Wohnungen betroffen sind, ohne Wohnungsinhaber zu sein, bleibt es bei der Anwendung des informationellen Selbstbestimmungsrechts nach Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG.

21 BVerfGE 32, 54, 68 ff.; 76, 83, 88; nach BVerfGE 97, 228, 265 gilt dies auch, wenn der Hausrechtsinhaber Betriebs- und Geschäftsräume der Öffentlichkeit zugänglich gemacht hat; s. jüngst BVerwG DÖV 2005, 517 ff. - öffentlich zugängliches Vereinslokal; dazu Mittag, NVwZ 2005, 649 ff.; BGH NJW 2005, 3295 ff. - Selbstgespräch im Krankenzimmer; dazu Kolz, NJW 2005, 3248, 3249.

22 Art. 13 Abs. 1 GG schützt hingegen nicht vor einer Verpflichtung zur Auskunftserteilung über die privaten Wohnverhältnisse: BVerfGE 65, 1, 40.

Normen der Strafprozessordnung (StPO) nicht gerecht wurden.[23] Insbesondere bedürfen Lauschangriffe einer Abgrenzung vom Fernmeldegeheimnis. Das Abhören von Ferngesprächen durch "Anzapfen" der Leitung unterfällt dem Schutzbereich des Art. 10 Abs. 1 GG und nicht Art. 13 GG. Art. 13 GG ist hingegen sedes materiae, wenn durch technische Verwanzung der Wohnung Äußerungen in einem Telefongespräch abgehört werden.

III. Determinanten der Wandlungsprozesse und verfassungsgerichtliche Antworten

Das Grundgesetz ist verfassungsrechtliche Rahmenordnung. Die Rahmensetzung soll einerseits dem Parlamentsrecht Luft zum Atmen geben, indem sie nicht jede legislative Entscheidung *en detail* determiniert.[24] Die Verfassungsordnung muss in der Lage sein, auf gewandelte Gefährdungslagen zu reagieren. Will der Gesetzgeber aber den verfassungsrechtlichen Rahmen verschieben, setzt Art. 79 Abs. 3 GG die äußerste Grenze.

1. Fortentwicklung der Technik

Verfassungsgerichtliche Antworten auf die technologischen Wandlungsprozesse betreffen einerseits bereits die Konturierung des *Schutzbereichs* der Grundrechte. So ist zum Beispiel für das Fernmeldegeheimnis durch die Rechtsprechung des BVerfG anerkannt, dass auch neuere Kommunikationsmedien wie der Mobilfunk und der E-Mail-Verkehr vom Fernmeldegeheimnis umfasst sind. Entscheidend sind weder die Übermittlungsart noch die Ausdrucksform.[25] Dass nicht nur der Inhalt, sondern auch die Umstände der Kommunikation geschützt sind, entspricht seit geraumer Zeit der

---

[23] BVerfGE 109, 279, 316 ff. zu den aus Art. 79 Abs. 3 i.V.m. Art. 1 Abs. 1 GG folgenden Schranken; 109,279, 325 ff. zu §§ 100c, d StPO; das Sondervotum der Richterinnen Jaeger und Hohmann-Dennhardt hielt eine "verfassungskonforme" Auslegung von Art. 13 Abs. 3 GG nicht für möglich, vgl. 109, 279, 386 ff.; krit. auch Lepsius, Jura 2005, 433, 437 f.; s. nunmehr das Gesetz zur Umsetzung des BVerfG-Urteils vom 24.06.2005, BGBl. I, S. 1841; zum Gesetzentwurf krit. Leutheusser-Schnarrenberger, ZRP 2005, 1 ff.

[24] Grundlegend Böckenförde, NJW 1976, 2089, 2099.

[25] BVerfGE 106, 28, 36.

Rechtsprechung des BVerfG.[26] Diese Schutzseite hat besondere Bedeutung erlangt, weil neuere Telekommunikationsmedien routinemäßig die Modalitäten des Informationsverkehrs wie etwa abgehende, empfangene oder nicht beantwortete Anrufe aufzeichnen. Dies hat das BVerfG veranlasst, die Beschlagnahme eines Mobiltelefons zwecks Auslesens der gespeicherten Informationen an Art. 10 GG zu messen.[27]

Auch bei weiteren Ausprägungen der Rechte auf Privatheit ist verfassungsgerichtlich durch Schutzbereichsmodifizierungen reagiert worden. So ist die Ergänzung des Schutzbereichs des allgemeinen Persönlichkeitsrechts um eine räumliche Sphäre auch die verfassungsgerichtliche Antwort auf die Fortschritte optischer Observationstechniken, die sich Paparazzi zunutze machen.[28] Die Einbeziehung manipulierter Bilder in den Schutzbereich des Rechts am eigenen Bild ist Reaktion darauf, dass eine das Aussehen ändernde Bildmanipulation heute mit recht einfachen technischen Mitteln bewerkstelligt werden kann.[29] Und unter den technischen Bedingungen akustischer Überwachung muss das Grundrecht des Art. 13 Abs. 1 GG nicht nur gegen physisches, sondern auch gegen ein technisch vermitteltes Eindringen schützen.[30] Dabei soll nach der Mehrheitsmeinung des BVerfG ein eingriffsfester Kernbereich des Art. 13 Abs. 1 GG nicht raum-, sondern vor allem verhaltensbezogen bestimmt werden.[31]

Technikinduzierte Beeinträchtigungen der Schutzbereiche sind zumeist nichtförmliche, faktische *Eingriffe*. Dass aber Art. 2 Abs. 1, 10 Abs. 1 und 13 Abs. 1 GG die Figur des faktischen Grundrechtseingriffs voraussetzen, ist ebenfalls schon seit langem anerkannt. Bereits durch eine funktionale Schutzbereichsbestimmung reagiert das BVerfG auf die "Eingriffsketten", die unter den Bedin-

---

[26] BVerfGE 67, 157, 172; 85, 386, 396; 100, 313, 358; 107, 299, 312 f.; BVerfG NJW 2004, 2213, 2215; NJW 2005, 1637, 1639; NJW 2005, 2603, 2604.

[27] BVerfG-K NJW 2005, 1637, 1639; zu den technischen Möglichkeiten infolge der Digitalisierung s. BVerfGE 107, 299, 319.

[28] Mangels Grundrechtsbindung der Paparazzi kommen diese Vorgaben als Ausfluss staatlicher Schutzpflichten gegenüber dem streitentscheidenden Richter zum Tragen; zur grundrechtlichen Konstruktion s. BVerfGE 146, 149; 99, 185, 194 f.

[29] BVerfG NJW 2005, 3271, 3273.

[30] BVerfGE 65, 1, 40; 109, 279, 309.

[31] BVerfGE 109, 279, 314; krit. dazu Lepsius, Jura 2005, 433, 437, 439; Wefelmeier, NdsVBl. 2004, 289, 291; s.a. Ruthig, GA 2004, 587, 597 f.

gungen fortschreitender Datenverarbeitungstechniken typisch für informatorische Eingriffe sind. So schützt das Fernmeldegeheimnis nicht nur vor Eingriffen in den Übermittlungsvorgang, sondern auch vor Datenverarbeitungsprozessen, die sich hieran anschließen.[32]

Ein recht ausdifferenziertes Set von Vorgaben hat das BVerfG für die Anforderungen an die *Schranken* der Grundrechte unter den Bedingungen des technologischen Wandels entwickelt. Weil der Prozess technologischer Entwicklung neue Gefährdungen mit sich bringt, die der Gesetzgeber zunächst nicht vorausgesehen hat, nimmt das Gericht das *Parlament* in eine Beobachtungs- und Nachbesserungspflicht.[33] In seinem GPS-Urteil vom 12.04.2005 hat es allerdings die Erhebung und strafrechtliche Verwertung von GPS-generierten Daten als durch § 100f StPO gedeckt angesehen, obwohl dieses Gerät als Navigationsinstrument originär anderen Zwecken dient und im Übrigen mehr leistet als Peilsender oder Bewegungsmelder.[34]

Geht es beim Gesetzgeber um die richtige Einschätzung des grundrechtlichen Gefährdungspotentials, so muss bei der *Verwaltung* sichergestellt werden, dass sie nicht nur das Recht, sondern auch die Technik richtig anwendet. Der technische Fortschritt schafft neue Fehlerquellen. Die Grundrechte erfordern eine Gestaltung der Datenerhebung, mit der die inhaltliche Richtigkeit des Datums sichergestellt wird. Diese Anforderungen sah das Gericht bei einem Drogenscreening von Wehrdienstleistenden mittels Farbumschlagtests nicht gewahrt. Das technische Verfahren ermöglichte zwar eine fehlerfreie Feststellung von Drogenrückständen; es konnte aber nicht gewährleisten, dass die Testergebnisse der richtigen Person zugeordnet wurden.[35] Da eine Grundrechtsverletzung unabhängig davon besteht, ob das verfahrensfehlerhaft erhobene Datum in der Sache richtig ist, kommt den Verfahrensanforderungen

---

[32] BVerfGE 100, 313, 359, 366; 110, 33, 69; BVerfG NJW 2005, 2603, 2604; zum Eingriff in das Recht am eigenen Wort durch die zivilprozessuale Verwertung eines heimlich mitgeschnittenen Gesprächsinhalts s.a. BVerfGE 106, 28, 48; 85, 386, 399; zu Eingriffen in das informationelle Selbstbestimmungsrecht durch zivilprozessuale Verwertung von DNA-Analyse im Vaterschaftsanfechtungsprozess: BGH NJW 2005, 497, 498.

[33] BVerfGE 65, 1, 55; BVerfG-K NJW 2005, 1338, 1340.

[34] BVerfG-K NJW 2005, 1338, 1340; krit. Kutscha, NVwZ 2004, 1231, 1232 f.

[35] BVerfG RDV 2005, 214 ff.

"Selbststand" zu.[36] Die technischen Möglichkeiten schaffen zudem neue Gefährdungsquellen. Zur Sicherung eines abhörfreien Kernbereichs anempfiehlt deshalb das BVerfG einen Verzicht auf automatische Aufzeichnung der abgehörten Gespräche zugunsten einer Liveübertragung.[37]

2. Gefährdungen der staatlichen Sicherheit

Gefährdungen der staatlichen Sicherheit werden heute vor allem in Bedrohungen durch den internationalen Terrorismus und in der organisierten grenzüberschreitenden Kriminalität gesehen. Die staatlichen Antworten hierauf finden sich nur zum Teil im Bereich des materiellen Strafrechts. Größere Bedeutung haben Ermittlungs- und Eingriffsbefugnisse in der StPO, in den Sicherheitsgesetzen und in den Normen des Polizei- und Ordnungsrechts. Institute wie die polizeirechtliche Schleierfahndung oder die strategische Fernmeldeüberwachung nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Artikel 10 - G 10) ermöglichen eine verdachtslose Kontrolle von Personen im Vorfeld der konkreten Gefahrenabwehr. Normierte polizeiliche Vorfeldkontrollen sind teilweise überdies nicht allein auf die Straftatenverhütung, sondern eine später mögliche Strafverfolgung bezogen. Wenn sie zeitlich vor einer Straftat liegen, aber verfolgungsorientiert sind, verwischen sie die Grenze zwischen präventiver Gefahrenabwehr und repressiver Strafverfolgung.[38]

Die verfassungsgerichtlichen Antworten auf diese und weitere Eingriffslagen beanspruchen Geltung für *alle* Rechte auf Privatheit. Das BVerfG macht zum einen die *föderale*[39] *Kompetenzordnung* fruchtbar. Zu Recht wurde die Gesetzgebungskompetenz des Landes Niedersachsen für die vorsorgliche Überwachung der Telekommunikation im Hinblick auf eine allfällige spätere Strafverfol-

---

[36] BVerfG RDV 2005, 214, 215; s.a. jüngst BVerwG NJW 2005, 2330 ff.: Verletzung des informationellen Selbstbestimmungsrechts bei Datenweitergabe durch eine unzuständige Behörde.

[37] BVerfGE 109, 279, 323 f.; instruktive rechtsvergleichende Betrachtung mit den US-amerikanischen prozeduralen Sicherungen: Ruthig, GA 2004, 587, 602 ff.

[38] Nachdrücklich: BVerfG NJW 2005, 2603, 2605 f. zu § 33a NdsSOG.

[39] Zur (landes-)verfassungsrechtlich gebotenen Aufgabentrennung von Polizei und Verfassungsschutz s. instruktiv: SächsVerfGH NVwZ 2005, 1310 ff.; zur organisationsrechtlichen Trennung: SächsVerfGH LKV 1996, 273 ff.; s. dazu Kutscha, NVwZ 2005, 1232, 1234 m.w.N.

gung (Strafverfolgungsvorsorge) verneint, weil der Bund in der StPO die Überwachung zwecks Sicherung von Beweisen für das Strafverfahren kompetenzgerecht und abschließend geregelt habe.[40] Damit wurde ein langjähriger Streit um die Kompetenz für derartige Vorfeldmaßnahmen mit beträchtlichen Folgen für die Polizeigesetze der Länder entschieden.[41] Andererseits kann der Bund unter Umständen kraft Sachzusammenhangs auch präventivpolizeiliche Aufgaben regeln.[42]

Das Gebot, Beschränkungen des informationellen Selbstbestimmungsrechts nur durch Normen herbeizuführen, die qualifizierten Anforderungen an die *Bestimmtheit und Klarheit* gerecht werden,[43] hat das BVerfG unter ausdrücklicher Bezugnahme auf das Volkszählungsurteil auf die Schranken des Art. 10 GG übertragen und verstärkt.[44] Während die Bestimmtheitsanforderungen bei der Ermächtigung zu Maßnahmen der Strafverfolgung oder der Gefahrenabwehr wegen vorhandener tatbestandlicher Anknüpfungen relativ leicht zu wahren sind, gilt dies nicht für Vorfeldermittlungen. Diese sind wegen der Ungewissheit des späteren Handlungsablaufs besonders fehleranfällig. Umso bedeutsamer ist es, den handelnden Organen präzise Vorgaben zu machen, in welchen Fällen Maßnahmen der Strafverhütung oder der Vorsorge für eine spätere Strafverfolgung getroffen werden dürfen. Die Klarheit über die tatbestandlichen Voraussetzungen fehlte nach Auffassung des BVerfG sowohl den Überwachungsnormen im Außenwirtschaftsgesetz (AWG), deren Klarheit und Bestimmtheit an der Länge und Un-

---

[40] BVerfG NJW 2005, 2603, 2605 f. mit der Annahme einer Zuständigkeit nach Art. 74 Abs. 1 Nr. 1 GG. Die Straftatenverhütung rechnet allerdings kompetentiell zu der Gefahrenabwehr; zur Kompetenz nach Art. 74 Abs. 1 Nr. 1 GG bei der Regelung der DNA-Analyse für potentielle künftige Strafverfahren: BVerfGE 103, 21, 30.

[41] Zu den Konsequenzen s. Kutscha, NVwZ 2005, 1231, 1233; Stephan, VBlBW 2005, 410, 411; Waechter, NordÖR 2005, 393, 395; insb. zur Videoüberwachung: Zöller, NVwZ 2005, 1235, 1238 ff.

[42] Zu Maßnahmen der Straftatenverhütung nach § 39 AWG im Sachzusammenhang mit der ausschließlichen Kompetenz nach Art. 73 Nr. 5 GG: BVerfGE 110, 33, 48; zu den Bundeskompetenzen für die internationale Verbrechensbekämpfung nach Art. 73 Nr. 1 GG: BVerfGE 100, 313, 369 f.

[43] BVerfGE 65, 1, 44, 54.

[44] BVerfGE 100, 313, 359, 372; 110, 33, 53; BVerfG NJW 2005, 2603, 2607; zur Unverletzlichkeit der Wohnung nach Landesverfassungsrecht: SächsVerfGH NVwZ 2005, 1310, 1313.

übersichtlichkeit der Verweisungsketten litt,[45] als auch den polizeirechtlichen Normen des Landes Niedersachsen über die vorsorgliche Überwachung des Telekommunikationsverkehrs.[46]

Erhebliche Bedeutung kommt dem *Richtervorbehalt* zu. Er zielt auf eine vorbeugende Kontrolle durch eine unabhängige und neutrale Instanz, die am ehesten geeignet sein soll, die Interessen des Betroffenen zu wahren.[47] Eine vorherige richterliche Entscheidung ist bei Wohnraumdurchsuchungen (Art. 13 Abs. 2 GG), beim "Großen Lauschangriff" (Art. 13 Abs. 3 und Abs. 4 GG) und bei Freiheitsentziehungen (Art. 104 Abs. 2 GG) von Grundrechts wegen angeordnet. Eine richterliche Entscheidung über Observationsmaßnahmen hält das BVerfG aber auch dort für erforderlich, wo sie das Grundrecht nicht ausdrücklich vorsieht. § 163f Abs. 4 Satz 2 StPO, der Observationen im Bereich der Strafverfolgung von mehr als einem Monat unter Richtervorbehalt stellt, wurde ausdrücklich im Rahmen der Schrankenprüfung am Maßstab des Art. 2 Abs. 1 GG herangezogen,[48] und der einfachgesetzliche Richtervorbehalt der §§ 100g und h StPO für das Abfragen von Telekommunikationsdaten bei den Telekommunikationsanbietern soll erst recht gelten, wenn ein Mobiltelefon zum Zwecke des Auslesens der Daten beschlagnahmt wird.[49]

In der Sache muss der richterliche Beschluss messbar und kontrollierbar sein, er ist keine bloße Formsache.[50] Das prozedurale Erfordernis einer vorgängigen richterlichen Entscheidung ist selbst wiederum durch Organisation und Verfahren zu sichern. Sie müssen dafür Sorge tragen, dass die richterliche Entscheidung der Regelfall und die staatsanwaltliche Anordnung als Eilkompetenz die

---

45 BVerfGE 110, 33, 57 ff., s. nunmehr die Neuregelung durch Gesetz vom 21.12.2004, BGBl. I, S. 3603.

46 BVerfG NJW 2005, 2603, 2607 ff.; eine Annäherung an die Voraussetzungen konkreter Gefahrenabwehr konstatiert Waechter, NordÖR 2005, 393, 396.

47 BVerfGE 103, 142, 151; 109, 279, 358; BVerfG-K NJW 2005, 275 f.; BVerfG-K NJW 2005, 1637, 1638.

48 BVerfG NJW 2005, 1338 ff.

49 BVerfG-K NJW 2005, 1637, 1640.

50 BVerfGE 103, 142, 151 f.; 109, 279, 359; problematisch deshalb BVerfG-K NJW 2005, 275 f.: Ein vom Amtsgericht verwendetes Formular für einen Durchsuchungsbeschluss i.S.v. Art. 13 Abs. 2 GG, in dem Tatvorwurf und -umstände nur anzukreuzen sind, wird den grundrechtlichen Anforderungen noch gerecht.

begründungsbedürftige Ausnahme ist.[51] Durch organisationsrechtliche Vorkehrungen ist deshalb die Erreichbarkeit eines Richters nicht nur tagsüber, sondern auch während der Nachtzeit sicherzustellen, wenn hierfür ein praktisches Bedürfnis besteht. Die Vollzugsbeamtinnen und -beamten dürfen eine Durchsuchung nicht durch vorheriges Zuwarten selbst unaufschiebbar machen.[52] Die prozeduralen Vorgaben werden bis zu den Vollzugsorganen heruntergebrochen. Wird ohne einen vorherigen Richterbeschluss eingegriffen, müssen Staatsanwaltschaft und Vollzugsbeamtinnen und -beamten in einem Vermerk die genauen Umstände ihres Handelns dokumentieren, um eine nachträgliche gerichtliche Überprüfung der Voraussetzungen der Gefahr im Verzuge zu ermöglichen.[53] Überdies ist im Rahmen der Strafverfolgung gegebenenfalls durch länderübergreifende Koordination sicherzustellen, dass nicht verschiedene Hoheitsträger in Doppelverfahren kumulativ in Grundrechte eingreifen.[54]

Soweit Gesetze an diesen oder weiteren Vorgaben scheitern,[55] dienen die materiellen Grenzen, maßgeblich das Verhältnismäßigkeitsprinzip, nur noch als bestätigende Gegenkontrolle.[56] Allerdings hat das BVerfG in seiner Entscheidung zum "Großen Lauschangriff" mit dem abhörfreien Kernbereich eine *substantielle Grenze* gesetzt, die auch durch ausgefeilte Verfahren nicht überwunden werden kann. Der Menschenwürdegehalt des Art. 13 Abs. 1 GG lässt es auch bei überwiegenden Interessen der Allgemeinheit nicht zu, in diesen Kernbereich einzugreifen.[57] Sofern es dennoch zur Überwachung von höchstpersönlichen Gefühlsäußerungen, Äußerungen des unbewussten Erlebens oder Ausdrucksformen der

---

[51] Zu den Anforderungen an die Gefahr im Verzuge: BVerfGE 103, 142, 154 f.; zum Sonderfall des Art. 13 Abs. 3 S. 4 GG: BVerfGE 109, 279, 362.

