Informationelle Selbstbestimmung

Entscheidungen des Bundesverfassungsgerichts zur Online-Durchsuchung, Vorratsdatenspeicherung und automatischen Erfassung von Kfz-Kennzeichen

Heiner Adamski


Heiner Adamski

Moderne Gesellschaften sind Informationsgesellschaften. In Behörden unterschiedlichster Art – von Einwohnermeldeämtern bis zu Nachrichtendiensten – und in fast allen Bereichen der wissenschaftlichen Forschung und der Wirtschaft werden die Möglichkeiten der Erfassung und Bearbeitung von Daten durch Maschinen (Computer) genutzt. In der Privatsphäre vieler Menschen ist der Computer ebenfalls ein selbstverständliches Arbeitsinstrument. Ihm wird vieles anvertraut. Festplatten sind oft eine Art Dossier über die Nutzer.

Der Einsatz von Computern ist sinnvoll. Die elektronische Datenverarbeitung hat aber auch eine andere Dimension: Durch Sammlungen und Verknüpfungen von Informationen kann ein konzentriertes personenbezogenes Wissen entstehen. Dieses Wissen ist Macht – und Macht kann Freiheit nicht nur schützen. Macht kann Freiheit auch bedrohen. Es ist möglich, dass in Behörden und Verwaltungen Daten gesammelt werden und die Betroffenen davon keine Kenntnis haben bzw. nur wissen, dass Daten gespeichert, verarbeitet sowie ausgetauscht und verknüpft werden können. Die Möglichkeiten dazu und erst recht die Erfassung von Daten gegen den Willen der betroffenen Personen können beruflich und privat zu Einengungen führen. Wenn jemand weiß, dass er beobachtet und kontrolliert wird oder werden kann, dann verhält er sich – obwohl seine Absichten legal und legitim und eventuell sogar hochmoralisch sind – vielleicht doch anders: er fühlt und verhält sich nicht frei. Es kann sogar zu einer Einschränkung der staatlich zu garantierenden Freiheitsrechte (Grundrechte) des Individuums gegenüber der Staatsmacht durch den Staat und dadurch zu einer Bedrohung der Freiheitsrechte durch den Staat kommen. Zu diesen Rechten gehören unter anderem die Achtung und der Schutz der unantastbaren Würde des Menschen durch alle staatliche Gewalt (Art. 1 GG), das Recht auf die freie Entfaltung der Persönlichkeit (Art. 2 GG), das Recht auf die Meinungs- sowie Informations- und Pressefreiheit, das Recht auf die Freiheit der Kunst und der Wissenschaft, das Recht auf das Post- und Fernmeldegeheimnis und das Recht auf die Unverletzlichkeit der Wohnung (Art. 13 GG). Diese Rechte sind auch so zu verstehen, dass der einzelne Mensch selber bestimmen kann, welches Wissen

Gesellschaft – Wirtschaft – Politik (GWP) Heft 2/2008, S. 259-268

er über sich preisgibt und eben nicht einem „wissensdurstigen“ Staatsapparat oder anderen Institutionen oder Organisationen ausgeliefert ist. Bürger werden in ihren Rechten beeinträchtigt, wenn in einer für sie unkontrollierbaren Weise sie betreffende Daten gesammelt, verarbeitet und weitergegeben werden und dabei – was nach den Vorstellungen mancher Regierungskreise und Parlamente (Gesetzgeber) rechtlich möglich sein soll – etwa zur Gefahrenabwehr sogar Festplatten von dienstlichen und privaten Computern ausgespäht und über die Erfassung von Telekommunikationsdaten und Kfz-Kennzeichen Bewegungsabläufe bzw. Kommunikationsbeziehungen festgestellt werden. Durch die Möglichkeiten der Sammlung von Informationen – der Sammlung von Wissen über Menschen – hat der alte Satz „Wissen ist Macht“ des englischen Juristen, Philosophen und Staatsmanns Francis Bacon eine zu seiner Zeit (1561-1626) ungeahnte Bedeutung bekommen.

Probleme der Erfassung und des Umgangs mit personenbezogenen Daten waren in den letzten Jahren mehrfach Gegenstand von Verfahren vor dem Bundesverfassungsgericht. Dabei hat das Gericht 1983 ein Recht auf „informationelle Selbstbestimmung“ begründet. In den ersten Monaten dieses Jahres hat es wichtige Entscheidungen zur Online-Durchsuchung, zur sog. Vorratsdatenspeicherung und zur automatischen Erfassung von Kfz-Kennzeichen verkündet. In allen Fällen hat es den Vorstellungen mancher Politiker von gesetzlich fixierten weiten staatlichen Zugriffsmöglichen auf Daten widersprochen und Grenzen gezogen.

I. Historische Aspekte und die Begründung des Rechts auf informationelle Selbstbestimmung durch das Bundesverfassungsgericht

Auseinandersetzungen um den Datenschutz reichen bis in die 60er Jahre des vorigen Jahrhunderts. In den USA gab es damals Planungen der Regierung zur Erfassung aller amerikanischen Staatsbürger in einer Datenbank des Statistischen Bundesamtes. Dieses Vorhaben wurde von der Bevölkerung als unverhältnismäßiger Eingriff in die Privatsphäre empfunden und diskutiert. Dabei wurde aufgedeckt, dass die Armee bereits riesige Datensammlungen über politisch verdächtige Personen angelegt hatte und dass es in Auskunfteien massenhafte Sammlungen von Daten persönlichster Natur gab. 1974 wurde dann in den USA ein Privatsphärengesetz (Privacy Act) erlassen, das die Regierung zur Einhaltung von Grundprinzipien zur Sicherung der Privatsphäre verpflichtet (die Gesetzgebung wurde aber nicht auf Privatunternehmen ausgedehnt; dies hat dazu geführt, dass es heute beim „Export“ von Daten an amerikanische Unternehmen aus Ländern mit Datenschutz Probleme des Schutzes dieser Daten gibt).

In den folgenden Jahren hat dann der Datenschutz in Informationsgesellschaften Bedeutung gewonnen. 1980 hat die OECD Empfehlungen über „Leitlinien für den Schutz des Persönlichkeitsbereichs und grenzüberschreitenden Verkehr personenbezogener Daten“ vorgelegt. 1981 hat der Europarat in einer Konvention 108 ein „Übereinkommen zum Schutz des Menschen bei der auto-

matischen Verarbeitung personenbezogener Daten“ beschlossen. 1990 haben die Vereinten Nationen „Richtlinien betreffend personenbezogene Daten in automatisierten Dateien“ verabschiedet. Im Jahr 2000 wurde der Datenschutz auch in die Charta der europäischen Grundrechte (die mit Inkrafttreten des EU-Verfassungsvertrages rechtsverbindlich werden soll) aufgenommen. In Artikel 8 heißt es: „Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.“

In der Bundesrepublik Deutschland sind 1978 das erste Bundesdatenschutzgesetz und bis 1981 auch in den Ländern Landesdatenschutzgesetze in Kraft getreten (in Hessen gab es ein solches Gesetz aber schon 1970). Ein rechtspolitisch wichtiger Schnittpunkt war das Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz (1) aus dem Jahre 1983. In ihm hat das Gericht ein Recht auf „informationelle Selbstbestimmung“ begründet. Es hat praktisch die Qualität eines Grundrechts. In den Leitsätzen heißt es:

1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

2. Einschränkungen dieses Rechts auf informationelle Selbstbestimmung sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

3. Bei den verfassungsrechtlichen Anforderungen an derartige Einschränkungen ist zu unterscheiden zwischen personenbezogenen Daten, die in individualisierter, nicht anonymer Form erhoben und verarbeitet werden, und solchen, die für statistische Zwecke bestimmt sind. Bei der Datenerhebung für statistische Zwecke kann eine enge und konkrete Zweckbindung der Daten nicht verlangt werden. Der Informationserhebung und -verarbeitung müssen aber innerhalb des Informationssystems zum Ausgleich entsprechende Schranken gegenüberstehen.