[52] BVerfGE 103, 142, 152, 155; BVerfG-K NJW 2005, 1637, 1638.

[53] BVerfG-K NJW 2005, 1337, 1338; zur vollen gerichtlichen Kontrolle: BVerfGE 103, 142, 156 ff.

[54] BVerfG NJW 2005, 1337, 1338.

[55] Zu den Rechtsschutz ermöglichenden Mitteilungspflichten nach dem G 10 und der Kontrolle durch die G 10-Kommission: BVerfGE 100, 313, 397 ff., 401 ff.; zu Benachrichtigungspflichten nach Art. 13 Abs. 3 GG: BVerfGE 109, 279, 363 ff.

[56] So etwa in BVerfG NJW 2005, 2603, 2609 ff.

[57] BVerfGE 109, 279, 313; zur Übertragung auf die durch Art. 13 Abs. 4 GG erlaubten Eingriffe: SächsVerfGH NVwZ 2005, 1310, 1314; Kutscha, NVwZ 2005, 20, 22; Gusy, JuS 2004, 457, 461; Ruthig, GA 2004, 587, 606; Wefelmeier, NdsVBl. 2004, 289, 290, 292 ff.

Sexualität kommt, gebietet wiederum die prozedurale Seite des Grundrechts Vorkehrungen, die die Eingriffsfolgen mildern. Das BVerfG nennt den sofortigen Abbruch der (Live-)Überwachung bei unerwarteter Aufnahme von Intimäußerungen, die Löschung bereits erlangter Daten und strafprozessuale Verwertungsverbote.[58] Auch diese Maßgaben hat das Gericht auf weitere privatheitsbezogene Rechte, maßgeblich Art. 10 GG, übertragen.[59]

3. Internationalisierung der Kommunikationsbeziehungen

Kommunikationsbeziehungen zwischen Privaten, aber auch solche zwischen öffentlichen Stellen internationalisieren sich in zunehmendem Maße. Erleichterte technische Bedingungen spielen hierbei ebenso eine Rolle wie die internationale Verflechtung Deutschlands in der Staatengemeinschaft. Es entspricht der Völkerrechtsfreundlichkeit des Grundgesetzes, sich den Rechtsentwicklungen der internationalen Staatengemeinschaft zu öffnen.[60] Ein eng verstandenes Territorialitätsprinzip könnte aber dazu führen, dass nur Grundrechtsbeeinträchtigungen, die von deutscher staatlicher Gewalt auf deutschem Boden verübt werden, am Grundgesetz zu messen sind. Das BVerfG hat indessen klargemacht, dass der Grundrechtsschutz weiter reicht.[61] In der *Maastricht*-Entscheidung sieht es den "Grundrechtsschutz in Deutschland und insoweit nicht nur gegenüber deutschen Staatsorganen" gewährleistet.[62] Deshalb können auch Akte anderer Staaten oder zwischenstaatlicher Ein-

---

[58] BVerfGE 109, 279, 318 f.; 324, 332 f.; SächsVerfGH NVwZ 2005, 1310, 1314; s. nunmehr § 100c Abs. 5 S. 3 StPO; zur strafprozessualen Verwertung von Daten aus der Kernsphäre: BGH NJW 2005, 3295 ff. - Selbstgespräch im Krankenzimmer; dazu Kolz, NJW 2005, 3248 ff.

[59] BVerfG NJW 2005, 2603, 2611 f.; Kutscha, NVwZ 2005, 20, 22; ders., NVwZ 2005, 1231, 1232; Puschke/Singelnstein, NJW 2005, 3534, 3536; zu den technischen Schwierigkeiten der Übertragung auf die Überwachung des Fernmeldeverkehrs: Stephan, VBlBW 2005, 410, 412.

[60] Siehe nur Präambel und Art. 1 Abs. 2, 9 Abs. 2, 23 - 26, 59 Abs. 2 GG; zur Völkerrechtsfreundlichkeit des GG und ihren Konsequenzen: BVerfGE 6, 309, 362 f.; 31, 58, 75; 75, 1, 17; Tomuschat, VVDStRL 36 (1978), 7, 18; Bernhardt, DÖV 1977, 457 ff.; Bleckmann, DÖV 1996, 137 ff.

[61] Instruktiver Überblick von Ruthig: Einwirkungen der Grundrechte auf das Zivilrecht, Öffentliche Recht und Strafrecht, Wolter/Riedel/Taupitz (Hrsg.),1999, S. 271.

[62] BVerfGE 89, 155, 175, in Abweichung von BVerfGE 58, 1, 27 - Eurocontrol.

richtungen im territorialen Geltungsbereich des Grundgesetzes ihre Grenze an den Grundrechten finden.[63]

Zudem hat das Gericht in räumlicher Beziehung frühzeitig eine Entterritorialisierung eingeleitet und Akte der deutschen Gewalt dem Grundrechtsschutz unterstellt, soweit sie im Ausland ausgeübt werden oder ihre Wirkungen im Ausland eintreten.[64] Diese Entwicklungslinie ist auch für die Rechte auf Privatheit bedeutsam, sofern deutsche Organe in ausländische Kommunikationsbeziehungen eingreifen. In seiner Entscheidung zum G 10 urteilte das BVerfG folgerichtig, dass auch ausländische Telekommunikationsbeziehungen in den Schutzbereich des Art. 10 Abs. 1 GG fallen, wenn sie von auf deutschem Boden stationierten Empfangsanlagen des Bundesnachrichtendienstes (BND) abgehört werden können. In diesem Fall ist eine Kommunikation im Ausland mit dem Handeln deutscher Behörden derart verknüpft, dass die Grundrechtsbindung ungemindert[65] eingreifen muss.[66] Diese Entwicklungslinie ist umso bemerkenswerter, als andere Staaten dem Territorialitätsprinzip deutlich enger verhaftet bleiben. Eine auf das Staatsgebiet begrenzte Grundrechtsbindung liegt etwa dem US-amerikanischen Verfassungsverständnis zugrunde und erklärt, weshalb es "grundrechtsfreie" Einrichtungen wie den auf Kuba gelegenen Stützpunkt *Guantánamo* gibt.[67]

---

[63] Allerdings hat das BVerfG in der Maastricht-Entscheidung an seiner Solange II-Entscheidung (E 73, 339, 387) festgehalten und die Ausübung seiner Prüfungskompetenzen über (abgeleitetes) EG-Recht weitgehend zurückgestellt, s. BVerfGE 89, 155, 175; nachdrücklich 102, 147, 163 f. - Bananenmarktordnung. Die Erstreckung des Grundrechtsschutzes dürfte gegenüber solchen zwischenstaatlichen Einrichtungen zum Tragen kommen, die einen vergleichbaren Grundrechtsschutz nicht aufweisen, so auch Ruthig (Fn. 61), S. 278.

[64] BVerfGE 6, 290, 295; 31, 58, 75 f.; 92, 26 ff.

[65] In der Zweitregister-Entscheidung hatte das BVerfG dem Gesetzgeber einen größeren verfassungsrechtlichen Spielraum für Regelungen mit Auslandsbezügen eingeräumt und damit eine "geminderte" Grundrechtsbindung zugelassen, s. BVerfGE 92, 26, 41 f.

[66] BVerfGE 100, 313, 363 f.

[67] Siehe etwa 494 U.S. 259, 264 (1990) zur Wohnungsdurchsuchung durch US-amerikanische Behörden in Mexiko; weitere Nachweise bei Ruthig (Fn. 61), S. 289.

4. Privatisierung staatlicher Dienste der Daseinsvorsorge

Die Privatisierung staatlicher Dienste der Daseinsvorsorge ist Ausweis eines geänderten Verständnisses von Umfang und Art staatlicher Aufgaben. Die Privatisierung der Telekommunikationsdienstleistungen in Deutschland verdankt sich vornehmlich den Vorgaben des Gemeinschaftsrechts. Art. 87f GG umschreibt die geänderte Rolle des Staates: Während Telekommunikation und postalische Dienstleistungen in privatwirtschaftlicher Form erbracht werden (Art. 87f Abs. 2 GG), gewährleistet der Bund flächendeckend angemessene und ausreichende Dienstleistungen (Art. 87f Abs. 1 GG). Der Staat hat sich damit vom unmittelbaren Leistungserbringer zum Garanten einer angemessenen Infrastruktur gewandelt. Die verfassungsrechtliche Pflicht zur Infrastrukturgewährleistung wird einfachgesetzlich vor allem durch das Telekommunikationsgesetz (TKG) umgesetzt, das ein bedeutsames Element eines neuen so genannten Regulierungsverwaltungsrechts ist. Die grundrechtlichen Implikationen, die mit der Privatisierung einhergehen, lassen sich am Beispiel des Fernmeldegeheimnisses beleuchten.[68]

Der Wortlaut des Art. 10 Abs. 1 GG entspricht dem Stand der Kommunikationsentwicklung von 1949. Als *Abwehrrecht* sollte das Fernmeldegeheimnis sowohl vor Abhörmaßnahmen staatlicher Sicherheitsorgane schützen als auch vor Eingriffen, die vom staatlichen Fernmeldewesen selbst ausgehen.[69] Allerdings ist dem Grundrecht in letzterer Hinsicht der Adressat abhanden gekommen. Dies gilt zum einen unbestritten, sofern private Anbieterin-

---

[68] Auch das Postgeheimnis bedarf der Anpassung, weil die postalische Beförderung mit der Privatisierung nicht mehr in staatlicher Hand ist. Zur Verhinderung von Schutzlücken wird teilweise für die unmittelbare Drittwirkung des Postgeheimnisses plädiert, so Skouris, EuR 1999, 111, 125 f.; vorzugswürdig erscheint demgegenüber der Weg, auch die Beförderung durch private Anbieter als postalische Dienstleistung und damit als Post i.S.v. Art. 10 Abs. 1 GG zu qualifizieren und insoweit den Schutzgegenstand jedenfalls gegenüber Maßnahmen der Sicherheitsdienste zu erhalten; weil aber private Diensteanbieterinnen und -anbieter selbst nicht grundrechtsverpflichtet sind, sind Eingriffe durch sie nicht an der Abwehrfunktion zu messen; insoweit muss der Gesetzgeber sicherstellen, dass das Postgeheimnis auch bei der Beförderung durch Private gewahrt bleibt, s. Pieroth/Schlink, Grundrechte, Rn. 771; Löwer, in: v. Münch/Kunig, GG, Bd. 1, Art. 10 Rn. 14 f.; Groß, JZ 1999, 326, 332 f.

[69] BVerfGE 67, 157, 172; 85, 386, 396, jeweils mit Betonung des Schutzes gegenüber den Sicherheitsbehörden.

nen oder Anbieter Telekommunikationsdienstleistungen erbringen. Als privatwirtschaftliche Unternehmen sind sie nicht an die Grundrechte und damit auch nicht an das grundrechtliche Fernmeldegeheimnis gebunden.[70] Nach ganz überwiegender Auffassung ist aber auch die Deutsche Telekom AG als Nachfolgerin des einstigen staatlichen Monopolanbieters nicht mehr grundrechtsverpflichtet, auch wenn sich circa 43 Prozent der Aktien noch im Besitz der öffentlichen Hand befinden.[71]

Die Lücken des abwehrrechtlichen Schutzes, die aus der materiellen Privatisierung resultieren, lassen sich aber über die *Schutzfunktion* der Grundrechte teilweise schließen. Drohen grundrechtliche Gefährdungen durch private Dritte, muss alle staatliche Gewalt im Rahmen ihrer jeweiligen Kompetenzen grundrechtlichen Schutz gewährleisten.[72] Diese Schutzpflicht gilt auch für das Fernmeldegeheimnis, wie das BVerfG betont hat.[73] Der Gesetzgeber hat seine Schutzpflichten insbesondere durch § 88 TKG erfüllt, der detaillierter als Art. 10 GG den Schutzumfang des Telekommunikationsgeheimnisses regelt und alle gewerblichen Diensteanbieterinnen und -anbieter in die Pflicht nimmt. Daneben bestehen zivilrechtli-

---

[70] Ein dem Staat zurechenbarer Eingriff in das Fernmeldegeheimnis liegt jedoch vor, wenn privatrechtliche TK-Anbieterinnen und -anbieter von staatlichen Stellen angewiesen werden, bei Bürgerinnen und Bürgern Verbindungsdaten zu erheben, BVerfGE 107, 299, 313 f.

[71] Nach Löwer, in: v. Münch/Kunig, GG, Bd. 1, Art. 10 Rn. 9 ließ bereits die Organisationsprivatisierung die Grundrechtsbindung entfallen; auf Art. 87f Abs. 2 GG abstellend auch: BVerwGE 114, 160, 189; Lang, NJW 2004, 3601 ff.; nimmt man hingegen die Wesensformel des Art. 19 Abs. 3 GG zum Ausgangspunkt, ist vor allem das "personale Substrat" entscheidend; für die eigenständige Willensbildung der Deutschen Telekom AG spricht der starke Streubesitz, dazu der Umstand, dass - ungeachtet der immer noch recht hohen staatlichen Beteiligungsquote - der Bund keinen beherrschenden Einfluss im Rahmen der Beteiligungsverwaltung ausüben kann, s. dazu ausführlich Windthorst, VerwArch 95 (2004), 377, 388 ff.; s.a. v. Arnauld, DÖV 1998, 437 ff. Das BVerfG wird demnächst in einem Verfassungsbeschwerdeverfahren zum grundrechtlichen Eigentumsschutz der Deutschen Telekom AG für Betriebs- und Geschäftsgeheimnisse Stellung nehmen müssen - dazu die angegriffenen Beschlüsse des BVerwG: NWVBl 2004, 18 ff.; DVBl 2004, 62 ff.; NVwZ 2004, 745 ff.

[72] BVerfGE 39, 1, 42 ff.; 46, 160, 164; 49, 89, 140; 77, 170, 214; 88, 203, 251; 89, 214, 229 ff.

[73] BVerfGE 106, 28, 37; s.a. Groß, JZ 1999, 326, 332 ff.; Schoch, VVDStRL 57 (1998) 158, 206.

che Schadensersatzansprüche (§ 44 TKG), und das strafrechtliche Verbot wurde neu gefasst (§ 206 Strafgesetzbuch - StGB).

Gleichwohl sind Schutzlücken bei der Umwandlung der Abwehr- in die Schutzfunktion des Grundrechts nicht auszuschließen. Dies folgt aus der unterschiedlichen Struktur von Abwehr- und Schutzrechten. Liegt nämlich ein grundrechtlicher Eingriff vor, so bildet diese konkrete staatliche Maßnahme auch den Gegenstand für die Prüfung der verfassungsrechtlichen Rechtfertigung. Steht hingegen das Unterlassen von Schutz in Frage, so stehen der staatlichen Gewalt zumeist verschiedene Optionen der Schutzpflichtenerfüllung zur Verfügung,[74] sofern diese ein ausreichendes Maß an Schutz gewährleisten (Untermaßverbot).[75] Der strukturelle Spielraum bildet sich in der verfassungsgerichtlichen Judikatur ab, die individuelle Schutzansprüche der Bürgerinnen und Bürger auf staatliches Handeln zwar grundsätzlich anerkennt, die Überprüfung gesetzgeberischer Aktivitäten aber darauf beschränkt, ob sie zur Schutzpflichtenerfüllung evident untauglich sind.[76] In der prozessualen Durchsetzbarkeit des Untermaßverbots hinken deshalb die Schutzansprüche den Abwehrrechten systematisch hinterher. Diese Einsicht lässt sich über das Telekommunikationsgeheimnis hinaus auf andere Felder materieller Privatisierung mit Gefährdungsgehalt für die Privatheit übertragen. Sie ist umso misslicher, als das Grundgesetz nur wenige unverrückbare Privatisierungssperren kennt.

5. Die Tyrannei der Intimität

Der amerikanische Soziologe *Richard Sennett* sah bereits in den 70er Jahren des vergangenen Jahrhunderts den Verfall der Öffentlichkeit vor allem in einer neuen Tyrannei der Intimität.[77] Das sozialpsychologische Gegenstück zu Habermas "Strukturwandel der

---

[74] Dazu auch BVerfGE 96, 56, 64; s.a. Alexy, Theorie der Grundrechte, 3. Aufl., 1996, S. 420 ff.

[75] Zum Untermaßverbot prägend: Canaris, AcP 184 (1984), 201, 228; aufgegriffen in BVerfGE 88, 203, 254.

[76] BVerfGE 77, 170, 215; 92, 26, 47; BVerfG NJW 2002, 1638 ff.; VGH BW VBlBW 2004, 262 ff.; krit. zur Bedeutung des Untermaßverbots für die verfassungsgerichtliche Kontrolle Schoch, VVDStRL 57 (1998) 158, 206; s.a. Kämmerer, JZ 1996, 1042, 1049.

[77] Sennett, The Fall of Public Man, 1974; dt. Ausgabe unter dem Titel: Verfall und Ende des öffentlichen Lebens. Die Tyrannei der Intimität, 1983.

Öffentlichkeit" diagnostizierte einen Drang zu narzisstischen Formen der Veröffentlichung des Privaten. Die Formen der Selbstgefährdung der Privatheit sind vielfältig. Um sie zu erfassen, bedarf es nicht der Augenscheinnahme nachmittäglicher Fernseh-Talkshows. Es reicht vollkommen aus, sich zu beliebiger Zeit in den Speisewagen eines ICE zu setzen, um nach kürzester Zeit unfreiwilliger Ohrenzeuge von telefonisch ausgetragenen Beziehungskonflikten zu werden oder sachkundige Erörterungen über allenfalls halblegale Steuertricks unter präziser Angabe des zu verschleiernden Einkommens zu hören. Der Laie staunt, die Datenschützerin verzweifelt.

Die beschriebenen Formen der Selbstentäußerung im öffentlichen Raum haben gemein, dass sie Kommunikation zwischen Privaten betreffen, die ihrerseits allein grundrechtsberechtigt sind. Insoweit ist die freiwillige Preisgabe intimer Informationen über die eigene Person Grundrechtsgebrauch. Können die Worte von einer unbestimmten Vielzahl von Personen mitgehört werden, so haben sich die Sprecherin oder der Sprecher deren Kommunikationsteilhabe selbst zuzuschreiben.[78]

Anders stellt sich aber die Lage dar, wenn ein privates Telefongespräch mittels einer gebräuchlichen Mithörvorrichtung von einer dritten Person mitgehört wird. Das BVerfG hat sich in überaus deutlichen Worten gegen die Annahme der Zivilgerichte verwahrt, mit dem Mithören einer dritten Person sei angesichts der Verbreitung von Lautstellvorrichtungen und Zweithörern immer zu rechnen, weshalb im Führen eines Telefongesprächs letztlich eine stillschweigende Einwilligung in die Informationsteilhabe Dritter zu sehen sei.[79] Wenn auch das BVerfG die Möglichkeit einer konkludenten Einwilligung nicht generell verwirft, verlangt es doch zu Recht klare Anhaltspunkte dafür, dass unter den gegebenen Bedingungen des sozialen, geschäftlichen oder privaten Kommunikationsverhaltens von der Zustimmung zum Mithören auszugehen sei.[80] Berechtigte Vertraulichkeitserwartungen können nicht gehegt wer-

---

78 BVerfGE 106, 28, 40.

79 Zum Problem der konkludenten Einwilligung in Telefonwerbung BGH NJW 1989, 2820; BGH JZ 1990, 251 ff.

80 Bzgl. der zivilprozessualen Verwertung mitgehörter Gesprächsinhalte: BVerfGE 106, 28, 47; eine Einwilligung kommt von vornherein nicht in Betracht, wenn nur auf Antrag einer der an der Telekommunikation beteiligten Personen eine Fangschaltung installiert wird: BVerfGE 85, 386, 398 f.

den, wenn an der Geräuschkulisse bemerkt werden kann, dass die Gesprächspartnerin oder der Gesprächspartner in einem nicht abgeschlossenen Raum telefoniert und gleichwohl das Gespräch fortsetzt.[81] Es ist allerdings zu befürchten, dass das reale Telekommunikationsverhalten der meisten Bürgerinnen und Bürger mit der abstrakten Einsicht in die geminderte Vertraulichkeit bei Gesprächen in nicht räumlich abgetrennten Telefonzellen oder mit Mobiltelefonen bislang nicht Schritt hält.

Von freiwilligen Entäußerungen sind des weiteren Handlungs- und Äußerungsformen zu unterscheiden, deren öffentlicher Charakter allein daraus resultieren soll, dass sie von einer Person des öffentlichen Lebens ausgehen. Das BVerfG hat in seiner *Caroline*-Entscheidung unmissverständlich klargestellt, dass Schutzbedürfnisse gegenüber medialen Zugriffen auch bei Personen bestehen, die aufgrund von Rang, Ansehen oder aus anderen Gründen besondere öffentliche Beachtung finden.[82] Es hat aber zu Recht darauf hingewiesen, dass der grundrechtliche Schutz entfällt, wenn sich jemand etwa durch Abschluss von Exklusivverträgen über die Berichterstattung damit einverstanden erklärt, dass als privat geltende Angelegenheiten öffentlich gemacht werden. In diesem Fall lässt sich eine unautorisierte Veröffentlichung nicht unter Berufung auf das allgemeine Persönlichkeitsrecht verhindern, das keinen Schutz der "Kommerzialisierung der eigenen Person" gewährt.[83] Die Auffassung des BVerfG, angesichts der modernen Entwicklung zum Infotainment könne auch ein legitimes Bedürfnis der Öffentlichkeit an Umständen aus dem rein privaten Leben Prominenter bestehen,[84] ist allerdings auf den Widerspruch des Europäischen Gerichtshofs für Menschenrechte (EGMR) gestoßen. Er sieht die Presse in einer traditionellen "Wachhund"-Rolle und erkennt ein Bedürfnis an der Veröffentlichung privater Umstände allenfalls bei Personen an, die öffentliche oder amtliche Funktionen wahrnehmen.[85] Das Plädoyer für eine strikte Trennung von öffentlichen und privaten Funktionen hat wegen seiner Ignoranz des Zusammen-

---

81 BVerfGE 106, 28, 47.

82 BVerfGE 101, 361, 383.

83 BVerfGE 101, 361, 389; zur Selbstpreisgabe als Grenze des Schutzes s.a. BGH NJW 2004, 766 f. - Feriendomizil II; BGH NJW 2005, 594, 595 f. - Begleiterin von Teewag.

84 BVerfGE 101, 361, 390 f.; Soehring, AfP 2000, 230 ff.; Soehring/Seelmann-Eggebert, NJW 2000, 2466 ff.

85 EGMR NJW 2004, 2647, 2649 ff., Nr. 63 ff., in Auslegung von Art. 8 und 10 EMRK; dazu Heldrich, NJW 2004, 2634 ff.

hangs von Prominenz, Medien und Publikum und seines verengten Blickwinkels auf die Funktionen der Presse berechtigte Kritik gefunden.[86] Auch wenn das EGMR-Urteil unmittelbare Bindungswirkung nur für den entschiedenen Fall erzeugt,[87] wird aber seine Orientierungswirkung vor allem die zivilgerichtliche Kategorisierung von so genannten absoluten und relativen Personen der Zeitgeschichte beeinflussen.[88]

IV. Ausblick

1. Bereichsspezifik oder Konvergenz des Grundrechtsschutzes?

Der nur kursorische Überblick über die Entwicklungen der Rechte auf Privatheit zeigt zum einen, dass das BVerfG in der Bestimmung der Schutzbereiche der betroffenen Grundrechte überaus filigrane Abgrenzungen getroffen hat. Dies leuchtet jeder Verfassungsrechtlerin und jedem Verfassungsrechtler unmittelbar ein, weil Art. 2 Abs. 1, 10 Abs. 1 und 13 Abs. 1 GG unterschiedlichen verfassungsrechtlichen Schranken unterliegen. Indessen lässt sich das Gericht bei der Bestimmung der Eingriffsschranken von einer grundrechtsüberspannenden Dogmatik leiten, die ihren Ausgangspunkt bei den

---

[86] Ladeur, ZUM 2004, 879, 881 ff.; Bölke/Gostomzyk, Jura 2005, 336, 337 f.

[87] Art. 46 Abs. 1 EMRK; zu Umfang und den Grenzen der Bindungswirkung der EMRK und Urteilen des EGMR: BVerfGE 111, 307 ff.: die EMRK teilt den Rang des Zustimmungsgesetzes i.S.v. Art. 59 Abs. 2 GG als einfaches Bundesgesetz und ist - auch in ihrer Auslegung durch den EGMR - für deutsche Gerichte nach Art. 20 Abs. 3 GG beachtlich; unbeschadet der Völkerrechtsfreundlichkeit des GG kann es aber Konstellationen geben, in denen nicht nur der allein der Verfassung unterworfene Gesetzgeber, sondern auch die Gerichte die EMRK nicht beachten müssen, wenn diese gegen tragende Grundsätze der Verfassung verstößt; s.a. Meyer-Ladewig/Petzold, NJW 2005, 15 ff.

[88] Zur Grundlegung dieses Begriffs Neumann-Duesberg, JZ 1960, 114; der EGMR äußert Zweifel, ob sich der zivilgerichtliche Begriff der absoluten Person der Zeitgeschichte mit seinen Implikationen mit Art. 8 EMRK vereinbaren lässt, NJW 2004, 2647, 2650, Nr. 73; für eine Restriktion Heldrich, NJW 2004, 2634, 2636; Bölke/Gostomzyk, Jura 2005, 336, 338; auch unter Berücksichtigung der Maßstäbe des EGMR hielt der BGH jüngst in drei Parallelentscheidungen Zeitungsberichte über gravierende Verkehrsverstöße von Ernst August von Hannover für gerechtfertigt, s. BGH, Urt. v. 15.11.2005 - VI ZR 286-288/04 - jeweils Umdruck S. 11 ff.

Vorgaben des Urteils zum Volkszählungsgesetz nimmt. Es spricht für die Frische oder doch für die Zeitlosigkeit dieser Entscheidung, dass ihre Vorgaben an den grundrechtsbeschränkenden Gesetzgeber sich als flexibel für künftige Konfliktlagen erwiesen haben. Das BVerfG geht offenbar von einem weiten *right of privacy* aus, das sich auf verschiedene Grundrechtsnormen verteilt, und für das gemeinsame Schranken maßgeblich sind.

Die Konvergenz der grundrechtlichen Anforderungen kontrastiert allerdings auffällig mit der Buntscheckigkeit der einfachgesetzlichen Lage. Es ist die besondere Pointe des grundrechtsüberspannenden Gebots "bereichsspezifischer" Regelungen,[89] dass die Unzahl derartiger bereichsspezifischer und sachlich divergierender Regelungen[90] für die allgemeinen Datenschutzgesetze nur noch residuale Anwendungsräume belässt.

2. Verfassungsrechtliche Anforderungen: Procedure over Substance?

Die Schrankenanforderungen, die das BVerfG grundrechtsübergreifend zugrunde legt, sind ganz überwiegend prozeduraler Art. Dies beginnt bei Verfahrenspflichten des Gesetzgebers in Gestalt von Beobachtungspflichten und setzt sich fort in Anforderungen an die Beschaffenheit der Norm hinsichtlich ihrer Bestimmtheit und Klarheit. Jedenfalls im Bereich der staatlichen Sicherheit und der Strafverfolgung ist der Richtervorbehalt bedeutsam.

Mit dem Einbau verfahrensrechtlicher Sicherungen werden aber substantielle Schranken nicht überflüssig. Dies zeigt sich besonders deutlich bei den Grenzen des "Großen Lauschangriffs", der bei einer abhörfreien Kernzone von Verfassung wegen enden muss. Die Verfahrensvorgaben wurden überdies gerade deshalb entwickelt, um in besonderer Weise den Schutz der Privatsphäre rechts-

---

89 BVerfGE 65, 1, 46; 100, 313, 360; 110, 33, 53.

90 Insbesondere die polizeirechtlichen Datenschutzregelungen divergieren erheblich: So sind z.B. durch Einsatz technischer Mittel gewonnene Daten in Rheinland-Pfalz und Bayern nach zwei Monaten zu vernichten (§ 27 Abs. 6 Satz 2 POG Rh-Pf, Art. 32 Abs. 4 BayPAG), in Nordrhein-Westfalen jedenfalls Videoaufnahmen bereits nach 14 Tagen (§ 15a Abs. 2 PolG NRW). Eine Telekommunikationsüberwachung kann in Rheinland-Pfalz beliebig oft verlängert werden, in Hessen jedoch höchstens dreimal (§ 31 Abs. 5 Satz 3 POG Rh-Pf, § 15a Abs. 4 Satz 4 i.V.m. § 15 Abs. 5 HSOG).

staatlich zu umhegen.[91] Sie stellen keinen Ersatz für ein materielles Konzept des Schutzes der Privatheit dar. So können etwa unpräzise Eingriffsnormen nicht durch das Gebot einer vorherigen richterlichen Entscheidung kompensiert werden.[92] Die Vorstellung einer substantiell geschützten Kernsphäre der Persönlichkeit kann aber nicht dauerhaft *gegen* die Bürgerinnen und Bürger verteidigt werden, die diesen Kern nicht selten preisgeben oder gar - ebenfalls nicht selten - geschwätzig Intimitäten Dritter verbreiten. Bei Gefährdungen durch private Dritte mögen legislative Schutzgesetze für eine begrenzte Remedur sorgen. Gegen unveranlasste Selbstpreisgaben ist hingegen ein grundrechtliches Kraut nicht gewachsen.

---

[91] Zur rechtsstaatlichen Sicherungsfunktion von Verfahren: BVerfGE 60, 253, 295 ff.; grundlegend zur verfahrensmäßigen Absicherung der Grundrechte: BVerfGE 53, 30 ff.; Hesse, EuGRZ 1978, 427, 434 ff.

[92] BVerfGE 110, 33, 67 f.; BVerfG NJW 2005, 2603, 2609; zum Verhältnis materieller und verfahrensrechtlicher legislativer Steuerung s.a. Alexy (Fn. 74), S. 445 f.

Von der Volkszählung zum implantierten Chip? - Zur Entwicklung der Privatheit im Recht

Ivo Geis

Der Trend zum so genannten "Ubiquitous Computing" (übersetzt: allgegenwärtige Datenverarbeitung), hat Konsequenzen für die traditionelle Datenschutzsystematik (I.). Die Grenze zwischen öffentlichem und nicht-öffentlichem Bereich, eine grundlegende Unterscheidung des Datenschutzrechts, wird durch die Telekommunikation, den Datenaustausch durch Telefonieren und E-Mail-Kommunikation im Festnetz und Mobilfunknetz, aufgehoben (II.). Die Möglichkeiten datenschutzrechtlicher Kontrolle drohen durch vernetzte Chip-Systeme verloren zu gehen (III.). Die Effektivität des Datenschutzes ist damit unter den neuen Vorzeichen der Kommunikation, der Vernetzung in internationalen Systemen, in Frage gestellt. In diesem Bedrohungspotential ist eine Besinnung auf rechtliche Schutzmöglichkeiten notwendig, über die internationales Verständnis besteht (IV.).

I. Trend zur allgegenwärtigen Datenverarbeitung

Der Blackberry-Effekt kennzeichnet den Trend zum Ubiquitous Computing: Ein Taschencomputer, der automatisch alle eingehenden E-Mails anzeigt. Wenn Blackberry-Kundinnen und Kunden eine neue E-Mail erhalten, werden die Daten zunächst von deren Firmencomputer an einen Blackberry-Server weitergeleitet. Dort werden die E-Mails an die Mobilfunkunternehmen in den einzelnen Ländern verteilt, die sie schließlich auf dem Display der Endgeräte anzeigen. Der Blackberry ist permanent mit dem E-Mail-Postfach seiner Nutzerinnen oder seines Nutzers verbunden, erhält die Nachricht automatisch (Push-Service) und erlaubt so die Bearbeitung der eingehenden E-Mails von unterwegs über das Mobilfunk-

netz.[93] Microsoft greift Blackberry mit dem Betriebssystem für Mobilfunknetze "Windows Mobile" direkt an: Die Daten werden auf dem Server von Microsoft gespeichert und von dort auf die international rund 130 Millionen E-Mail-Postfächer mit der Exchange Software verteilt. In das Windows-Mobile-Paket wird die Internet-Telephonie (Voice over IP - VoIP) integriert, die über drahtlose Funknetze (Wireless Local Area Network - WLAN) auf einen Breitbandanschluss zugreift und sich laufend mit dem E-Mail-Postfach, dem Terminkalender und der Adressbank synchronisiert.[94] Durch diesen Eintritt von Microsoft in den Markt der dezentralisierten Fernsprech- und E-Mail-Kommunikation wird der Trend zur allgegenwärtigen Datenverarbeitung verstärkt und beschleunigt. Technische Grundlage für diese Entwicklung sind die Telekommunikationsnetze.

II. Aufhebung von öffentlichem und nicht-öffentlichem Bereich

Mit wachsender E-Mail-Kommunikation gewinnt der Datenschutz durch das Telekommunikationsgesetz an Bedeutung (1.). Geschützt werden Bestandsdaten (2.) und Verkehrsdaten (3.). Sicherheitsbehörden können auf die von den Telekommunikationsdiensten gespeicherten Daten zugreifen. Dadurch verschwimmen die Grenzen zwischen öffentlichem und nicht-öffentlichem Bereich (4.).

1. Datenschutz durch das Telekommunikationsgesetz

Das neue Telekommunikationsgesetz (TKG) vom 22.06.2004[95] ist ein neuer Rechtsrahmen für Diensteanbieterinnen und -anbieter von Telekommunikation (TK). Der Kreis der Anbieterinnen und Anbieter ist weit gezogen: Solche, die die Nutzung der TK-Dienste durch die Öffentlichkeit ermöglichen und solche, die die Nutzung durch definierte Nutzergruppen ermöglichen. Auf Grund der "Europäischen Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kom-

---

[93] Süddeutsche Zeitung (SZ) vom 07.10.2005, S. 11, Spion in der Tasche.

[94] Frankfurter Allgemeine Zeitung (FAZ) vom 08.10.2005, S. 20, Microsoft greift Blackberry frontal an.

[95] BGBl. I, Nr. 29, S. 1190 ff.,
abrufbar unter bmwa.bund.de/Service/Gesetze .

munikation"[96] ist ein neues Datenschutzrecht für TK-Dienste entstanden. Die Datenschutzvorschriften des TKG gelten auch für die Übermittlung von elektronischer Post (E-Mail).[97] Dies soll durch ein Telemediengesetz (TMG) klargestellt werden, das als Arbeitsentwurf zur Anhörung der beteiligten Kreise vorliegt.[98]

2. Bestandsdaten und der Zugriff der Sicherheitsbehörden

2.1 Bestandsdaten

Die Datenverarbeitung der Bestandsdaten ist an den Zweck des TK-Dienstevertrages gebunden. Nach § 95 Abs. 1 Satz 1 TKG dürfen die Bestandsdaten der Teilnehmerinnen und Teilnehmer nur für die in § 3 Nr. 3 TKG genannten Zwecke erhoben und verwendet werden: Für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste. Endet das Vertragsverhältnis, sind die Bestandsdaten von den Diensteanbieterinnen und -anbietern mit Ablauf des Kalenderjahres zu löschen, das auf die Beendigung des Vertrages folgt, § 95 Abs. 3 TKG. Damit bilden die Bestandsdaten für die Dauer des TK-Dienstevertrages einen Datenspeicher mit Informationen über die Teilnehmerinnen und Teilnehmer. Über diese Daten sind die Diensteanbieterinnen und -anbieter gegenüber den Sicherheitsbehörden zur Auskunft verpflichtet.

2.2 Auskunftspflichten gegenüber Sicherheitsbehörden

Die Auskunftspflichten der Diensteanbieterinnen und -anbieter gegenüber den Sicherheitsbehörden sind neu gefasst. Sie sind für geschäftsmäßige und öffentliche Diensteanbieterinnen und -anbieter unterschiedlich geregelt: Geschäftsmäßige haben Rufnummer, Name, Anschrift, Datum des Vertragsbeginns und Geburtsdatum der Rufnummerninhaberinnen und -inhaber und bei Festnetzanschlüssen auch die Anschrift des Anschlusses zu speichern, § 111 Abs. 1 Satz 1 TKG. Über diese Daten müssen die

---

96 Richtlinie 2002/58/EG, ABl. EG Nr. L 201, S. 37 ff.

97 So BT-Drucksache 15/4725, Antwort der Bundesregierung auf die große Anfrage: Überprüfung der personengebundenen datenschutzrechtlichen Bestimmungen.

98 Elektronischer Geschäftsverkehr-Vereinheitlichungsgesetz (ElGVG), BMWA - VII B 2.

Diensteanbieter im "manuellen Verfahren" den Sicherheitsbehörden im Einzelfall Auskunft erteilen, § 113 Abs. 1 Satz 1 TKG. Hierzu gehören auch Daten, die wie PIN (Personal Identification Number) und PUK (Personal Unblocking Key) den Zugriff auf Endgeräte ermöglichen, § 113 Abs. 1 Satz 2 TKG. Als Bestandsdatum, über das Auskunft zu geben ist, werden nach der Rechtsprechung auch statische sowie dynamische IP (Internet Protokoll) -Adressen und die Telefonnummer verstanden.[99] Über Daten, die dem Fernmeldegeheimnis unterliegen, kann nur Auskunft erteilt werden, wenn dies gesetzlich vorgesehen ist, § 113 Abs. 1 Satz 3 TKG. Über die Auskünfte ist gegenüber den Kundinnen und Kunden sowie gegenüber Dritten Stillschweigen zu wahren, § 113 Abs. 1 Satz 4 TKG. Anbieterinnen und Anbieter von Telekommunikationsdiensten für die Öffentlichkeit sind verpflichtet, die nach § 111 Abs. 1 Sätze 1 und 3 und Abs. 2 TKG erhobenen Daten unverzüglich in Kundendateien zu speichern und diese im "automatisierten Verfahren" für Gerichte und Sicherheitsbehörden verfügbar zu halten, § 112 Abs. 2 TKG.

3. Verkehrsdaten und Vorratsdatenspeicherung

3.1 Verkehrsdaten

Verkehrsdaten können im Rahmen des § 96 Abs. 1 TKG gespeichert werden. Hierzu zählen die Rufnummer der Anruferin oder des Anrufers, die Rufnummer des angerufenen Anschlusses, Datum, Uhrzeit, und Dauer der Verbindung sowie die Art der von der Teilnehmerin oder des Teilnehmers in Anspruch genommenen TK-Dienste. Die gespeicherten Verkehrsdaten dürfen nach § 96 Abs. 2 Satz 1 TKG über das Ende der Verbindung hinaus nur verwendet werden, soweit sie zum Aufbau weiterer Verbindungen oder für die in den §§ 97, 99, 100 und 101 TKG genannten Zwecke erforderlich sind. Damit sind die Entgeltermittlung nach § 97 TKG, der Einzelverbindungsnachweis nach § 99 TKG, die Störungen von Telekommunikationsanlagen und der Missbrauch von Telekommunikationsdiensten nach § 100 TKG und das Mitteilen ankommender Verbindungen nach § 101 TKG erfasst. In allen anderen Fällen sind die Verkehrsdaten nach § 96 Abs. 2 Satz 2 TKG nach Beendigung der Verbindung unverzüglich, das heißt ohne schuldhaftes Zögern, zu löschen. Teilnehmerbezogene Verkehrsdaten dürfen nach § 96

[99] LG Stuttgart, Beschluss vom 04.01.2005, Computer und Recht (CR) 2005, 598 ff.

Abs. 3 TKG zur Vermarktung von TK-Diensten, zu deren bedarfsgerechter Gestaltung und zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Zeitraum verwendet werden. In jedem Fall muss die Einwilligung der Teilnehmerinnen und Teilnehmer vorliegen. Verkehrsdatenspeicherung ist damit aus der Perspektive des Datenschutzes so angelegt, dass die Daten unmittelbar nach Ende des TK-Vorgangs gelöscht werden. Dies läuft den Interessen der Sicherheitsbehörden entgegen, sich über die Bewegung der Nutzerinnen und Nutzer zur präventiven Verbrechensbekämpfung informieren zu können. Sicherheitsbehörden sind deshalb an einer Speicherung der Verkehrsdaten interessiert.

3.2 Vorratsdatenspeicherung für die Sicherheitsbehörden

In der Diskussion um das neue TKG artikulierten die Sicherheitsbehörden ihr Interesse an einer Speicherung der Verkehrsdaten und der Möglichkeit, auf die Daten zugreifen zu können. Eine solche gesetzliche Regelung ermöglicht die "Europäische Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation"[100] mit Art. 15 Abs. 2. Hierfür fand sich bisher im Bundestag keine Mehrheit.[101] Aktuell zeichnet sich im Hinblick auf ein Rechtsinstrument in Europa (EU) zur Speicherung von TK-Verkehrsdaten zur Strafverfolgung und Terrorismusbekämpfung ein Konflikt zwischen der EU-Kommission und dem Ministerrat ab. In der Folge der Terroranschläge in Madrid hatten Frankreich, Irland, Großbritannien und Schweden bereits im März 2004 einen Entwurf für einen EU-Rahmenbeschluss zur erweiterten Verkehrsdatenspeicherung auf Vorrat vorgelegt. Danach sollen alle Anbieterinnen und Anbieter von TK- und Internetdiensten zur pauschalen Speicherung sämtlicher Daten über die Nutzerinnen und Nutzer dieser Dienste für einen Zeitraum von einem bis zu drei Jahren verpflichtet werden können.[102] Diesem Entwurf hat die Generaldirektion "Justiz, Freiheit und Sicherheit" der EU-Kommission einen eigenen Entwurf für eine Richtlinie über die Vorratsdatenspeicherung von Verkehrsdaten entgegengesetzt. Dieser Entwurf sieht vor, Verkehrsdaten

---

[100] Richtlinie 2002/58/EG, ABl. EG Nr. L 201, S. 37 ff.