II. Aktuelle Entscheidungen

A. Online-Durchsuchung

In dem Verfahren zur Online-Durchsuchung ging es um Verfassungsbeschwerden gegen ein Ende 2006 in Kraft getretenes Änderungsgesetz zum nordrhein-westfälischen Verfassungsschutzgesetz (VSG). Strittig waren die Erlaubnis zur Beobachtung und Aufklärung des Internets (z.B. Sichtung der Internet-Kommunikation) und die Ermächtigung zum heimlichen Zugriff auf informationstechnische Systeme (die sog. Online-Durchsuchung) nach § 5 Abs. 2 Nr. 11 VSG. Die Norm spezifizierte nicht näher, welche Arten von Zugriffen auf informationstechnische Systeme gesetzlich erlaubt sein sollen. Technisch denkbar und unter Ermittlungsgesichtspunkten möglicherweise zielführend könnten diese Zugriffe sein: Der einmalige Zugriff auf die auf der Festplatte des betroffenen Computers gespeicherten Daten; eine kontinuierliche Überwachung der gespeicherten Daten, bei der jede Änderung des Datenbestands mitgeschnitten wird; der Zugriff auf weitere Funktionen des betroffenen Rechners (etwa Mitverfolgung der Tastatureingaben und Zugriff auf über das Internet geführte Telefonate). Weitere Punkte waren die Benachrichtigungspflichten der nachrichtendienstlich „behandelten" Personen bzw. das Unterbleiben der Benachrichtigung gem. § 5 Abs. 3 VSG; die Befugnis zur Erhebung von Kontoinhalten gem. § 5 a Abs. 1 VSG; die Befugnis zur akustischen Wohnraumüberwachung gem. § 7 Abs. 2 VSG; der gem. § 8 Abs. 4 Satz 2 VSG vorgesehene Erhalt personenbezogener Daten in sog. elektronischen Sachakten auch in den Fällen, in denen die zu der betreffenden Person geführten Dateien gelöscht worden sind; die Ermächtigung der Verfassungsschutzbehörde in § 13 VSG, ihre Erkenntnisse in gemeinsamen Dateien nicht nur – wie bereits bisher – mit anderen Verfassungsschutzbehörden, sondern auch mit weiteren Sicherheitsbehörden zu verarbeiten.

Nach Auffassung der Beschwerdeführer verletzt die Online-Durchsuchung das Recht auf Unverletzlichkeit der Wohnung. Viele vertrauliche Informationen, die früher in körperlicher Form in der Wohnung aufbewahrt wurden und damit in den räumlichen Schutzbereich der Wohnung fielen, würden heute auf dem heimischen Computer gespeichert und fielen daher ebenfalls in den Schutzbereich des Art. 13 GG. Die Unverletzlichkeit der Wohnung könne nur unter den Voraussetzungen des Art. 13 Abs. 2 bis 7 GG eingeschränkt werden. Die Online-Durchsuchung werde aber von keiner der dort vorgesehenen Einschränkungsmöglichkeiten erfasst. Darüber hinaus rügten die Beschwerdeführer eine Verletzung des Rechts auf informationelle Selbstbestimmung. Die Regelung über die Online-Durchsuchung wahre weder das Gebot der Normenklarheit noch den Grundsatz der Verhältnismäßigkeit. Soweit § 5 Abs. 2 Nr. 11 VSG das Beobachten des Internets vorsehe, verletze die Norm auch das Fernmeldegeheimnis. Soweit es um die Benachrichtigung des Betroffenen im Anschluss an eine Maßnahme nach § 5 Abs. 2 Nr. 11 VSG geht, sehe § 5 Abs. 3 VSG zu weit reichende Ausnahmen von der Benachrichtigungspflicht vor und sei daher mit der Rechtsschutzgarantie des Art. 19 Abs. 4 GG nicht vereinbar. § 5 a Abs. 1 VSG, der die Erhebung von Konteninhalten regelt, verstoße gegen das Recht auf informationelle Selbstbestimmung. § 7 Abs. 2 VSG entspreche nicht den

Vorgaben, die das Bundesverfassungsgericht in seinem Urteil zur strafprozessualen akustischen Wohnraumüberwachung aufgestellt habe. Es fehle an kernbereichsschützenden Regelungen und Vorschriften zur Kennzeichnung der gewonnenen Daten. § 8 Abs. 4 Satz 2 VSG verletze das Recht auf informationelle Selbstbestimmung, da es an einer Regelung über die Löschung personenbezogener Daten in den Sachakten fehle. § 13 VSG schließlich verstoße gegen das Trennungsgebot zwischen Geheimdiensten und Polizeibehörden und damit gegen das Rechtsstaatsprinzip.

Das Bundesverfassungsgericht hat im Februar 2008 in seinem Urteil dazu (2) Vorschriften zur Online-Durchsuchung und zur Aufklärung des Internet als nichtig erklärt. In den Leitsätzen heißt es:

1. Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

2. Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen.

3. Die heimliche Infiltration eines informationstechnischen Systems ist grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen. Das Gesetz, das zu einem solchen Eingriff ermächtigt, muss Vorkehrungen enthalten, um den Kernbereich privater Lebensgestaltung zu schützen.

4. Soweit eine Ermächtigung sich auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden, ist der Eingriff an Art. 10 Abs. 1 GG zu messen.