[101] Hierzu Ohlenburg, Der neue Telekommunikationsdatenschutz, MultiMedia und Recht (MMR) 2004, 431, 434.

[102] Rossnagel/Scheuer, Das europäische Medienrecht, MMR 2005, 271, 276 f.; Breyer, EU-Pläne zur systematischen Vorratsspeicherung von Kommunikationsdaten, MMR 2005, 69 f.

über Nachrichtenübermittlungen im Fest- und Mobilfunknetz für ein Jahr und Internet-Verkehrsdaten für sechs Monate auf Vorrat zu speichern. Welcher Vorschlag sich durchsetzen wird, ist noch nicht klar.[103] Der Bundesbeauftragte für den Datenschutz lehnt diese Entwicklung ab und warnt davor, die Speicherung von Verkehrsdaten auszudehnen.[104]

4. Ergebnis: Symbiose von TK-Diensten und Sicherheitsbehörden

TK-Dienste und Sicherheitsbehörden leben in einer erzwungenen Symbiose. Die Unterscheidung zwischen öffentlichem und nichtöffentlichem Datenschutz ist dadurch relativiert. Sicherheitsbehörden können unter den rechtlichen Anforderungen der §§ 111-113 TKG auf Bestandsdaten zugreifen, die TK-Dienste gespeichert haben. Die politische Diskussion um die Speicherung der Verkehrsdaten und den Zugriff der Sicherheitsbehörden ist noch nicht abgeschlossen.

III. Verlust der Kontrolle in vernetzten Systemen

Die Chiptechnologie ermöglicht faszinierende Techniken, Daten zu erheben und in vernetzten Systemen zu kombinieren und zu übermitteln (1.). Rechtlicher Schutz soll durch das Prinzip der Transparenz erreicht werden (2.).

1. RFID-Tags und Implantate

"Radio Frequency Identification" (RFID) dient dem kontaktlosen Speichern und Auslesen von Daten. Die Daten werden auf einem sogenannten "RFID-Tag" gespeichert, einem Mikrochip, der überall befestigt werden kann. Diese Systeme sollen die üblichen Barcodes ablösen. Barcodes sind zwar maschinenlesbar, benötigen aber eine Sichtverbindung. RFID-Tags können dagegen Distanzen von bis zu 30 Metern überbrücken. Ein Barcode identifiziert ein Objekt als zu einer bestimmten Kategorie gehörend. RFID-Tags können jedes

[103] MMR 2005, Heft 10, XVIII, EU: Kommisions-Richtlinie zur Verbindungsdatenspeicherung?.

[104] MMR 2005, Heft 10, XIX, BfD: Keine Vorratsdatenspeicherung für TK- und Internetdienste.

Objekt mit einer eindeutigen Kennung versehen, durch die sich Informationen zu diesem Gegenstand mit einer Datenbank abgleichen lassen. Hierdurch entstehen zahlreiche Anwendungsmöglichkeiten, so für die Lagerverwaltung, für Zugangskontrollen, für Wegfahrsperren, für die Tierkennzeichnung oder Mautsysteme. In Verbindung mit Informationen aus anderen Datenbanken können Einkaufs- und Nutzungsprofile personalisiert werden.[105] Dieses Datenerhebungs- und Datenübermittlungssystem der RFID-Tags wird perfektioniert. "Smart Dusts" sind Chips, die sich miteinander vernetzen, ihre Umgebung überwachen und die dabei anfallenden Daten an eine Basisstation übersenden. "Ambient Intelligent Landscape" ist eine Welt, in der Gegenstände miteinander kommunizieren und auf die Anwesenheit von bestimmten Personen mit spezifischen Verhaltensweisen reagieren. Funkchips werden in Alltagsgegenstände integriert, etwa in Medikamente implantiert.

2. Rechtlicher Schutz

RFID-Tags ermöglichen die versteckte Datenerhebung und übermitteln die Daten. Hierauf können die davon Betroffenen nicht Einfluss nehmen. Rechtlicher Schutz soll durch das Prinzip der Transparenz gewährt werden. Dies ist ein internationales datenschutzrechtliches Verständnis mit unterschiedlicher Ausprägung. Nach deutschem Recht gelten RFID-Funktionen als "mobile personenbezogene Speicher- und Verarbeitungsmedien" im Sinne von § 6c BDSG, wenn die gespeicherten Daten ohne Beeinflussung durch die Betroffenen übermittelt werden.[106] Damit muss die Stelle, die den RFID-Tag ausgibt, die Betroffenen über ihre Identität und darüber unterrichten, wie sie ihre Rechte auf Auskunft, Berichtigung, Löschung und Sperrung wahrnehmen können.[107] Die Internationale Konferenz der Datenschutzbeauftragten hielt 2003 in einer Resolution fest, dass personenbezogene Daten aus RFID-Tags nur in einer offenen und transparenten Weise erhoben werden dürfen, um einen ungerechtfertigten Eingriff in die Privatsphäre zu verhindern. Das US-amerikanische "Auto-ID Center" des MIT (Massachusetts Institute of Technology) verlangt ein Unterrichtungsrecht darüber, ob ein Produkt ein EPC-Tag (Electronic Product Code Tag) enthält ("right to know whether a product contains an EPC-Tag").

---

[105] Hierzu Westerholt v./Döring, Datenschutzrechtliche Aspekte der Radio Frequency Identification, CR 2004, 710, 711-713.

[106] Gola/Schomerus, BDSG, 8. Auflage, 2005, § 6c Rz. 2.

[107] Hierzu Bizer, in: Simitis u.a., BDSG, 5. Auflage, 2003, § 6c Rz. 50 f.

Nach dem Kalifornischen Gesetz zum Konsumentenschutz können personenbezogene Daten, die anhand von RFID-Tags ermittelt werden, nur nach schriftlicher Einwilligung der Betroffenen auf dem RFID-Tag oder bei den Händlerinnen und Händlern gespeichert werden.[108]

IV. Das Recht auf Information - ein Lösungsvorschlag

Ubiquitous Computing, in seinen Facetten von mobiler Telekommunikation bis zu Chip-Implantaten, zeigt die Grenzen des traditionellen Datenschutzrechts auf (1.). Für den Rechtsschutz ist das entscheidende Problem die nationale Beschränktheit der Gesetze. Dies entspricht nicht der international vernetzten Datenverarbeitung im Ubiquitous Computing. Deshalb wird eine Lösung gesucht, deren Grundlage ein international entwickeltes Rechtsverständnis ist (2.).

1. Konsequenzen für das traditionelle Datenschutzrecht

In einer Welt mobiler und allgegenwärtiger Datenverarbeitung wirkt das Schutzprogramm des Bundesdatenschutzgesetz (BDSG) nicht mehr funktionsfähig. Die Wirksamkeit grundlegender Rechtsinstitute muss in Frage gestellt werden.[109]

- Die Einwilligung für jeden Akt der Erhebung, Verarbeitung und Nutzung überfordert die Beteiligten.

- Das Ziel der Zweckbindung und Erforderlichkeit, die Datenverarbeitung zu begrenzen, steht im Konflikt mit dem Ziel von Ubiquitous Computing, den Nutzerinnen und Nutzern unbemerkt, spontan und umfassend zu unterstützen.

- Mitwirkungs- und Korrekturrecht der Betroffenen werden wegen der Komplexität der Datenverarbeitung an Durchsetzungsfähigkeit verlieren.

---

[108] vgl. unter www.datenschutz.de: Kalifornischer Gesetzesentwurf zum Schutz der Verbraucher vor RFID im Einzelhandel.

[109] Rossnagel, Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MMR 2005, 71, 72.

- Die Vielzahl der Beteiligten führt zu einer Diffusion der Verantwortlichkeit für die datenverarbeitenden Vorgänge.

2. Kernbereich privater Lebensgestaltung und Right to Privacy

Die aktuelle Rechtsprechung des Bundesverfassungsgerichts weist den Weg zu einer Lösung: Durch die Urteile des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung vom 03.03.2004[110] und vom 27.07.2005[111] zu dem Gesetz des Landes Niedersachsen zur präventiven Verbrechensbekämpfung durch Datenspeicherung ist der "Kernbereich privater Lebensgestaltung" entwickelt worden. Die nach Art. 1 Abs. 1 GG garantierte Unantastbarkeit der Menschenwürde fordert, auch im Gewährleistungsbereich des Art. 10 Abs. 1 GG Vorkehrungen zum Schutz individueller Entfaltung im Kernbereich privater Lebensgestaltung zu treffen.[112] Diese kann durch die Erhebung und Weitergabe von Informationen aus diesem Bereich beeinträchtigt werden. In den "Kernbereich privater Lebensgestaltung" sollte deshalb auch das Recht einbezogen werden, über die Erhebung und Verarbeitung der Daten im Ubiquitous Computing informiert zu sein. Die Lösung für den Datenschutz im internationalen Ubiquitous Computing liegt nicht in nationalen Gesetzen oder in einem nationalen Rechtsverständnis, sondern in der Entwicklung eines internationalen Rechtsverständnisses für ein Recht auf Information. In der internationalen Vernetzung des allgegenwärtigen Computing ist die Orientierung und Akzeptanz durch das US-Recht entscheidend, um Rechte durchsetzen zu können. Das in der amerikanischen Rechtskultur[113] und in der Rechtsprechung des Supreme Court verankerte "Right of Privacy",[114] abgeleitet aus der Bill of Rights,[115] ist eine Grundlage, aus der ein Recht auf Information über die Datenverarbeitung abgeleitet werden kann. Das Recht auf Information hat damit eine

---

110 BVerfG, Urteil vom 03.03.2004, NJW 2004, 999 ff.
111 BVerfG, Urteil vom 27.07.2005, NJW 2005, 2603 ff.
112 BVerfG, Urteil vom 27.07.2005, NJW 2005, 2603, 2612.
113 Grundlegend: Warren/Brandeis, The Right to Privacy, Harvard Law Review 1890, S. 193 ff.; hierzu: Büllesbach/Garstka, Meilensteine auf dem Weg zu einer datenschutzgerechten Gesellschaft, CR 2005, 720, 721.
114 O`Brien, Constitutional Law and Politics, Volume two, Civil Rights and Civil Liberties, fifth edition, 2003, WW Norton, N.Y., S. 1211 mit Verweis auf die Grundsatzentscheidung Griswold v. Connecticut, S. 335 - 343.
115 O`Brien (Fn. 22), S. 1211.

internationale Grundlage. Datenschutz in der modernen Datenverarbeitung des Ubiquitous Computing hängt von der dogmatischen Aufarbeitung und Entwicklung dieses Rechts auf Information in seinem internationalen Verständnis ab.

Sicherheitsillusion auf Kosten der Freiheit

Wolfgang Hetzer

Sehr geehrte Frau Sokol, meine sehr verehrten Damen und Herren, ich bedanke mich für die Einladung. Sie ist nicht nur ehrenvoll, sondern auch *herausfordernd.* Bei der Würdigung mancher Vorstellungen des Gesetzgebers zur Abwehr terroristischer Bedrohungen und anderer Ideen zum Umgang mit potentiellen und tatsächlichen Gefährdungen fällt die Einhaltung des Zurückhaltungsgebotes nämlich nicht immer leicht.

In einem zu Beginn des Jahres 2005 veröffentlichten Pressekommentar finden Sie die Bemerkung, dass Teile der gegenwärtigen Rechts- und Innenpolitik vielleicht nur noch unter Einbeziehung von Hilfswissenschaften (zum Beispiel Psychologie, Psychiatrie) verstehbar sind. Im Zusammenhang mit der Debatte über die DNS-Analyse hat ein Kritiker immerhin *"Hysterie"* ausgemacht und das Bundesverfassungsgericht als die *"Nervenheilanstalt der Republik"* anerkannt, weil man dort politische Psychosen verarzte und die Aufgeregtheiten des Regierungsbetriebes abkühle. [116]

Die Einladung ist also (auch) deshalb herausfordernd, weil die vorgegebene Thematik ohne die Heranziehung von Hilfswissenschaften nicht angemessen zu erörtern ist. Als erste Annäherung schlage ich drei Fragen vor:

I. Große Oper oder Voodoo - Zauber?

Wie haben mindestens einen klaren Befund: Es gibt ein neues "Zauberwort": *Terrorismus*. Zumindest in der Politik der inneren

[116] Prantl, Süddeutsche Zeitung (SZ) Nr. 17 vom 22./23.01.2005, S. 5.

Sicherheit scheint sich der Begriff zum funktionellen Äquivalent eines *"Sesam öffne dich"* entwickelt zu haben. Vielleicht erübrigt sich deshalb sogar eine Debatte über die Frage, ob das Zeitalter des sicherheitspolitischen "Voodoo" angebrochen ist oder ob sich Sicherheitspolitik nur als "Große Oper" darstellt. Wie dem auch sei: Alleine der Hinweis auf die Notwendigkeit einer möglichst frühzeitigen und damit angeblich besonders wirkungsvollen Bekämpfung terroristischer Attentäter öffnet immer mehr Türen. Es wird aber immer unklarer, *wohin* sie führen. Hier und da entsteht der Eindruck, dass sogar schon an einem *Konzept der Schleusenöffnung* gearbeitet wird. Hinter einigen der schon geöffneten Türen mögen sich zwar *einzelne* rechtsstaatliche Wege zu einer verbesserten Erkennung und Abwehr terroristischer Bedrohungen abzeichnen. Andere Türen könnten aber aus dem gegenwärtigen Kreis der verfassungsrechtlichen Grundlagen und spezialgesetzlichen Regelungen herausführen.

Die Anschläge in den USA (2001), in Madrid (2004) und in London (2005) sowie eine weitere Vielzahl terroristisch motivierter Massenmorde machen es nachvollziehbar, dass man Wege gehen möchte, die - sicherheitspolitisch - in der *besten aller Welten* enden. Man scheint sich jedoch nicht mehr überall daran zu erinnern, dass der präventive und repressive Umgang mit der Gefahr und dem Verdacht strafbaren Handelns unvermeidlich mit dem Eingriff in die Freiheitsrechte von Personen verbunden ist, die bis zu einer rechtskräftigen Verurteilung als unschuldig gelten (Art. 6 Abs. 2 Konvention zum Schutz der Menschenrechte und Grundfreiheiten - EMRK). *Gleichzeitig* sollen Verhinderung und Verminderung von Kriminalität gerade dem Schutz dieser Individualrechte dienen. Wir haben also ein (*ungelöstes*) Optimierungsproblem.

Die Entwicklung von staatlichen Eingriffsbefugnissen zur Kriminalitätsbekämpfung scheint immer stärker durch eine Betonung der staatlichen Macht zu Lasten von Individualgrundrechten bestimmt zu werden. Dazu haben auch die Vorschriften moderner Polizeigesetze über "Vorfeldermittlungen" beigetragen. Es ist nicht mehr auszuschließen, dass man die überkommenen Eingriffsschwellen präventiven und repressiven staatlichen Handelns (Polizeigefahr/ Straftatverdacht) zugunsten einer schrankenfreien Ermittlungsbefugnis *noch weiter* hinter sich lassen wird. Nach den Anschlägen vom 11. September 2001 wird deshalb eine *neue Rechtsstaatsdebatte* gefordert, zumal kein einziges Teilgesetz der Antiterrorismusgesetzgebung in der Bundesrepublik Deutschland die Anschläge dieses Tages hätte verhindern können. Den Sicherheitsgesetzen

wird weniger eine praktische als eine ideologische Bedeutung für die Politik zugeschrieben: Die Kaschierung des Staates im Hinblick auf seine soziale Verantwortlichkeit.

Der Diskurs über die Bedrohung der westlichen Wertegemeinschaft durch terroristische Anschläge hat fast eschatologische Züge angenommen. Das ist angesichts der in der amerikanischen Außen- und Sicherheitspolitik etablierten Unterscheidung zwischen "Gut" und "Böse" nicht allzu verwunderlich. Dort hat man eine (zunächst) besonders wirkungsvolle Strategie der Prävention entwickelt, zu der vorbeugende Schläge (*"preemptive strikes"*) der amerikanischen Streitkräfte gehören. In den USA scheint man die Überzeugung gewonnen zu haben, dass das jüngste Gericht mit seinem eigenartigen Sitzungsrhythmus nicht mehr alle irdischen Bedürfnisse nach Gerechtigkeit rechtzeitig befriedigt.

Der Präsident der USA hat die Welt in seiner zweiten Inaugurationsrede wissen lassen, dass sein Land eine *"Berufung von jenseits der Sterne"* erhalten habe. Es ist also nur konsequent, dass sich George W. Bush auf den Weg des Herrn gemacht hat. Sein ehemaliger Außenminister, Colin Powell, hat dagegen Anfang September 2005 der Weltöffentlichkeit erklärt, dass die Präsentation unbewiesener Behauptungen zur Rechtfertigung des Angriffs auf den Irak vor dem Sicherheitsrat der Vereinten Nationen ein "Schandfleck" in seiner Karriere ist, der ihn immer noch schmerzt.

Der Sicherheitsdiskurs hat sich seit dem 11. September 2001 auch in der Bundesrepublik Deutschland fundamental verändert. Die Abwehr terroristischer Anschläge ist *Leitmotiv* der Innen- und Außenpolitik geworden. Für das *"ewige Thema"* der Zuordnung von Freiheit und Sicherheit gelten neue Vorzeichen.

Spätestens mit der Erkenntnis der Begrenztheit der Rechte des Staates gegenüber seinen Bürgern war das Dilemma zwischen Freiheit und Sicherheit entstanden. Die Prinzipien der Ungewissheit und der Unschuldsvermutung begründen ein *Paradoxon*: Die Herstellung von Sicherheit als Voraussetzung von Freiheit ist untrennbar mit der Reduktion von Freiheit und damit der Sicherheit Einzelner verbunden. Dies erfordert den ständigen Ausgleich zwischen den Bedürfnissen der Strafverfolgung und dem Anspruch des Bürgers, vom Staat ungestört zu bleiben. Entsprechende Anstrengungen sind besonders wichtig, weil es in der Geschichte immer die reale oder vorgeschobene Sorge des Staates um die Sicherheit - also auch die Freiheit - seiner Bürger war, die zum Aufbau eines

mehr oder minder perfekten Kontrollsystems führte. Solche Entwicklungen wurden auch durch die mangelnde Unterscheidung zwischen der *Sicherheit durch den Staat* und der *Sicherheit vor dem Staat* begünstigt. Heute hat der Vorrang von Prävention und Bekämpfung einen Umfang und eine Qualität angenommen, dass es schwer fällt, noch von einem *Gleichgewicht* zwischen der Erhaltung des Individualrechtsschutzes und der Durchführung einer effizienten Verbrechenskontrolle zu sprechen. Es drängt sich die Frage auf, ob die Furcht vor dem internationalen Terrorismus so groß ist, dass man weitgehende Eingriffe in grundrechtlich geschützte Positionen nur noch auf der bloßen Behauptungsebene rechtspolitisch und parlamentarisch *"rechtfertigen"* muss.

Die Maßnahmen der amerikanischen Regierung zeigen, mit welcher Leichtigkeit zahlreiche Errungenschaften des modernen Grundrechtsschutzes aufgegeben werden. Die formellen und materiellen Grundrechte sind dort mit einer Art Notstandsgesetzgebung auf ein kaum noch erkennbares Minimum reduziert worden. Es reicht bereits die tatsächlich nicht belegte Annahme einer Gefährdung aus - also die Gefahr, dass eine Gefahr entstehen könnte - um den denkbar schärfsten Eingriff, nämlich einen völkerrechtswidrigen Angriffskrieg, vorzunehmen.

Der Aufruf zum *"Krieg gegen den Terrorismus"* führte zur totalen Entrechtung des Gegners. Es geht nicht mehr um die Klärung eines Verdachts zur Verfolgung begangener Straftaten oder die Bekämpfung von Verdächtigen, denen bis zur Verurteilung die prozessualen und nach der Verurteilung die materialen Menschenrechte zustehen. Es soll das schlechthin *"Böse"* bekämpft werden, welches so böse ist, dass man die einem Kriegsgegner zustehenden Rechte nicht mehr respektieren muss. *"Präventive Exekutionen"* des flüchtigen oder sich versteckenden Gegners sind in dieser politischen Theologie nur folgerichtig. Ebenso konsequent ist es darüber hinaus, Gefangene unter der Fiktion einer *"Exterritorialität"* rechtlos zu halten.

II. Gefahrenabwehr oder Risikomanagement?

Mit solchen fragmentarischen Hinweisen ist noch nicht die Frage beantwortet, ob man warten muss, bis die Gefahren, die sich bei einer *externen* Bedrohung der nationalen inneren Sicherheit zeigen, eine *interne* Verdichtung nach Maßgabe des polizeilichen Gefahrenbegriffs oder des strafrechtlichen Verdachts erreicht haben,

um (erst dann) tätig zu werden. Mit Blick auf die etablierte Praxis der proaktiven Ermittlungstätigkeit scheint die Antwort auf der Hand zu liegen. So überzeugend der Gedanke einer frühzeitigen Intervention zur Schadensverhinderung auf den ersten Blick ist, so sehr muss man sich jedoch vor naiven Verallgemeinerungen hüten.