5. Verschafft der Staat sich Kenntnis von Inhalten der Internetkommunikation auf dem dafür technisch vorgesehenen Weg, so liegt darin nur dann ein Eingriff in Art. 10 Abs. 1 GG, wenn die staatliche Stelle nicht durch Kommunikationsbeteiligte zur Kenntnisnahme autorisiert ist. Nimmt der Staat im Internet öffentlich zugängliche Kommunikationsinhalte wahr oder beteiligt er sich an öffentlich zugänglichen Kommunikationsvorgängen, greift er grundsätzlich nicht in Grundrechte ein.

Im Urteil wird für Recht erkannt:

1. § 5 Absatz 2 Nummer 11 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen ... ist mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Ab-

satz 1, Artikel 10 Absatz 1 und Artikel 19 Absatz 1 Satz 2 des Grundgesetzes unvereinbar und nichtig.

2. Damit erledigen sich die von den Beschwerdeführern gegen § 5 Absatz 3 und § 17 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen erhobenen Rügen.

3. Die Verfassungsbeschwerde ... wird zurückgewiesen, soweit sie gegen § 5a Absatz 1 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen gerichtet ist.

4. Im Übrigen werden die Verfassungsbeschwerden verworfen.

In einer zentrale Aussage zu den Gründen sagt das Bundesverfassungsgericht: „Der Grundrechtseingriff, der in dem heimlichen Zugriff auf ein informationstechnisches System liegt, entspricht im Rahmen einer präventiven Zielsetzung angesichts seiner Intensität nur dann dem Gebot der Angemessenheit, wenn bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen, selbst wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt. Zudem muss das Gesetz, das zu einem derartigen Eingriff ermächtigt, den Grundrechtsschutz für den Betroffenen auch durch geeignete Verfahrensvorkehrungen sichern."

B. Vorratsdatenspeicherung

Das Verfahren zur Vorratsdatenspeicherung betraf das Gesetz zur Neuregelung der Telekommunikationsüberwachung vom Dezember 2007. Mit dem Gesetz wird unter anderem die Richtlinie der Europäischen Union über die Vorratsdatenspeicherung in deutsches Recht umgesetzt. Gegenstand einer dazu erhobenen Verfassungsbeschwerde waren die neu geschaffenen §§ 113a und 113b Telekommunikationsgesetz (TKG). § 113a TKG regelt die Speicherungspflicht für Daten. Danach werden Anbieter von Telekommunikationsdiensten verpflichtet, bestimmte Verkehrs- und Standortdaten, die bei der Nutzung von Telefon, Handy, E-Mail und Internet anfallen, für einen Zeitraum von sechs Monaten zu speichern. 113b TKG regelt die Verwendung der gespeicherten Daten. Danach kann der bevorratete Datenbestand zum Zwecke der Verfolgung von Straftaten, der Abwehr erheblicher Gefahren für die öffentliche Sicherheit und der Erfüllung nachrichtendienstlicher Aufgaben abgerufen werden. Die Norm enthält keine eigenständige Abrufbefugnis, sondern setzt gesonderte gesetzliche Bestimmungen über einen Datenabruf unter Bezugnahme auf § 113a TKG voraus. Bislang nimmt lediglich die Strafprozessordnung (§ 100g StPO) auf § 113a TKG Bezug und ermöglicht zum Zweck der Strafverfolgung ein Auskunftsersuchen über solche Telekommunikations-Verkehrsdaten, die ausschließlich aufgrund der in § 113a TKG geregelten Bevorratungspflicht gespeichert sind. Der Antrag der Beschwerdeführer, §§ 113a, 113b TKG im Wege der einstweiligen Anordnung bis zur Entscheidung über die Verfassungsbeschwerde außer Kraft zu setzen, hatte teilweise Erfolg. Im Beschluss des Bundesverfassungsgerichts vom März 2003 (3) heißt es:

1. § 113b Satz 1 Nummer 1 des Telekommunikationsgesetzes in der Fassung des Gesetzes vom 21. Dezember 2007 ... ist bis zur Entscheidung in der Hauptsache nur mit folgenden Maßgaben anzuwenden: Aufgrund eines Abrufersuchens einer Strafverfolgungsbehörde nach § 100g Absatz 1 der Strafprozessordnung, das sich auf allein nach § 113a des Telekommunikationsgesetzes gespeicherte Telekommunikations-Verkehrsdaten bezieht, hat der durch das Abrufersuchen verpflichtete Anbieter von Telekommunikationsdiensten die verlangten Daten zu erheben. Sie sind jedoch nur dann an die ersuchende Behörde zu übermitteln, wenn Gegenstand des Ermittlungsverfahrens gemäß der Anordnung des Abrufs eine Katalogtat im Sinne des § 100a Absatz 2 der Strafprozessordnung ist und die Voraussetzungen des § 100a Absatz 1 der Strafprozessordnung vorliegen. In den übrigen Fällen des § 100g Absatz 1 der Strafprozessordnung ist von einer Übermittlung der Daten einstweilen abzusehen. Der Diensteanbieter hat die Daten zu speichern. Er darf die Daten nicht verwenden und hat sicherzustellen, dass Dritte nicht auf sie zugreifen können.