Die Regeln für ein Risikomanagement wie sie angesichts legaler Gefährdungshandlungen gelten, sind nicht ohne weiteres auf das Polizei- und Strafverfahrensrecht übertragbar. Wollte man eine Migration entsprechender Regelungen in das Strafrecht zulassen, würde man zu berücksichtigen haben, dass damit ein moralisch-ethisches Unwerturteil verbunden ist. Dies setzt zumindest einen Verdacht personal zurechenbaren Unrechts voraus, der aber im Vorfeld präventiven Wirkens gerade nicht besteht. Die Schaffung von abstrakten Gefährdungsdelikten ist eine rechtsstaatlich dornige Variante. Rechtsgutsbeschreibungen und Bestimmtheitserfordernisse werden diffus. Durch materiellrechtlich vorgegebene Beweiserleichterungen geraten zudem prozessuale Garantien (nicht nur die Unschuldsvermutung) in Gefahr.

Noch wichtiger ist die Frage, ob wir in einer kriminalpolitischen Lage sind, die ein völlig neues Verständnis von deliktischer Realität verlangt. Dreh- und Angelpunkt der Debatte ist das Argument der besonders großen Gefahr, die insbesondere der neuzeitliche Terrorismus darstellt. Das Schadenspotential ist unbestreitbar hoch. Die terroristische Strategie zielt auf die Schlüsselsymbole und die Infrastruktur der entwickelten Welt. Die Anzahl der Ziele ist deshalb unbegrenzt. Zweifelhaft bleibt aber, ob dies exklusiv durch die neue Ruchlosigkeit und Verblendetheit der Täter zu erklären ist oder ob sich damit "nur" moderne Strukturen manifestieren, die sich unter den Oberbegriff *"Risikogesellschaft"* zusammenfassen lassen.

Die Polizei hat die Aufgabe, die allgemein oder im Einzelfall bestehenden Gefahren für die öffentliche Sicherheit und Ordnung abzuwehren. Dazu zählt auch die vorbeugende Tätigkeit, weil sie der wirkungsvollen Abwehr von Gefahren und der Verhütung von Straftaten dient. Das Verhüten, also das vorbeugende Bekämpfen von Straftaten, Ordnungswidrigkeiten und verfassungsfeindlichen Handlungen gehört zu den ursprünglichen Aufgaben der Polizei. Es ist Teil des allgemeinen Polizeirechts, für das die Länder die Gesetzgebungskompetenz besitzen, und ist nur insoweit ausgegliedert als das Strafverfahrensrecht reicht.

Die Vorsorge für die Verfolgung künftiger Straftaten (zum Beispiel § 1 Abs. 1 Polizeigesetz des Landes NRW - PolG NRW) kann im Rahmen der polizeirechtlichen Aufgabenweisung *landesrechtlich* geregelt werden, weil Maßnahmen der vorbeugenden Bekämpfung von Straftaten keine schuld- und rechtsfolgenrelevante Bedeutung für ein bestimmtes Strafverfahren haben und insbesondere eine antizipierte Strafverfolgung die Grenzen des § 152 Abs. 2 Strafprozessordnung (StPO) überschreitet, der für alle Ermittlungsmaßnahmen eine begangene Straftat voraussetzt.

Das Bundesverfassungsgericht hat zudem klargestellt, dass zum *"Strafrecht"* im Sinne des Art. 74 Abs. 1 Nr. 1 Grundgesetz (GG) - und damit zur Bundeskompetenz - nur *die* Regelungen gehören, die an Straftaten anknüpfen, *ausschließlich* für Straftäter gelten und ihre *sachliche* Rechtfertigung aus der Straftat beziehen. Einen derartigen Sachzusammenhang setzen Maßnahmen der vorbeugenden Straftatenbekämpfung gerade *nicht* voraus. Solche Maßnahmen können nicht nur gegenüber Straftätern, sondern auch gegenüber anderen Personen - insbesondere bloß Verdächtigen - ergriffen werden. Die Polizei kann personenbezogene Daten erheben, wenn dies zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. Dabei ist die Abwehr abstrakter, nicht konkreter Gefahren gemeint. Im Freistaat Bayern hat der Gesetzgeber mit seiner Entscheidung, dass auch die vorbeugende Bekämpfung von Straftaten zur Gefahrenabwehr gehört und damit in den Bereich des präventiven, nicht des repressiven Handelns der Polizei fällt, einen seit längerem ausgetragenen Streit entschieden.

Repressives polizeiliches Einschreiten ist immer mit einer präventiven Komponente verwoben. Das entsprechende Sammeln und Bereithalten einzelner Informationen wird in zunehmendem Maße Voraussetzung für eine wirksame Strafverfolgung. Polizeiliches Handeln geschieht also in einer *"Gemengelage"*. Die Polizei kann von öffentlichen und nichtöffentlichen Stellen die Übermittlung von personenbezogenen Daten bestimmter Personengruppen aus Dateien insbesondere Namen, Anschriften, Tag und Ort der Geburt und fahndungsspezifische Suchkriterien zum Zweck des Abgleichs mit anderen Datenbeständen verlangen, soweit dies zur Abwehr von Straftaten von erheblicher Bedeutung erforderlich ist ("Rasterfahndung"). Dabei muss sich die Gefahr als Grundlage der Maßnahme nicht innerhalb Bayerns oder der Bundesrepublik Deutschland verwirklichen. Vielmehr ist die Maßnahme auch dort durchführbar, wo die Grundlagen zu derartigen Straftaten gelegt wer-

den. Das folgt aus der umfassenden Aufgabe der Polizei zur Gefahrenabwehr, aus dem Weltrechtsprinzip (§ 6 Strafgesetzbuch - StGB) und auch aus der Verfassung (Art. 1 Abs. 2 GG). Eine gegenwärtige Gefahr wird in Bayern, anders als in anderen Bundesländern, nicht verlangt.

Ausreichend ist eine abstrakte Gefahr, auch wenn sie sich etwa mangels möglicher Anschlagsziele noch nicht weiter konkretisiert hat. Die Integration einer *"Dauergefahr"* sprengt jedoch *ohne Not* das von Konkretheit *und* Abstraktheit bestimmte Wesen des Gefahrenbegriffs. An die Wahrscheinlichkeit des Gefahreneintritts ist angesichts der Bedrohung elementarer Rechtsgüter und des Ausmaßes des zu erwartenden Schadens durch Straftaten von erheblicher Bedeutung ein großzügiger Maßstab anzulegen. Dies gilt insbesondere im Hinblick auf terroristische Anschläge. Zur Bekämpfung einfacher bis mittelschwerer Kriminalität bleibt die Rasterfahndung hingegen unzulässig.

III. Abgesang oder Ouvertüre?

Die Prüfung der Frage, ob man die für ein gesellschaftliches und politisches System insgesamt charakteristische Freiheit schützen kann, indem man wichtige Grundfreiheiten aller Staatsbürger schon im Vorfeld, also weitab eines konkreten Verdachts oder einer Gefahr beschränkt oder gar aufhebt, muss mit größter Sorgfalt erfolgen. Sie ist ohne Rücksicht auf die Profilierungsbedürfnisse der jeweils nur für eine *vorübergehende* Zeit verantwortlichen Amts- und Entscheidungsträger zu führen. Deren Erfolgsinteresse ist weder nach Zielrichtung noch nach Wirkungsdauer immer und zwangsläufig vollkommen identisch mit den Interessen einer unübersehbaren Vielzahl von Betroffenen, die mit den Eingriffen in ihre Grundrechte auch die *langfristig* wirksame und gefährliche Unterhöhlung ihrer freiheitlichen Verfassungsordnung zu ertragen haben. Die Aufrechterhaltung der diese Ordnung prägenden Machtbalance ist wichtiger als der Talmiglanz, den manch ein Akteur in der politischen Arena vielleicht in der Hoffnung verbreiten möchte, dass er als Zeichen für die ausschließliche Orientierung am Gemeinwohl missverstanden werden möge.

Die deutsche Sicherheitspolitik hat noch nicht den Übergang von der *"Brave New World"* (Huxley) zur Welt des *"Minority Report"* (Hollywood) eröffnet. Dort scheint der Preis auf, der für die Etablierung *totaler* Sicherheit zu zahlen wäre. Er liegt in der *totalen*

Kontrolle der Bürger einerseits und dem *Ausschluss* jeder Kontrolle des Staates andererseits.

Die Regeln des *"Minority Report"* sind einfach. Der Zugriff auf den *potentiellen* (!) Verbrecher erfolgt *vor* Begehung der Straftat. Eine unabhängige gerichtliche Überprüfung ist also überflüssig. Derjenige, der nichts getan hat, kann auch seine Unschuld nicht beweisen. Die Verhinderung des Verbrechens ist die (*nachträgliche*) Rechtfertigung für den (*vorherigen*) Zugriff des Staates.

Diese Regeln sind *zwar* (noch) nicht Teil der kriminalpolitischen Agenda in der Bundesrepublik Deutschland. Es wird *aber* behauptet, dass die Erfüllung der Forderungen zur Ausweitung der Befugnisse des Bundeskriminalamtes (BKA) die schärfsten Überwachungsgesetze in der Geschichte der Bundesrepublik Deutschland mit sich brächten. Anscheinend ist die Metamorphose des Magazins "Der Spiegel" vom "Sturmgeschütz der Demokratie" zur regierungsamtlichen Konfettikanone noch nicht *ganz* abgeschlossen. Immerhin haben vier seiner Redakteure ihrer Empfindung Ausdruck verliehen, dass dies der Anfang vom Ende des Föderalismus bei der inneren Sicherheit wäre. Im politischen System der Bundesrepublik Deutschland käme dies einer *"mittleren Revolution"* gleich.[117]

Hier sind die mehr oder minder feinen Unterschiede zwischen einem *"Staatsstreich"* und einer *"Revolution von oben"* nicht herauszuarbeiten. Die verfassungsrechtlich relevante Aufladung der zitierten Formulierung von Journalisten ist ohnehin begrenzt. Schon wegen der geschuldeten Loyalität gegenüber der freiheitlich-demokratischen Grundordnung verbietet sich hier auch ein Aufruf zur *"Revolution"* oder *"Gegen-Revolution"*. Die Teilnahme an derartigen Veranstaltungen kommt unter den gegenwärtigen Bedingungen erst recht nicht in Betracht.

Die rechtsanalytische und empirische Aufarbeitung und Überprüfung mancher sicherheitspolitischer Wunschvorstellungen ist - ebenso wie Ihre Einladung - herausfordernd genug. Angesichts der mit der Übertragung präventiver Befugnisse verbundenen Beeinträchtigungen verfassungsmäßig garantierter Freiheitsrechte mag immerhin der Gedanke an eine *"Gegen-Prävention"* aufkommen. Vielleicht lässt sich so verhindern, dass der Rechtsstaat Bun-

[117] Cziesche/Meyer/Stark/Ulrich, Der Spiegel Nr. 46 vom 08.11.2004, S. 34 ff.

desrepublik Deutschland zum Gegenstand nostalgischer Erinnerungen degeneriert.

Wollte man dem ehemaligen Bundesminister des Innern, Otto Schily, glauben, dann wäre der Terrorismus, dem wir uns gegenübersehen, eine "epochale Bedrohung". Attentate wie in Madrid und London sind in der Tat auch in Deutschland nicht auszuschließen. Gerade deshalb ist es in seinen Augen so wichtig, die Vorfeldaufklärung durch die Polizei nutzbar zu machen.[118] Das müsse auch dann geschehen, wenn es nicht um die Aufklärung einer schon geschehenen Straftat gehe, sondern um Vorbeugung. Wenn man dann jemanden "ins Visier" genommen habe, müsse man nach den Grundsätzen vorgehen, die die Polizei bei der Gefahrenabwehr anwende. Dort gelte- anders als im Strafverfahren - nicht der Grundsatz "Im Zweifel für den Angeklagten", sondern da sei "Sicherheit" der entscheidende Gesichtspunkt.[119]

Das sind im Hinblick auf das für einen Rechtsstaat konstitutive Prinzip der Gewaltenteilung und angesichts der Essenz justizförmiger Wahrheitsfindung inspirierende Überlegungen, auf die hier nicht angemessen einzugehen ist. In der öffentlichen Diskussion wird indes die viel interessantere Frage gestellt, was die Beschwörungsformeln, mit denen sich die europäischen Innenminister nach dem 11. März 2004 in die Hand versprachen, ihre Geheimdienste enger zusammenarbeiten zu lassen und was auch die guten Beziehungen nutzten, deren sich Innenminister Schily zum amerikanischen Heimatschutzminister rühmte, wenn an entscheidender Stelle die Politik der Justiz im Wege steht?

Einerseits wird behauptet, dass die Behandlung der Fälle Motassadeq und Mzoudi das Vertrauen in die Urteilsfähigkeit und Wirksamkeit unserer Justiz erschüttere. Andererseits betont man, dass es nicht die Kraft der Beweismittel und erst recht nicht die Blindheit der Justiz gewesen seien, die Motassadeq zunächst aus dem Gefängnis herausgebracht haben. Dem Hamburger Oberlandesgericht seien die Hände gebunden gewesen, weil die amerikanische und die deutsche Regierung ihm den Zeugen bin al Shibb vorenthalten

---

[118] Das Thema ist nicht ganz neu. Ausführlich: Hetzer, Der Kriminalist 2002, S. 14 ff.

[119] Vgl. insgesamt: Otto Schily, Frankfurter Allgemeine Sonntagszeitung (FAZ) Nr. 12 vom 21.03.2004, S. 7 (linke Spalte).

hätten. Nicht an der Justiz, sondern an einer Politik, die der Terrorabwehr solche Niederlagen beschert, müsse man zweifeln.[120]

Mittlerweile gibt es unterhaltsame Spekulationen darüber, wie sich Schily und der bayerische Innenminister Beckstein verhalten hätten, wenn sie als Cicero und Cato gelebt hätten und im alten Rom schon für Fragen der inneren Sicherheit zuständig gewesen wären. Sie hätten dann zum Zwecke der Terrorbekämpfung - so die Hypothese eines Kommentators - einen Senatsbeschluss zur Verteidigung des Staates gefasst. Damit wäre der innere Gegner benannt worden. Die jeweilige Person, und alle, die ihm halfen, wurden seinerzeit durch "senatus consultum ultimum" zu "Staatsfeinden" erklärt. Diese "Feinderklärung" ist nicht mit einem Urteil nach einem ordentlichen Gerichtsverfahren gleichzusetzen. Sie war viel schlimmer. Damit wurde die bürgerliche Existenz des Betroffenen beendet. Aus dem Bürger wurde ein rechtloser Feind. Der Feind galt als "Barbar" und wurde entsprechend (das heißt *"barbarisch"*) behandelt.

Ein Beobachter ist der Auffassung, dass der hinter der Feinderklärung stehende Gedanke die für die innere Sicherheit verantwortlichen Politiker angesteckt habe. Manche Fragen könnten dies verdeutlichen:

1. *Kann man, soll man mit fundamentalistischen "Gefahrpersonen" so verfahren, wie man mit normalen Straftätern verfährt?*
2. *Muss man, der außerordentlichen Gefahren wegen, hier nicht die geltenden Prinzipien des Rechtsstaates auf Eis legen oder gar umkehren - nicht im Zweifel für, sondern gegen den Angeklagten?*
3. *Muss man diese Personen wirklich ausstatten mit den Rechten, die der Rechtsstaat bereithält?*
4. *Sind islamistische Fundamentalisten eigentlich resozialisierbar?*

Solche Fragen hält Prantl für "minoisch". In der Kultur von Minos hatte man dem Ungeheuer Minotaurus alljährlich Kinder geopfert, um so vermeintlich Sicherheit zu gewinnen. Eine demokratische Kultur, die ihre Prinzipien dem Terrorismus opfert, handle nicht

[120] FAZ Nr. 84 vom 08.04.2004, S. 1 (rechte Spalte); über das "Netzwerk des Wirrwarrs" in der Terrorbekämpfung Europas: Klingst/Fritz-Vannahme, Die Zeit Nr. 14 vom 25.03.2002, S. 5.

anders. Sie arbeite den gewalttätigen Islamisten in die Hände. Die Überlegungen, ein Sonderstrafrecht, ein Feindstrafrecht zu etablieren, führten zurück in die Zeit vor der Aufklärung. Sie endeten mit der Abschaffung der Gleichheit vor dem Gesetz. Die Person werde zur Unperson, zum Feind, zum Kriegsgegner eines Krieges im Inland. Damit rechtfertige man "Guantánamo",[121] und gehe noch darüber hinaus.

Letztlich werde auf diese Weise, meint Prantl, der "Staatsrechtler und Nazi-Apologet" Carl Schmitt, der dem Staat das Kriegsrecht auch im Inneren und damit das Recht der Bestimmung des inneren Feindes eingeräumt habe, rehabilitiert. Derjenige, der ein Feindstrafrecht braucht, glaube nicht an die Überlegenheit des Rechtsstaates über den Fundamentalismus. Die Schlussfolgerung ist anspruchsvoll:

"Der Terrorist ist mein Feind. Aber der Rechtsstaat braucht kein Feindstrafrecht, sondern rechtsstaatliche Kraft und Phantasie. Ein starker Staat ist er dann, wenn er seine Prinzipien verteidigt." [122]

Die Diskussion über den Einsatz der Bundeswehr im Inneren, die Überlegungen mancher Politiker zum Verhältnis zwischen strafrechtlichen Ermittlungen und polizeilichen Maßnahmen der Gefahrenabwehr, die Anleihen bei der römischen Geschichte und die Hinweise auf eine angeblich nazistische Staatsräson zeigen, dass die Begriffe in Bewegung geraten sind. Irgendwann wird man sich vielleicht auch der Frage stellen müssen, welche Entwicklung beunruhigender ist: Die entsetzliche Gewalttätigkeit terroristisch motivierter Massenmörder oder eine Bekämpfungsstrategie, die rechtsstaatliche Kategorien auf den Abfallhaufen der Geschichte wirft, "Prävention" mit militärischen Mitteln betreibt und zudem die eigenen Protagonisten zu vorsätzlichen oder fahrlässigen Falschangaben zur "Begründung" völkerrechtswidriger Aggression verführt?

Sie mögen selbst entscheiden, ob die folgenden zehn Bemerkungen die Schlussakkorde eines Abgesangs auf den Rechtsstaat sind oder die Ouvertüre zu einer Debatte über die verfassungsrechtlichen Voraussetzungen und Grenzen des Rechtsgüterschutzes in einem freiheitlichen und demokratischen Gemeinwesen sein können.

---

[121] Über die Verhältnisse in dieser Einrichtung: Rüb, FAZ Nr. 85 vom 10.04.2004, S. 3.

[122] Prantl, SZ Nr. 73 vom 27./28.03.2004, S. 4.

1. Die bisherigen Reaktionen des Gesetzgebers auf die Anschläge vom 11. September 2001 waren in einem Klima angstvoller Konditionierung noch nicht im gebotenen Umfang Gegenstand einer kritischen Analyse.

2. Angesichts der anhaltenden weltweiten terroristischen Bedrohung werden auch in Deutschland weitere Vorschläge zur Ausweitung präventiv-polizeilicher Befugnisse diskutiert, deren Zweckmäßigkeit und Erforderlichkeit zweifelhaft sind.

3. Wegen der Furcht vor weiteren Anschlägen, war der Begründungsaufwand zur Durchsetzung weitgehender Freiheitsbeschränkungen bislang sehr gering. Eine neue Rechtsstaatsdebatte ist umso dringlicher.

4. Der internationale Terrorismus hat eine Entwicklung potenziert, die schon seit geraumer Zeit stattfindet: Ausweitung von Eingriffsbefugnissen unter Bevorzugung staatlicher Macht zu Lasten von Freiheitsrechten.

5. Sicherheitsstrategien zur polizeitaktischen Effizienzsteigerung führen zu einem abnehmenden Grenznutzen justiziellen Rechtsgüterschutzes: Vorfeldbefugnisse konterkarieren nicht nur die *repressive* Eingriffsschwelle des Verdachts. Die *präventionsrechtliche* Einbindung der Kategorie "Gefahr" wird zugunsten eines "Selbsteintrittsrechts" der Sicherheitsbehörden marginalisiert.

6. Eine unreflektierte Steigerung von Kontrollmacht verwandelt den Staatsdiener zum Störer gegenüber den Bürgern, ein Umstand der zusätzlichen Kontrollaufwand erforderlich macht.

7. Es ist eine Spiralentwicklung in Gang gekommen, die das Kontrollparadigma ad absurdum führt. Ansätze zur Machtkontrolle könnten eher Beiträge zur inneren Sicherheit leisten als rechtspolitische und militärische Trittbrettfahrerei auf dem "Expresszug" der Terrorismusbekämpfung.

8. Gesellschaftliche Angstzustände und politische Ambitionen erschweren die Einsicht in das Wesen einer möglichen Krise des Rechtsstaates: Die Orientierung auf "Vorsorge" macht das Recht letztlich irrelevant; Risikosicherheit überlagert zunehmend die Rechtssicherheit.

9. Die Rationalität der Prävention scheint konkurrenzlos. Bei der Befriedigung des Grundbedürfnisses nach Sicherheit sollte sich eine freiheitlich verfasste Gesellschaft dennoch nicht nur auf Amtsträger verlassen, die als galoppierende "weiße Ritter" die weiten Ebenen eines (nicht mehr ganz so) freien Landes in Besitz nehmen wollen.

10. Weitere *"Geländegewinne"* auf dem Feld der inneren Sicherheit sind nur bei drastisch steigenden Preisen möglich. Die entsprechenden Kosten fallen auf der Seite des Rechtsstaates an. Sie werden von all denjenigen getragen, die nichts anderes getan haben als ein rechtstreues Leben zu führen.

Informationelle Selbstbestimmung - ein zeitgemäßes Leitprinzip?

Für eine normative Konkretisierung informationsethischer Belange

Ralf Grötker

Die neuen Techniken der Kontrolle

"Befinden wir uns auf dem Weg in eine Überwachungsgesellschaft?" Was soll man auf eine solche Frage antworten! Natürlich trifft es zu, dass Techniken, die zusammenfassend als solche der Überwachung bezeichnet werden, immer ausgefeilter werden und immer größere Verbreitung finden und dass im Zuge der seit dem 11. September 2001 verabschiedeten Anti-Terror-Gesetze die Befugnisse von Polizei und Nachrichtendiensten ausgeweitet worden sind. Ein Beispiel für die neuen Techniken ist der RFID - Chip (*Radio Frequency Identifikation - Chip*).[123] Auf RFID-Chips können Informationen gespeichert und per Funk berührungslos abgelesen werden. Die Chips sind so klein, dass man sie kaum bemerkt, und zunehmend auch so billig, dass sie auf allen möglichen Konsumgütern angebracht werden können. Ähnlich wie mittels eines Barcodes, lassen sich so Produkte mit einer Nummer kennzeichnen. Anders als beim Bar- oder Strichcode, weist diese Nummer aber nicht nur auf eine Produktkategorie hin, sondern ermöglicht die eindeutige Bezeichnung des individuellen Gegenstandes. Wenn Sie also eine mit einem RFID-Chip ausgezeichnete Tüte Erdnussflips kaufen, die an der Kasse automatisch erkannt und der Rechnung hinzugefügt wird, wenn Sie zusätzlich beim Einkauf eine Kundenkarte

[123] Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI), Risiken und Chancen des Einsatzes von RFID-Systemen, BSI/SecuMedia, 2004, http://www.bsi.bund.de/fachthem/rfid/studie.htm .

verwenden und wenn Sie dann die leere Flipstüte auf der Wiese im Park liegen lassen, dann wäre es - technisch zumindest - durchaus möglich, dass man Sie als Verursacher dieser kleinen Verschmutzung dingfest macht.[124] Mautsysteme auf Fernstraßen sind ein tatsächliches Anwendungsfeld der RFID-Technik: Hier können Bewegungsprofile von Fahrzeugen erstellt werden. Im menschlichen Körper eingepflanzt, können RFID-Chips zum Zwecke der Identifizierung verwendet werden oder zur Standortbestimmung von Personen.[125]

RFID ist ein Beispiel unter vielen. Daneben kennen wir Videokameras in Einkaufszentren und im öffentlichen Raum,[126] nebst angeschlossener Software zum Erkennen von Personen oder verdächtigen Bewegungsprofilen, die vielfältigen Möglichkeiten, das Surfverhalten von Internet-Nutzern zu erfassen, die Überprüfung der persönlichen Daten von Fluggästen oder Maßnahmen zur weltweiten Kommunikationsüberwachung wie das amerikanische Spionagesystem Echelon.[127]

Unser Rechtssystem wird mehr und mehr ausgebaut, um die neuen Techniken bei der Verbrechensbekämpfung und der Terrorismusabwehr auch zum Einsatz zu bringen. Nach der neuen Telekommunikationsüberwachung werden Internet-Service-Anbieter und Telekommunikationsfirmen die Verbindungsdaten ihrer Kunden monatelang speichern müssen - für den Fall, dass die Daten

---

[124] Das Beispiel wurde leicht verändert übernommen von der Webseite der Kampagne des FoeBuD e.V. zum Thema RFID, http://www.foebud.org/rfid, siehe auch http://www.stoprfid.de/ .

[125] Rötzer, Mexikanische Strafverfolger an der elektronischen Leine, Telepolis vom 13.07.2004, http://www.telepolis.de/r4/artikel/17/17867/1.html .

[126] Vgl. die Sonderausgabe von Surveillance and Society, Vol. 2, Nr. 2/3 (2004), http://www.surveillance-and-society.org/cctv.htm . Zur Diskussion nach den Anschlägen auf die Londoner U-Bahn im Juni 2005 siehe z.B. Zurawski, Von Angsträumen und Terroristen, Telepolis vom 21.07.2005, http://www.telepolis.de/r4/artikel/20/20572/1.html .

[127] Vgl. generell zum Thema Überwachungstechniken, Ström, Die Überwachungsmafia. Das gute Geschäft mit unseren Daten, Carl Hanser Verlag, 2005.

für Ermittler interessant werden. Die Bestimmungen zur Speicherung des genetischen Fingerabdrucks wurden gelockert;[128] das Bankgeheimnis wurde teilweise aufgehoben. Und vieles mehr.

Suche nach der richtigen Metapher

Trotz all dem leben wir noch lange nicht in einer totalitären Welt, wie sie George Orwell in seinem Roman "1984" beschreibt, sondern in einem demokratischen Rechtsstaat - einem Rechtsstaat, in dem es zum Beispiel verboten ist, Selbstgespräche abzuhören und vor Gericht zu verwenden.[129] Aber nicht deshalb ist es so schwierig, die Frage "Befinden wir uns auf dem Weg in eine Überwachungsgesellschaft?" zufriedenstellend zu beantworten, weil sie dort polarisiert, wo Differenzierung und Abwägung gefordert wäre. Im Gegenteil: In einem gewissen Sinne ermöglichen uns Metaphern und Geschichten wie "1984" erst, dort allgemeine Züge zu erkennen, wo wir ansonsten lediglich unzusammenhängende Details wahrnehmen würden. Aus anderem Grund ist die Frage nach der "Überwachungsgesellschaft" so schwierig zu beantworten: Nicht, weil sie zu allgemein, sondern weil sie *schief* gestellt ist. Als Bedrohungsszenario fasst die "Überwachungsgesellschaft" den Ernstfall der Gefahr zu eng. Gleichzeitig legt sie die Hürde der Beweislast unnötig hoch: Bis wir uns in einer "Überwachungsgesellschaft" befinden, muss in der Tat einiges zusammenkommen.

Genau genommen, kann von "Überwachung" in vielen Fällen gar nicht die Rede sein. Zwar werden zahlreiche Informationen erhoben und ausgewertet. Meist aber sind es Maschinen, die diese Informationen verarbeiten. Und die Informationen sind relativ verstreut. Es gibt keine zentrale Instanz. Kein menschliches Bewusstsein, kein "Big Brother" hat Einblick in die Gesamtheit dessen, was hier gesammelt wird. Auch das Ziel eines Großteils der beschriebe-

---

[128] Die Neuerungen: Der Richtervorbehalt für eine genetische Untersuchung von Körperzellen entfällt, wenn eine Person freiwillig in die Untersuchung einwilligt. Auch bei Gefahr im Verzug bedarf es künftig keiner gerichtlichen Anordnung mehr. Die Speicherung von Gendaten für eine künftige Strafverfolgung soll nun auch bei Tätern möglich sein, die wiederholt nicht erhebliche Straftaten begehen. Bislang ist eine Speicherung nur bei erheblichen Straftaten und Sexualdelikten möglich. Nach: Süddeutsche Zeitung vom 09.06.2005, S. 6.

[129] Urteil des 1. Strafsenats des BGH vom 10.08.2005 - 1 StR 140/05 -.

nen Techniken ist nicht die Überwachung, sondern vielmehr, uns besser mit Produkten (und mit Werbung) zu versorgen.[130]

Auch mit Blick auf die Betroffenen selbst zeigt sich, dass der Tatbestand der Überwachung in den meisten Fällen nicht erfüllt ist. Denn Überwachung im eigentlichen Sinne geht mit Normierung einher. Benthams berühmtes Panoptikum - jener Gefängnisturm, dessen Architektur es dem Aufseher ermöglicht, alle Insassen zu beobachten, ohne dabei selbst gesehen zu werden - funktioniert nur, weil die Insassen die Überwachung internalisieren. Benthams Gefangene müssen jederzeit davon ausgehen, beobachtet zu werden. Und dementsprechend richten sie ihr Verhalten aus. Die moderne Form von "Überwachung", die zur Prävention von Verbrechen und Terrorismus eingesetzt wird, bedient sich jedoch gerade eines anderen Prinzips. Rasterfahndung und Screening von Flugpassagieren funktionieren nur, wenn die Muster, nach denen gesucht wird, geheim bleiben. Sind die Muster bekannt, ist es für die Betreffenden leicht, der Falle zu entgehen.[131]

Wie anders als mit Rückgriff auf den Begriff der Überwachung soll man die skizzierten Entwicklungen zusammenfassend bezeichnen? Kafkas "Prozess", nicht Orwells "1984", schreibt der amerikanische Jurist Daniel Solove, sei der geeignete Referenzrahmen. Im "Prozess" verfolgt die Macht kein spezifisches Ziel, die Zwecke bleiben im Dunkeln, es gibt keinen teuflischen Plan der Unterdrückung. Und trotzdem wird ein Gefühl der Machtlosigkeit erzeugt.[132]

---

[130] Zur Kritik an der Leitmetapher des "Panoptizismus" vgl. Simon, The Return of Panopticism, Supervision, Subjection and the New Surveillance, in: Surveillance and Society, Vol. 3, Nr. 1 (2005), http://www.surveillance-and-society.org/Articles3(1)/return.pdf .

[131] Chakrabarti/Strauss, Carnival Booth: An Algorithm for Defeating the Computer-Assisted Passenger Screening System, in: First Monday, Vol. 7, Nr. 10 (2002), http://firstmonday.org/issues/issue7_10/chakrabarti/index.html .

[132] Solove, Privacy and Power: Computer Databases and Metaphors for Information Privacy, in: 53 Stanford Law Review 1393 (2001), http://docs.law.gwu.edu/facweb/dsolove/Privacy-Power.pdf; vgl. ders., The Digital Person, in: New York University Press 2004, S. 40 - 41.

Informationelle Selbstbestimmung: Schutz vor mehr als Überwachung

Um dieses Gefühl der Machtlosigkeit zu thematisieren, können wir, zumindest in Deutschland und in Europa, auch auf etwas anderes zurückgreifen als das Metaphernkonglomerat von Kafkas "Prozess": Auf ein Prinzip, welches zugleich weiter gefasst und feiner gestaltet ist als der Komplex um den Begriff der Überwachung. Es handelt sich um das Prinzip der informationellen Selbstbestimmung. Feiner gestaltet ist dieses insofern, als es nicht nur Einschränkungen der individuellen Handlungs- und Entscheidungsfreiheit in den Blick nimmt, die durch Übergriffe in die Privatsphäre entstehen, sondern auch Verletzungen so genannter informationeller Privatheit. Informationelle Privatheit wird bereits dann beeinträchtigt, wenn der Einzelne nicht mehr kontrollieren kann, wer Zugang hat zu Informationen, die ihn betreffen. In dem Maße, wie wir diesen Zugang nicht mehr kontrollieren können, sind wir und fühlen uns beobachtbar. Wer aber willkürlich beobachtet werden kann, ist gewissermaßen nicht mehr Herr über sich selbst: Er vermag nicht mehr zu steuern, als wer er sich geben, wie er sich anderen präsentieren will. Und dies wiederum kann als wesentliche Einschränkung menschlicher Freiheit aufgefasst werden.[133]

Informationelle Privatheit, und mit ihr das Prinzip der informationellen Selbstbestimmung, unterscheidet sich damit wesentlich von anderen Leitgedanken zum Thema Privatheit. Informationelle Selbstbestimmung ist weder beschränkt auf den Bereich der Intimsphäre oder auf Daten, die einem besonderen Geheimhaltungsanspruch unterliegen. Informationelle Selbstbestimmung ist nicht gebunden an den Gedanken der Unverletzlichkeit der Wohnung. Informationelle Selbstbestimmung kann auch dann beeinträchtigt werden, wenn die betreffenden Informationen sich bereits in der Sphäre der Öffentlichkeit befinden: Etwa durch Videoüberwachung an öffentlichen Plätzen oder wenn Daten, die einen Vertragsabschluss betreffen, von einem der Vertragspartner ohne Wissen und gegen den Willen des anderen an Dritte weiter gegeben werden.

Es ist ein historischer Zufall, dass der Datenschutz in Deutschland und auch in anderen europäischen Ländern um das 1983 in einem Urteil des Bundesverfassungsgerichts formulierte Prinzip der informationellen Selbstbestimmung zentriert ist. Ein Zufall, dass bedeutet: Es hätte auch anders kommen können. Der Datenschutz

[133] Vgl. Rössler, Der Wert des Privaten, Suhrkamp Verlag, 2001.

zum Beispiel in den USA[134] kennt weder die zentrale Einrichtung einer Datenschutzbehörde, noch die informationelle Selbstbestimmung als leitendes Prinzip - sondern vielmehr eine Reihe von Bestimmungen auf unterschiedlichen gesetzlichen Ebenen, die von verschiedenen Prinzipien ausgehen wie eben der Unverletzlichkeit der Wohnung oder dem Schutz der Intimsphäre - einem Schutz im Rahmen dessen, was vernünftigerweise und rechtmäßig zu erwarten ist. Einen Anspruch auf Schutz der Privatsphäre "im Rahmen dessen, was vernünftigerweise und rechtmäßig zu erwarten ist": Diese Lesart hat sich in der Interpretation der vierten Ergänzung zur amerikanischen Verfassung, der Bill of Rights, durchgesetzt. Die Formel der vernünftigen und rechtmäßigen Erwartbarkeit hat ihre eigenen Schwachstellen: Wenn Bürger - weil dies technisch möglich ist - damit rechnen müssen, dass ihre Häuser mit Infrarot-Kameras von außen auf mögliche Haschisch-Plantagen abgetastet werden, liegt keine Verletzung der Privatsphäre im Rahmen der vernünftigen und rechtmäßigen Erwartbarkeit vor. Das gleiche trifft zu, wenn beim Browsen im Internet Nutzerdaten erfasst werden. Denn mit einem besonderen Schutz der Privatsphäre ist hier, im Internet, nicht zu rechnen.[135]

Normative Konkretisierung

So wie das Prinzip der vernünftigen und rechtmäßigen Erwartbarkeit Privatheit nur in Grenzen zu schützen vermag, hat aber auch das Prinzip der informationellen Selbstbestimmung seine Schwachstellen. Der Schutzgehalt des Prinzips ist als Befugnis formuliert, über die Preisgabe und Verwendung von *Daten* selbst zu bestimmen. Nicht jedoch Daten sind hier das eigentliche Thema, sondern Informationen. Der Unterschied zwischen beiden ist relevant. Schutzbedürftig ist der Einzelne nicht deshalb, weil sich Daten (oder Informationen) *auf ihn beziehen*. Vielmehr sollte die informationelle Selbstbestimmung den Bürger, so die Informationsrechtlerin Marion Albers, "mit Blick auf den übergreifenden Kontext und die darin enthaltenen sozialen Positionen"[136] schützen. Dies betrifft, um ein Beispiel zu nennen, den Umgang mit genetischen o-

---

[134] Allen, Privacy in American Law, in: Rössler (Hrsg.), Privacies. Philosophical Evaluations, SUP 2004, S. 19 - 39; Solove, S. 65 - 75.

[135] Solove, Digital Dossiers and the Dissipation of Fourth Amendment Privacy, in: 75 Southern California Law Review 1083 (2002), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=313301 .

[136] Albers, Informationelle Selbstbestimmung, Nomos Verlag, 2005, S. 621.

der mit anderen gesundheitsrelevanten Informationen. Für sich genommen, sind diese Informationen wenig aussagekräftig. Ohne Zuhilfenahme der entsprechenden medizinstatistischen Datenbanken kann ein Patient sie gar nicht interpretieren. Erst im Kontext eines statistischen Wissens, über das Ärzte oder Versicherungen verfügen, gewinnen die Daten an Aussagekraft. [137]

Wenn man nun die Idee aufgibt, dass der Grad, zu dem Daten schützenwert sind, sich bereits aus einem eigentumsähnlichen Bezug zur Person ergibt, wird man verschiedene Arten von Kontexten, innerhalb derer Daten zu Informationen werden, auch konkretisieren müssen - und zwar mit Blick nicht nur auf informationelle Privatheit. Die verschiedenen Garantien, die unsere Verfassung bietet - Unantastbarkeits-, Achtungs-, Schutz- Rechts-, Unverletzlichkeits- und Freiheitsversprechen; die Freiheit des Glaubens und Gewissens, der Schutz von Ehe und Familie, Kommunikationsrechte, Privatheits- und Geheimnisgewährleistungen - all dies müsste in eine Konkretisierung von Kontexten, in den Informationen Bedeutung erlangen, mit einfließen.[138] Nur durch eine solche Konkretisierung, nicht aber durch die Berufung auf ein viel zu allgemeines Prinzip der informationellen Selbstbestimmung, können in all diesen Bereichen Lösungen gefunden werden, die auch zufriedenstellend begründbar sind. Ich schlage nicht vor, dass wir, wie in den USA, auf einen übergreifenden Datenschutz vollständig verzichten sollten und statt dessen eine Reihe von unzusammenhängenden Einzelgesetzen erlassen. Aber ich glaube, dass der Datenschutz einer gewissen Öffnung bedarf, wenn er nicht weiterhin als eine Agentur für Spezialfragen wahrgenommen werden will, als Instanz, die in Fragen der Technik und Fragen des Grundrechts zwar einerseits kompetent Rat geben kann, deren Urteil aber, aufgrund der

---

[137] Eine ähnliche Überlegung liegt auch dem Urteil im US-Gerichtsfall Dwyer v. American Express Co. zugrunde. Kreditkartenkunden verklagten die Firma American Express, weil diese ihre persönlichen Daten an Adresshändler weitervermietet hatte. Das Gericht stellte sich auf die Seite von American Express - weil den Kunden durch die Weitergabe der Daten kein finanzieller Schaden zugefügt worden sei. Wertvoll für Dritte, so das Gericht, seien die einzelnen Kundendaten schließlich erst dadurch geworden, dass American Express sie zu einer großen Datenbank zusammengefügt hatte. Siehe Solove, The Digital Person, in: New York University Press 2004, S. 89.

[138] Marion Albers hat dies in ihrer Arbeit "Informationelle Selbstbestimmung" ausführlich dargelegt. Vgl. auch Solove, A Taxonomy of Privacy, in: 154 U, Pennsylvania Law Review (im Erscheinen), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622 .

Komplexität der Materie, für den Laien selten nachvollziehbar ist. Datenschutz wird so zu einem Pokerspiel. Die einzige Karte, auf die seine Akteure immer wieder setzen, ist die Trumpfkarte: Die enge Anbindung der informationellen Selbstbestimmung an das Grundrecht. Geht dieser Stich verloren, ist der Datenschutz ganz aus dem Spiel. Ohne eine Öffnung, auch auf Orientierungslinien hin, die vielleicht etwas unterhalb des Ranges verfassungsrechtlicher Prinzipien angesiedelt sind, kann der Datenschutz die Probleme, die sich zukünftig stellen werden, kaum in die Griff bekommen.

Megadatenbanken

Insbesondere scheint mir, dass eine Politik des Informationsschutzes, die sich in erster Linie auf *individuelle Schutzrechte* bezieht, schlecht gerüstet ist, um den Problemen gerecht zu werden, die sich vor allem im Umgang mit großen Datenbanken stellen. Große Datenbanken sind sozusagen einer der Kontexte, innerhalb dessen Daten zu Informationen werden - und ein Bereich, wo normative Konkretisierung besonders vonnöten wäre. Große Datenbanken: Das sind Bestände aus demographischen Informationen, zusammengesammelten Einträgen aus öffentlichen Registern und aus Kundenbeziehungen, wie sie in Deutschland zum Beispiel unterhalten werden von Firmen wie Schober, GfK, AZ Direkt, Experian und Infas Geodaten, kurz: Von Auskunfteien, Adressmaklern und Scoring-Firmen. Bedeutsamer als diese deutschen Firmen sind international tätige Unternehmen wie etwa Acxiom, welches mit einem Petabyte an Daten handelt - das entspricht ungefähr dem Volumen von 80.467 Bibeln. Oder Choice Point mit seinen 17 Milliarden online verfügbaren Datensätzen. 40.000 kommen täglich hinzu. Auf mehr als 250 Terrabyte speichert Choice Point Daten über mehr als 200 Millionen Menschen. Würde man all das ausdrucken, könnte man mit dem Papier eine Strecke pflastern, die so lang ist wie 77mal eine Hin- und Rückreise zum Mond. Ein weiteres Beispiel: Lexis Nexis mit einigen Milliarden Datenbankeinträgen. Lexis Nexis begann in den 70er Jahren mit einer Service-Datenbank für Steuerbehörden. Hinzu kamen zunächst ein Telekommunikations-Netzwerk, Anwendungen für Geheimdienste und eine Datenbank mit Einträgen aus öffentlichen Registern. Dann übernahm Lexis Nexis RiskWise, eine Softwarefirma, die Programme zum Einschätzen von Kreditrisiken entwickelt. Und schließlich wurde noch ein weiterer großer Informationsdienst Lexis Nexis einverleibt: Die Firma Seisint, dessen Gründer in den 90er Jahren mit einer Daten-

bank von Automobilen in Florida begann - und einem Service mit den Namen "Auto Track". Seisint wiederum brachte Allianzen mit den Unternehmen Equifax (einer Direktmarketingfirma für den Finanzmarkt), Accenture (Customer Relation Marketing) und Naviant (Email-Marketing) in die Ehe mit Lexis Nexis ein. Insgesamt verfügt Lexis Nexis heute über 36.000 Informationsquellen. Sieben Millionen neue Dokumente werden jede Woche neu in das Netz eingespeist.[139]

Dass sich, mithilfe solcher Megadatenbanken, Informationen zu einem Persönlichkeitsprofil zusammenfügen lassen, ist nur eine der Gefahren. Wie weit uns in Deutschland das Grundrecht vor solchen Gefahren schützt, hat Margarete Schuler Harms an dieser Stelle, nämlich auf dem letztjährigen Symposium unter dem Motto "Living by Numbers", in ihrem Vortrag zur kommerziellen Nutzung statistischer Persönlichkeitsprofile dargelegt.[140] Große Datensammlungen implizieren jedoch auch Probleme, die über die Persönlichkeitsrechte hinausgreifen - und damit auch über den Bereich der informationellen Selbstbestimmung. Einige dieser Probleme möchte ich im Folgenden skizzieren.

Nichtdiskriminierung

"Nichtdiskriminierung" ist ein Schutzziel, welches unter anderem im Zusammenhang mit der Debatte darüber eine Rolle spielt, inwiefern es Versicherungsunternehmen gestattet sein soll, genetische Daten ihrer Kunden dazu zu verwenden, Versicherungsverträge nach individuellen Gesundheitsrisiken auszugestalten. Allein aufgrund der Tatsache, dass Firmen Daten und Datenbanken benutzen, um Kunden in verschiedene Kategorien einzuteilen, ist das Gebot der Nichtdiskriminierung eine Angelegenheit des Datenschutzes geworden. Genauer: Das Problem der *unfairen* Diskriminierung. Unfaire Diskriminierung findet zum Beispiel statt, wenn Kunden aufgrund von Merkmalen kategorisiert werden, die mit dem Sachverhalt, um den es geht, lediglich statistisch verknüpft sind - wenn also zum Beispiel ein Versandhändler aufgrund des

---

[139] Angaben nach O'Harrow Jr., No Place to Hide, Free Press/Simon and Schuster, 2005.

[140] Schuler-Harms, Die kommerzielle Nutzung statistischer Persönlichkeitsprofile als Herausforderung für den Datenschutz, in: Living by numbers - Leben zwischen Statistik und Wirklichkeit, Sokol (Hrsg.), 2005, S. 5 - 37.

Zustandes der Vorgärten in einem Wohngebiet oder mit Blick auf den Ausländeranteil in der Nachbarschaft keine Sendungen auf Rechnung dorthin liefert.

Nun mag man sich darüber streiten, welche Form der Diskriminierung fair ist und welche unfair. Mit Sicherheit unfair sind alle Formen der Diskriminierung - also der Unterteilung von Kunden in gute Kunden und schlechte Kunden, die zu unterschiedlichen Konditionen bedient werden - auf der Grundlage einer nicht hinreichend sorgfältigen Analyse von Informationen und statistischen Daten. Der amerikanische Jurist Jeffrey Rosen sieht hier eines der zentralen Probleme im Umgang mit Megadatenbanken, welches der Regulierung durch Datenschutzgesetze bedarf. "In einer Welt kurzer Aufmerksamkeitsspannen", schreibt Rosen, "in welcher Informationen nur allzu leicht mit Wissen verwechselt werden, schützt uns Privatheit davor, falsch eingeschätzt und aus dem Zusammenhang heraus beurteilt zu werden."[141] Dies gilt, der Sache nach, sowohl für die Nutzung von Datenbanken zum Zwecke der Pflege von Kundenbeziehungen wie auch für Sicherheitssysteme zum Screening von Fluggästen im Zusammenhang mit der Terrorismusabwehr.

Aber auch bei gründlicher und aufmerksamer Analyse von Daten bleibt die Frage, welche Formen von Diskrimierung - also zum Beispiel etwa der Privilegierung bestimmter Kundengruppen durch einen Dienstleistungsanbieter - als fair und welche als unfair betrachtet werden sollen. Die Europäische Datenschutzrichtlinie versucht dieses Problem zu umgehen, indem sie (in Artikel 15) verlangt, dass Entscheidungen, *die jemanden erheblich beeinträchtigen*, zumindest nicht ausschließlich aufgrund der *automatisierten* Verarbeitung von Daten getroffen werden sollen. Damit ist die Frage, welche Arten von Diskriminierung oder von Kategorisierung fair und welche unfair sind, aber noch nicht aus der Welt. Ob es richtig ist, wenn Menschen zum Beispiel aufgrund ihrer genetischen Disposition oder ihres gesundheitlichen Zustandes höhere Krankenkassenbeiträge zahlen müssen, ist eine moralische Frage. Der Datenschutz kann diese Frage nicht beantworten. Er kann lediglich darauf hinarbeiten, dass die Frage sich erst gar nicht stellt: Indem er bewirkt, dass die Daten, die zum Zwecke einer solchen Diskriminierung erforderlich wären, dem Versicherer nicht zur Verfügung gestellt werden.

---

[141] Rosen, The unwanted Gaze: The Destruction of Privacy in America, 2000, S. 8.

Im extremen Fall bedeutet Diskriminierung, dass jemand von bestimmten Dienstleistungen oder vom Bezug bestimmter Produkte ausgeschlossen wird - weil er zu einem Kreis von Kunden gehört, von dem ein Unternehmen sich keinen Gewinn verspricht. Ein harmloser Fall dieser Art ist es, wenn ein Kunde als Anrufer bei einer Kundenhotline an seiner Rufnummer als "schlechter Kunde" erkannt und gar nicht oder nur an letzter Stelle bedient wird. Schwerer wiegt es, wenn ihm die Eröffnung eines Kontos bei einer Bank verweigert wird.

Wiederum sind es Datenbanken, welche Unternehmen solche Formen der Diskriminierung ermöglichen. Die angemessene Antwort auf dieses Problem wäre es, eine Liste von Dienstleistungen und Produkten zu definieren, von deren Bezug niemand ausgeschlossen werden darf. Wer sollte sich dieses Problems annehmen? Zwar stellt es sich im Zusammenhang mit Techniken der Datenverarbeitung. Aber hat der Datenschutz deshalb auch die Kapazitäten, es zu lösen? Mit Berufung allein auf das Prinzip der informationellen Selbstbestimmung sicherlich nicht.[142]

Effizienz der Strafverfolgung

Ein weiteres Problem, welches kaum mit den Mitteln der informationellen Selbstbestimmung angegangen werden kann, ist eine neue Dimension gewöhnlicher Strafverfolgung, welche durch große Datenbanken ermöglicht wird. Es ist damit zu rechnen, dass die Verfahren der Strafverfolgung in Zukunft immer effizienter arbeiten. Noch einmal: Mittels eines einfachen RFID-Chips und den personenbezogenen Einkaufsdaten aus dem Payback-System lässt sich verfolgen, wer eine leere Flipstüte achtlos im Park hat liegen lassen. Informationen von Mautsystemen können verwendet werden, um die Fahrtzeit einzelner Wagen zwischen zwei Mautstellen zu berechnen - und Fahrer, die offensichtlich zu schnell gefahren sein müssen, abzustrafen.

[142] Beat Rudin hat mich auf dieses Problem aufmerksam gemacht.

Das gleiche kann realisiert werden, indem die Bewegung von Autofahrern mit Hilfe ihrer mitgeführten Mobiltelefone überwacht wird. Projekte in dieser Richtung sind bereits in Planung.[143]

Vieles wird möglich, woran zuvor niemand hat denken können.[144] Megadatenbanken, schreibt der amerikanische Bürgerrechtler Chris Hoofnagle vom Electronic Privacy Information Center (EPIC), "ermöglichen eine Effizienz in der Strafverfolgung, die von den Vätern der Verfassung nicht ins Auge gefasst wurde. Dadurch wird die *Balance of Power*, das Mächtegleichgewicht zwischen den Elementen des Staatswesens, ins Wanken gebracht."[145] Hier liegt auch ein wenig beachteter Effekt im Zusammenhang mit dem Aufbau von DNS-Datenbanken zur Verbrechensbekämpfung. Ob die Persönlichkeitsrechte von jemanden, dessen genetische Daten in eine solche Datenbank aufgenommen werden, verletzt werden, ist eine Sache. Um sie zu entscheiden, muss man sich anschauen, welchen Aufschluss über eine Person die hier erhobenen und gespeicherten Informationen ermöglichen. Eine andere Sache - die wiederum mit Persönlichkeitsrechten und informationeller Selbstbestimmung nur

---

[143] In den Vereinigten Staaten plant das Missouri Department of Transportation auf 8.800 Kilometern Straße die Überwachung von Autofahrermobiltelefonen zum Zwecke der Verkehrssteuerung: Verkehrsverdichtungen könnten auf diese Weise in Echtzeit erkannt und Maßnahmen zur Stauvermeidung ergriffen werden wie zum Beispiel Umleitungen. Das kanadische Unternehmen Delcan NET soll die Pläne im Auftrag des Bundesstaates realisieren. Nachzulesen in: State looks to track drivers. Firm would follow cars via cell phone, Columbia Tribune vom 09.10.2005; vgl. auch Blog-Eintrag: Do we really want perfect law enforcement?, in: http://www.concurringopinions.com/archives/2005/10/do_we_really_wa_1. html#more) .

[144] Ein anderes Beispiel: Lessigs Szenario eines "Wurms", der von staatlichen Ermittlern über das Internet verbreitet wird, um nach illegaler Software zu suchen. Nachzulesen in: Reading the Constitution in Cyberspace, Emory Law Journal, Summer 1996; vgl. ders., Code and other laws of Cyberspace, Basic Books, 1999, S. 17. ff.) oder Adlers Gedankenspiel einer "netzweiten Suche" nach genau definierten Dateien auf privaten Festplatten in: Cyberspace, General Searches and Digital Contraband. The Fourth Amendment and the Net-Wide Search, in: 105 Yale Law Journal 1093, 1996, http://www.hogen.org/research/paper/lj23/internet_e.html) . Rosen beschreibt das Spionagewerkzeug Carnivore als eine Realisation dieser Szenarien in: The naked crowed. Reclaiming Security and Freedom in an anxious Age, Random House, 2004).

[145] Zitat nach: O'Harrow Jr., No Place to Hide, a.a.O., S. 138.

wenig zusammenhängt - ist es, dass mithilfe umfangreicher DNS-Datenbanken die Strafverfolgung eine neuartige Perfektion erreichen kann. Insofern es unvermeidbar ist, dass Menschen ständig genetische Information, enthalten etwa in Hautschuppen oder in Haaren, absondern, ließe sich mittels DNS-Spurenlese auch bei geringfügigeren Vergehen leicht der Urheber ermitteln. In einem solchen Szenario kommt es nicht nur darauf an, wessen Daten erhoben und gespeichert werden, sondern ebenso, wie der Zugriff auf Datenbanken sich gestaltet: Wer Zugriff hat und zu welchem Zweck auf die Datenbanken zugegriffen werden darf. Diese Frage wurde im Zuge der Diskussion um DNS-Datenbanken in Deutschland weitgehend ausgeklammert.

Ich bin der Meinung, dass eine zu große Präzision in der Strafverfolgung etwas ist, das wir eigentlich nicht wollen können. Eine "Bestrafungsgesellschaft", in der bereits kleinste Vergehen sofort aufgespürt und geahndet werden, würde sozusagen der Corporate Identity unseres Gemeinwesens strikt zuwiderlaufen. Denn die Idee, dass wir unrechte Handlungen nicht nur dann unterlassen, wenn wir davon ausgehen können, mit Sicherheit ertappt und bestraft zu werden, ist ein Kernelement unseres moralischen Selbstverständnisses. Dies gilt zumindest für Bagatelldelikte. Wer möchte schon auf der Stelle erfasst und zur Kasse gebeten oder verklagt werden, weil er fünf Stundenkilometer zu schnell gefahren ist oder weil er eine von einem Freund kopierte Version des Textverarbeitungssystems Microsoft Word auf seinem Computer benutzt?

Den Einsatz von supereffizienten Techniken der Strafverfolgung auf Delikte ab eines gewissen Grades zu beschränken, würde allerdings nur bedingt helfen. Denn allein die Möglichkeit, dass der Kreis von Vergehen, bei welchen, wie in diesem Beispiel, die DNS-Analyse zum Einsatz gebracht werden kann, jederzeit erweitert werden kann, hinterlässt bei jedem einzelnen ein - begründetes - Gefühl der Unsicherheit.

Es gibt aber noch einen anderen Einwand gegen die Etablierung supereffizienter Instrumente der Strafverfolgung. Selbst in einer demokratischen Gesellschaft nämlich können bestimmte kriminelle Handlungen wertvolle Funktionen erfüllen. Gesetze können ungerecht sein oder schlecht durchdacht. Werden solche Gesetze von einem Teil der Menschen systematisch missachtet - sei es aus blo-

ßem Eigeninteresse, sei es aus zivilem Ungehorsam - kann dies ein Anlass sein, sie zu ändern.[146]

Abgesehen von all diesen Überlegungen, wäre zudem ein gesellschaftliches System, dass ausschließlich auf der Androhung von Strafen basiert, vermutlich auch weniger effizient als eines, welches von Kooperationsbereitschaft ausgeht - darauf deuten zumindest die Ergebnisse von Versuchen hin, die Wissenschaftler wie der Ökonom Ernst Fehr mit Probanden im Spiellabor unternommen haben.[147] Die Effizenz der Strafverfolgung zu beschränken ist, rechtlich gesehen, vermutlich keine leichte Aufgabe. Es ist unmöglich, einerseits Verhaltensweisen unter Strafe zu stellen, andererseits Aufklärungsmöglichkeiten mit dem Argument zu begrenzen, dass aus übergreifenden gesellschaftlichen Gründen nicht alle Straftaten aufgespürt und geahndet werden sollten. Das heißt, dass man im Rechtssystem *andere Argumente* braucht, die es rechtfertigen, dass im Ergebnis nicht alle Straftaten sofort bestraft werden, so dass das Rechtssystem mit übergreifenden gesellschaftlichen Anforderungen kompatibel wird.[148]

Outsourcing der Strafverfolgung

Abgesehen von der Effizienz der Verbrechensbekämpfung stellt sich aber noch eine weitere Frage: Wie weit soll es privaten Organisationen erlaubt sein, selbst Aufgaben der Strafverfolgung zu übernehmen? Wiederum ein Beispiel aus den USA. Jemand leiht sich bei dem Anbieter Acme Rent-A-Car einen Mietwagen. Nachdem er eine längere Strecke mit dem Wagen zurückgelegt hat, bekommt er beim Tanken Probleme mit seiner Kreditkarte. Ein Anruf bei der Bank klärt ihn auf. Sein Limit ist überzogen. Drei Mal ist ein Betrag in der Höhe von 450 Dollar eingezogen worden - als Strafe für Geschwindigkeitsüberschreitungen mit dem Mietwagen, zu zahlen an die Mietwagenfirma, welche ihre Fahrzeuge mit GPS ausstattet und Geschwindigkeitsüberschreitungen via Satellit beobachtet. Im Ernstfall können die Wagen sogar per Fernbedienung ausgeschaltet werden.

---

[146] Eine ausführliche Diskussion dieser Fragen: Adler, Cyberspace, General Searches, and Digital Contraband, a.a.O.

[147] Vgl. Fehr/Gächter, Fairness and Retaliation: The Economics of Reciprocity, in: Journal of Economic Perspectives, 14 (2000), S. 159 - 181, http://www.iew.unizh.ch/wp/iewwp040.pdf .

[148] Für diesen Hinweis bedanke ich mich bei Marion Albers.

Nun ist ein Unternehmen wie Acme Rent-A-Car nur ein kleiner Stein im großen Mosaik der Allianzen und Zusammenschlüsse zwischen den großen Informationsdiensten wie Choice Point oder Lexis Nexis. Choice Point hat mittlerweile in den USA bereits ein privates Vorstrafenregister aufbauen können. Über fünf Millionen Einträge in Strafregistern, so das Unternehmen, seien von Kunden im Jahr 2003 nachgefragt worden. Über 400.000 Fälle, wo jemand in den letzten sieben Jahren einen Eintrag in einem Strafregister erhalten habe, sollen dabei zu Tage getreten sein. Eine durch Choice Point durchgeführte Untersuchung von 200.000 Big Brother-Kandidaten erbrachte 38 Mörder und 67 Fälle sexueller Belästigung. In einer anderen Studie zeigte Choice Point, dass einer von vier Pizza-Auslieferern erst vor kurzem im Gefängnis war - und zog das Fazit: "Würden Sie das Risiko eingehen, mit einer Firma Geschäfte abzuschließen die nicht ihre Fahrer einem Screening unterzieht?" Firmen wie Choice Point agieren nicht nur in den Vereinigten Staaten: Die amerikanische Auskunftei World Compliance bietet seit einigen Monaten ihren Service auch deutschen Unternehmen an.[149]

Es bleibt nicht allein bei dieser Form des "Outsourcing". Im Zuge der Ermittlungen nach dem Anschlag auf das World Trade Center haben Polizei, FBI und Geheimdienste ungehindert auf die Datenbanken von Choice Point, Lexis Nexis und anderen Informationsdiensteanbietern zugreifen können. Die Datenbankbetreiber haben zu dieser Zeit ihre Dienste sogar von sich aus kostenlos zur Verfügung gestellt. Staatliche Ermittler, die sich aus dem Material bedient haben, waren weder für die Zuverlässigkeit der Daten verantwortlich noch für die Einhaltung entsprechender Datenschutzbestimmungen im Zusammenhang mit dem Betrieb der Datenbanken.[150]

Unmöglich ist so etwas auch in Deutschland nicht. Mit dem Instrument der Rasterfahndung zum Beispiel lassen sich auf eben diese Weise Datenbanken, die zu ganz anderen Zwecken angelegt wurden (und die sich auch nur nach Auflagen richten müssen, die eben diesen Zwecken genügen), für den Zeitraum einer Suche quasi verstaatlichen. Die geplante Vorratsdatenspeicherung von Telekommunikationsdaten ist ebenfalls ein ganz konkreter Fall, wo Datenbanken, die von privaten Unternehmen unterhalten werden, zu einem Instrument staatlicher Ermittlung werden.

---

[149] S. O'Harrow Jr., a.a.O.
[150] Ebd.

Zusammenfassung

Lassen Sie mich zum Schluss meine Überlegungen noch einmal kurz zusammenfassen.

1. Die Entscheidung für Begriffe, Metaphern und Geschichten, die wir wählen, um technische, soziale und politische Entwicklungen zu beschreiben, ist keine triviale Angelegenheit. Das Bedrohungsszenario der "Überwachungsgesellschaft" definiert den Ernstfall der Gefahr zu eng. Gleichzeitig wird die Hürde der Beweislast unnötig hoch angelegt. Tatsächlich verfügen wir jedoch über ein Konzept, welches weiter gefasst ist und zugleich präziser greift als die Metapher der Überwachung: Die informationelle Selbstbestimmung.

2. Das Prinzip der informationellen Selbstbestimmung hat seinerseits einen markanten Schwachpunkt. Dieser liegt in der Vorstellung begründet, dass der Einzelne vor allem deshalb schutzbedürftig sei, weil sich Daten (oder Informationen) *auf ihn beziehen.* Auf diese Weise lassen sich die verschiedenen Kontexte, innerhalb derer Daten zu Informationen werden, aber nur unzureichend generalisieren. Informationelle Selbstbestimmung ist viel zu allgemein gefasst, um damit in der großen Vielfalt der verschiedenen Fälle zu begründeten Urteilen zu kommen. Besser sollten die verschiedenen Anwendungsbereiche konkretisiert werden. Wichtig ist: In eine solche Konkretisierung sollten auch andere Grundrechte einfließen als das eng am Persönlichkeitsrecht orientierte Prinzip der informationellen Selbstbestimmung.

3. Ein Kontext, den ich für bisher unzureichend berücksichtigt halte, ist die Gewinnung von Informationen im Rückgriff auf Megadatenbanken. Hier ganz besonders ist es wichtig, sich bei der Gestaltung von rechtlichen Rahmenvorgaben nicht so sehr ausschließlich am Persönlichkeitsrecht und der informationellen Selbstbestimmung zu orientieren.

"Das Problem", schreibt der amerikanische Jurist Daniel Solove, "liegt nicht so sehr darin, dass es keine *individuelle* Kontrolle über Informationen gibt, sondern dass wir uns in einer Situation befinden, in der niemand eine nennenswerte Kontrolle über Informationen ausübt." Dies, so Solove beträfe weniger die Auskunftsrechte des Einzelnen, als die Anforderungen an das Design von großen Datenbanken: "Beunruhigend ist nicht, dass [Unternehmen wie]

Amazon Kunden ausspionieren oder ihre Daten verwenden, um sie zum Kauf von mehr Büchern zu verführen. Beunruhigend ist, dass Amazon ohne Einschränkung mit seinen Daten tun kann, was es will" - so wie dies geschehen war, als Amazon in den USA auf einen Schlag seine Privacy-Regeln veränderte und sich für den Fall einer Geschäftsaufgabe oder eines Verkaufs des Unternehmens das Recht zur Weitergabe der persönlichen Daten seiner Kunden herausnahm.

Nun wäre den Amerikanern schon viel geholfen mit einem Datenschutz, wie wir ihn hier in Europa haben, wie zum Beispiel:

- dem Auskunftsrecht: Dem Anspruch des Einzelnen, herauszufinden, welche Informationen über ihn gespeichert sind und wie diese verwendet werden

- der Zweckbindung: Der Einzelne muss verhindern können, dass ohne sein Wissen oder gegen seinen Willen Informationen über ihn zu anderen Zwecken verwendet werden, als dies ursprünglich vereinbart wurde

- einem Recht darauf, Informationen, die einen selbst betreffen, berichtigen oder vervollständigen zu können.

An dieser Ordnung müssen wir weiter arbeiten, auch über das Prinzip der informationellen Selbstbestimmung hinaus, wenn wir unfaire Diskriminierungen, ein Umsichgreifen von Selbstjustiz mit Hilfe von Auskunfteien und eine über das Ziel hinausschießende Strafverfolgung vermeiden wollen.

Next Generation: Welche Bedeutung haben informationelle Selbstbestimmung und Privatheit

Julia Kühn

Was ist zu sagen über die Bedeutung von informationeller Selbstbestimmung und Privatheit für junge Menschen, also über das Verhältnis junger Leute zum Thema Datenschutz. Zur Erinnerung: Was ist die informationelle Selbstbestimmung? Dahinter verbirgt sich das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Es ist eine Ausprägung des allgemeinen Persönlichkeitsrechts und wurde vom Bundesverfassungsgericht im so genannten Volkszählungsurteil anerkannt. Ausgangspunkt war die Überlegung, dass seine Gewährleistung eine elementare Bedingung eines freiheitlichen demokratischen Gemeinwesens ist, bei dem die Menschen mitwirken können sollen. Dazu muss jeder Mensch wissen, wer was wann und bei welcher Gelegenheit über ihn weiß. Dabei ist das Recht auf informationelle Selbstbestimmung weit gefasst und umfasst alle Arten von Daten, da durch Verarbeitungsmöglichkeiten auch ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen kann. Einschränkungen des Grundrechts müssen zwar möglich sein, bedürfen aber einer gesetzlichen Grundlage und besonderer Rechtfertigung. Die Abwägung zwischen dem Geheimhaltungsinteresse des Betroffenen und dem Informationsinteresse der verarbeitenden Stelle obliegt also dem Gesetzgeber.

Wie wichtig ist nun dieses Thema für junge Leute?

Welche Daten wollen junge Menschen geschützt wissen, oder denken sie, dass sie nichts zu verbergen haben?

Gibt es ein Leitbild des "angepassten" jungen Menschen, der Schutz nicht nötig hat, oder ihn für nicht nötig hält?

Ist demokratisches, bürgerrechtliches Engagement für Datenschutz in den Augen junger Menschen sinnvoll oder lohnend?

Diesen Fragen soll mit Hilfe von drei Beispielen nachgegangen werden. Doch zunächst war es für mich interessant festzustellen, dass es kaum Untersuchungen zu diesem Thema gibt. Weder die gängigen Jugendstudien wie shell, bravo, noch solche der Ministerien, Verbraucherzentralen oder Parteien befassen sich explizit mit dem Thema junge Leute und Datenschutz. Meist werden sie unter denselben Gesichtspunkten wie Erwachsene betrachtet. Lediglich die Verbraucherzentrale NRW geht auf ihrer Homepage für Jugendliche auf Kundenkarten ein. Dort wird erklärt, inwieweit man dort seine Daten preisgibt und zu welchen Schwierigkeiten das zum Beispiel bei der Ausbildungsplatzsuche führen kann.

Ein Artikel aus der Zeitschrift Prinz (Ausgabe Stuttgart) mag vielleicht einen Einblick in die allgemeine Wahrnehmung des Datenschutzes bei jungen Leuten geben. Er ist übertitelt mit "Der große Lauschangriff". Nanu, denkt man sich, eine Zeitschrift, die sich an die jüngere Bevölkerung wendet und gewöhnlich Tipps zur Freizeitgestaltung enthält, klärt nun über die Gefahren der akustischen Wohnraumüberwachung auf? Weit gefehlt. Statt über Einschränkungen des Grundrechts auf Unverletzlichkeit der Wohnung zu informieren preist der Autor, einer Werbung ähnelnd, verschiedene Handys und deren Fähigkeiten an. Kann man also bei jungen Leuten mit einem so umstrittenen Begriff Werbung machen? Die Verwendung des Titels deutet eher auf eine allgemeine Ignoranz hin. Der Autor benutzt hier ein durch die Nachrichten von jedem schon mal wahrgenommenen Begriff, wahrscheinlich in dem Bewusstsein, dass nur die Wenigsten wissen, wofür der Begriff steht. Umso erstaunlicher, da erst vor kurzem in allen Nachrichten berichtet wurde, dass das Bundesverfassungsgericht eine Reform des großen Lauschangriffs anmahnte.

Aus meinem eigenen Umfeld möchte ich folgende zwei Bereiche darstellen, in denen speziell Studierende von datenschutzrechtlich relevanten Maßnahmen betroffen sind: Zum einen die Einführung von Chipkarten, zum anderen die Videoüberwachung an Universitäten.

Seit einigen Jahren werden Chipkarten an manchen Universitäten eingeführt, um verschiedene Dienstleistungen zusammenzufassen. Die Funktionen der Chipkarten sind unterschiedlich: Möglich ist beispielsweise die Nutzung als Studierendenausweis, Fahrausweis, Schlüssel, Bibliotheksausweis oder Geldkarte aber auch zur Rückmeldung zum Semester. Die meisten Studierenden sind an das Medium der Karte gewöhnt, sei es durch EC- oder Payback-Karten, so dass ihnen der Gebrauch einer Karte auch im universitären Raum nicht fremd ist. Warum werden diese Chipkarten nun eingeführt? Im Vordergrund steht, dass Verwaltungskosten reduziert und der Service verbessert wird. Darüber hinaus braucht der Einzelne zum Beispiel kein Kleingeld mehr, besitzt nicht so viele verschiedene Karten und ist nicht mehr auf unflexible Öffnungszeiten der Verwaltung angewiesen. Unmut kommt höchstens einmal auf, wenn die Schutzgebühr zu zahlen ist. Aber sind die Gefahren nicht größer? Zum einen ist eine wirksamere Anwesenheits- und Leistungskontrolle möglich. Mit der Verbindung der verschiedenen Funktionen in einer Chipkarte könnten sogar Bewegungsprofile erstellt werden. Dies ist umso bedenklicher, als das Entwicklung und Bereitstellung der Technik durch privatwirtschaftliche Unternehmen erfolgt, die so an personenbezogene Daten von Studierenden gelangen. Für welche anderen Zwecke diese dann genutzt werden können, mag sich jeder denken.

Als zweiten Bereich, der die informationelle Selbstbestimmung innerhalb der Universität betrifft, gehe ich auf die Einführung von Videoüberwachung an Universitäten ein. Dabei werden je nach Universität unterschiedlichste Räume überwacht, manchmal nur Geräte, andernorts ganze Gebäude, die Bibliotheken oder Computerpools. Der Zweck ist meistens gleich: Diebstahl und Vandalismus entgegenwirken. Man geht davon aus, dass Videoüberwachung Kriminalität reduziert, also präventiv wirkt. Allerdings wird dabei außer Acht gelassen, dass Studierende und Lehrende, die beobachtet werden, auf die Wahrnehmung ihrer Freiheitsrechte verzichten könnten. Das ist besonders misslich, da die Universität als Ort der Forschung und Lehre besonders schützenswert ist.

Von der Universität Münster, an der ich studiere, kann ich Folgendes berichten: Die Masse der Studierenden scheint an dem Schutz der eigenen Daten wenig Interesse zu haben. Eine Aktion des Allgemeinen Studierendenausschusses (AStA) mit den kritischen Juristinnen und Juristen Münster zeigt ein anderes Bild, sobald Studierende auf technische Möglichkeiten oder bestehende Überwachung hingewiesen werden. Mit der Aktion "Bürgerrechte ernst

nehmen - Videoüberwachung verhindern!" die vom 28.-30. Juni 2005 in Gebäuden der Universität durchgeführt wurde, informierten wir die Studierenden mit großen Tafeln, welche Stellen in der Universität videoüberwacht werden und ob und wenn ja wie lange eine Speicherung der aufgezeichneten Bilder erfolgt.

Einzelne Räume wie das Rechenzentrum oder Bibliotheksteile werden schon seit einigen Jahren videoüberwacht, andere Kameras sind erst vor kurzem eingeführt worden. Die Videoüberwachung erfolgte zunächst jedoch ohne eine genaue Überprüfung der Notwendigkeit im Einzelfall und ohne Einschaltung des Datenschutzbeauftragten der Universität. Dieser versäumte eine Vorabkontrolle und die Erstellung eines Verfahrensverzeichnisses, wie es in § 8 Datenschutzgesetz des Landes NRW (DSG NRW) vorgesehen ist. Seit November gibt es immerhin eine Dienstvereinbarung zwischen dem Personalrat und der Dienststelle, in der nähere Voraussetzungen und der Umgang mit der Videoüberwachung geregelt sind. Außerdem ist dieser eine Anlage mit einem Verzeichnis der Kameras beigefügt. Laut dieser Anlage gibt es zurzeit 61 Kameras und eine Attrappe in den Gebäuden der Universität. Von diesen zeichnen zehn Kameras die Bilder als Ringspeicherkameras circa 24 Stunden auf, der Rest der Bilder wird direkt auf einen Bildschirm übertragen ohne gespeichert zu werden. Ob dieses Verzeichnis allerdings vollständig ist, weiß wohl keiner so recht, da laut der Kanzlerin der Universität Ziel der Dienstvereinbarung unter anderem sei, "eine möglichst vollständige Dokumentation zu erhalten". Leider entspricht das noch nicht den Vorgaben des Datenschutzgesetzes, das vorsieht in einer Vorabkontrolle eine genaue Aufstellung aller Kameras zu erstellen.

Der Datenschutzbeauftragte der Universität begründet die Videoüberwachung unter anderem mit der erhöhten Manipulationsfähigkeit einzelner Geräte. Zudem sollen in so genannten "Angsträumen" Schutz und Beruhigung gewährt werden. Die Dienstvereinbarung nennt allgemeine präventive Zwecke der Überwachung: Der Schutz vor Gewalt gegen Personen, vor unbefugtem Eindringen und vor Beschädigung oder Diebstahl. Damit wird aber nicht für jede einzelne installierte Kamera auch nachgewiesen, dass dies an der jeweiligen Stelle erforderlich ist. Wenn wie vielfach noch nicht einmal auf Kameras hingewiesen wird, ist es höchst zweifelhaft, dass die aufgestellten Kameras sich dazu eignen einen abschreckenden Effekt auf potentiell Kriminelle auszuüben.

In der Dienstvereinbarung eigens erwähnt wird zudem, dass keine Leistungs- und Verhaltenskontrolle der Mitarbeiter stattfinden soll. Daran wird deutlich, dass diese Möglichkeit technisch besteht, nur nicht genutzt werden soll. Gleiches kann für Studierende gelten, wenn Arbeitsräume überwacht werden oder gar Vorlesungssäle, gerade wenn man an die von der Landesregierung geplanten Studiengebühren denkt.

Mit der Kamera-Aktion des AStA erfuhren viele Studierende überhaupt zum ersten Mal, dass sie in manchen Teilen der Universität unter Videobeobachtung stehen. Tatsächlich zeigten sich die meisten Studierenden erstaunt darüber, dass viele Orte, an denen sie täglich verkehren, videoüberwacht werden und zwar ohne, dass sie dies merken und ohne, dass genau erklärt wird, warum die Kameras angebracht wurden.

Die innerhalb von wenigen Stunden gesammelten 350 Unterschriften - jede Menge für die angeblich so uninteressierten Studierenden - wurden daraufhin der Kanzlerin der Universität mit der Aufforderung übergeben, die unverhältnismäßige Videoüberwachung an der Universität Münster abzuschaffen und Studierende frühzeitig über geplante Maßnahmen zu informieren.

Aber auch an anderen Universitäten gibt es eine teilweise noch viel weitgehendere Videoüberwachung. Besonders hervorgetan hat sich die Universität Paderborn, die dafür auch den letztjährigen Big Brother Award in der Kategorie Regionales verliehen bekam. Die Humboldt-Universität Berlin hat sogar Kameras in Hörsälen eingesetzt.

Meiner Auffassung nach verträgt sich Videoüberwachung grundsätzlich nicht mit dem Auftrag der Universitäten, den Studierenden einen Freiraum der Bildung, des Lernens zu bieten und die Entwicklung von Persönlichkeiten zu unterstützen. Deshalb gehören Videokameras nicht in Universitäten, schon gar nicht in Hörsäle. Die Videoüberwachung käme allenfalls zur Sicherung einzelner Geräte in Frage. Allein die Überwachung, um eventuellen Diebstahl zu verhindern oder gegebenenfalls besser verfolgen zu können, reicht wohl nicht aus, hier sind andere Maßnahmen, die eine Wegnahme verhindern, doch sinnvoller. Zudem dürfte anzunehmen sein, dass mit ihr eine verstärkte soziale Kontrolle einhergeht. Videoüberwachung an Universitäten kann somit nur ausnahmsweise gerechtfertigt sein.

Wie das Bundesverfassungsgericht festgestellt hat, werden Menschen, die damit rechnen müssen, dass all ihre Handlungen registriert und gespeichert werden, möglicherweise alles tun, um nicht aufzufallen. Was dies für eine Gesellschaft und gerade an der Universität zu bedeuten hat, kann sich jeder denken: Konformitätsdruck führt dazu, dass Studierende ihre Grundrechte nicht mehr wahrnehmen, sich zum Beispiel scheuen zu demonstrieren.

So glauben beispielsweise immerhin 28% der knapp 50 Befragten zwischen 15 und 30 Jahren meiner freilich nicht repräsentativen Umfrage, dass sie sich anders verhalten als sonst, wenn sie wissen, dass sie sich im Bereich von Videoüberwachungskameras befinden. Besonders erstaunlich ist für mich, dass zwar 48% der Befragten angeben sich durch Videoüberwachung sicherer zu fühlen, aber nur 19% sich mehr Videoüberwachung wünschen. Insbesondere Schulen und Universitäten sollen ihrer Meinung nach nicht überwacht werden.

Während im Vorfeld des Volkszählungsurteils viele öffentliche Debatten um den Datenschutz stattfanden, ist es doch erstaunlich, wie wenig der Datenschutz in der öffentlichen Wahrnehmung von jungen Leuten heute eine Rolle spielt. Die Gründe für solch einen Wandel sind sicher vielfältig. Zum einen ist die Medienpräsenz solcher Themen sehr gering. Ein anderer Grund mag vielleicht in der veränderten politischen Landschaft liegen. Mitte der Achtziger Jahre gab es noch "das anderen Deutschland", regiert mit Hilfe eines Sicherheitsapparates, der die Bevölkerung bespitzelte. Gerade als Gegenmodell dazu war der Schutz der Daten Einzelner umso wichtiger. Mit Ende der Fronten des Kalten Krieges hat sich aber wohl auch die Staatswahrnehmung vielerseits geändert. Sah man früher die staatliche Sammlung von Daten als missbrauchsanfällig an, so werden heute durch das gesteigerte Sicherheitsbedürfnis vor Kriminalität auch erhöhte Anforderungen an den Staat gestellt, wobei man bereit ist für die Sicherheit eine Einschränkung eigener Rechte hinzunehmen.

Wie wichtig ist nun dieses Thema für junge Leute?

Die gängigen Argumente für eine Datentransparenz lauten: "Ich hab ja nichts zu verbergen", wenn der Staat kontrolliert oder: "Hauptsache, ich bekomme Rabatt", wenn sie Daten an Unternehmen weitergeben.

Sobald junge Menschen informiert werden, kann jedoch von einem allgemeinen selbstverständlichen Verzicht auf die informationelle Selbstbestimmung kaum die Rede sein. Im Gegenteil, durch die zunehmende Verwendung der technischen Mittel zur Datenerhebung, eben nicht nur durch den Akteur Staat, sondern auch durch die Wirtschaft, rückt der Datenschutz zumindest in den genannten Bereichen wieder ins Blickfeld von jungen Leuten.

Next Generation: Welche Bedeutung haben informationelle Selbstbestimmung und Privatheit

Tina Lorenz

Am 1. November 2005 wurde in Deutschland ein neuer Reisepass eingeführt. Er enthält erstmals als biometrisches Datum das Bild des Passinhabers in elektronischer Form. Diese Information wird auf einem Funk-Mikrochip (RFID) gespeichert. In Phase II soll zusätzlich ein elektronischer Fingerabdruck gespeichert werden.

Nach einer Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist die neue Technologie weder praxistauglich noch ausgereift. Die getesteten Verfahren wiesen zwischen 3 und 23 Prozent der teilnehmenden Personen fälschlich zurück. Wenn diese Systeme tatsächlich flächendeckend in der Passkontrolle eingesetzt werden, stehen täglich zehntausende Menschen an den Flughäfen vor rot blinkenden Bildschirmen. Ihre Fingerabdrücke oder digitalen Fotos würden von der Software nicht erkannt. Laut Bundesinnenministerium hätten diese Bürger dann mit einer "verschärften Kontrolle" zu rechnen.

Die BioPII-Studie kommt zu dem Schluss, dass zahlreiche technische Verbesserungen sowie eine weitere "gründliche Untersuchung der Funktionstüchtigkeit, der Erkennungsleistung und der Überwindungssicherheit" notwendig sind. Das BSI räumt damit selbst ein, dass die Technologie alles andere als einsatztauglich ist. Die deutschen Reisepässe gehören laut Bundeskriminalamt (BKA) zu den sichersten der Welt. Funkchips und Biometrie werden dieses Sicherheitsniveau senken, weil sich die Grenzbeamten zunehmend auf die unzulängliche Technik verlassen.

Nach und nach werden in den nächsten Jahren alle deutschen Passinhaber auf den Meldeämtern einer Prozedur unterzogen, die

der erkennungsdienstlichen Behandlung von Kriminellen gleicht. Ein Bild ihres Gesichts und ihrer Fingerabdrücke werden aufgezeichnet. In Folge der Einführung der biometrischen Ausweisdokumente wird das Grundrecht auf informationelle Selbstbestimmung verletzt, denn die im E-Pass gespeicherten Daten können an internationalen Grenzen ausgelesen und in Datenbanken gespeichert werden. Niemand weiß, wer Zugriff darauf hat und was mit den sensiblen biometrischen Daten weiter passiert.

Es ist nicht erkenntlich, welche Vorteile der E-Pass bringt. Um Ausweisdokumente fälschungssicherer zu machen, ist die Speicherung neuer personenbezogener Daten nicht nötig. Soll die Überprüfung der Zusammengehörigkeit von Ausweisträger und Ausweis verbessert werden, ist die Erfassung der Fingerabdrücke aller deutschen Staatsbürger unverhältnismäßig. Professionelle Straftäter oder gar Terroristen können weiterhin auf Ausweisdokumente anderer Staaten ausweichen. Zudem bleibt der Reisepass gültig, wenn der Chip nicht mehr funktioniert.

Doch der E-Pass ist erst der Anfang. Der nächste Schritt ist der biometrische Personalausweis. Biometrische Verfahren und die eingesetzten Funkchips bieten mannigfaltige Möglichkeiten zur Überwachung von Menschen. Und dass einmal installierte Technologien zur Identifizierung und Überwachung die Begehrlichkeiten von Geheimdiensten, Ermittlungsbehörden, aber auch kommerziellen Unternehmen wecken werden, ist kein neues Phänomen.