2. Die Bundesregierung hat dem Bundesverfassungsgericht zum 1. September 2008 nach Maßgabe der Gründe über die praktischen Auswirkungen der in § 113a des Telekommunikationsgesetzes vorgesehenen Datenspeicherungen und der vorliegenden einstweiligen Anordnung zu berichten. Die Länder und der Generalbundesanwalt haben der Bundesregierung die für den Bericht erforderlichen Informationen zu übermitteln.

C. Automatisierte Erfassung von Kfz-Kennzeichen

Das Verfahren zur automatisierten Kfz-Kennzeichenerfassung betraf Verfassungsbeschwerden gegen polizeigesetzliche Ermächtigungen zur automatisierten Erfassung von Kraftfahrzeugkennzeichen auf öffentlichen Straßen und Plätzen zum Zwecke eines elektronischen Abgleichs mit dem Fahndungsbestand. Angegriffen wurden § 14 Abs. 5 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) und § 184 Abs. 5 des Allgemeinen Verwaltungsgesetzes für das Land Schleswig-Holstein (Landesverwaltungsgesetz – LVwG –). Der technische Vorgang sieht so aus: Die Fahrzeuge werden durch stationäre Kameras oder mit mobilen Systemen auf Parkplätzen oder im fließenden Verkehr optisch erfasst. Dann wird über eine Software die Buchstaben- und Zeichenfolge des amtlichen Kennzeichens ermittelt. Die Kennzeichen werden automatisch mit dem Fahndungsbestand abgeglichen. Wenn ein Kennzeichen im Fahndungsbestand enthalten ist, werden die betreffenden Informationen gespeichert.

Die Beschwerdeführer – die regelmäßig auf öffentlichen Straßen in dem jeweiligen Bundesland unterwegs sind – sahen sich in ihrem Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG verletzt. Die angegriffenen Vorschriften hielten sie für zu unbestimmt. Insbesondere sahen sie den Verwendungszweck für erlangte Informationen nicht hinreichend klar geregelt. Außerdem sahen sie die informationelle Selbstbestimmung in unverhältnismäßiger Weise beschränkt. Mit einem einzigen Erfassungsgerät können ja pro Stunde mehrere tausend Kennzeichen erfasst

werden, so dass die Polizeibehörden voraussetzungslos zu einer massenhaften heimlichen Beobachtung von Unverdächtigen ermächtigt würden.

Das Bundesverfassungsgericht hat im März 2008 in einem Urteil (4) hessische und schleswig-holsteinische Vorschriften zur automatisierten Erfassung von Kfz-Kennzeichen für nichtig erklärt. In den Leitsätzen heißt es:

1. Eine automatisierte Erfassung von Kraftfahrzeugkennzeichen zwecks Abgleichs mit dem Fahndungsbestand greift dann, wenn der Abgleich nicht unverzüglich erfolgt und das Kennzeichen nicht ohne weitere Auswertung sofort und spurenlos gelöscht wird, in den Schutzbereich des Grundrechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) ein.

2. Die verfassungsrechtlichen Anforderungen an die Ermächtigungsgrundlage richten sich nach dem Gewicht der Beeinträchtigung, das insbesondere von der Art der erfassten Informationen, dem Anlass und den Umständen ihrer Erhebung, dem betroffenen Personenkreis und der Art der Verwertung der Daten beeinflusst wird.

3. Die bloße Benennung des Zwecks, das Kraftfahrzeugkennzeichen mit einem gesetzlich nicht näher definierten Fahndungsbestand abzugleichen, genügt den Anforderungen an die Normenbestimmtheit nicht.

4. Die automatisierte Erfassung von Kraftfahrzeugkennzeichen darf nicht anlasslos erfolgen oder flächendeckend durchgeführt werden. Der Grundsatz der Verhältnismäßigkeit im engeren Sinne ist im Übrigen nicht gewahrt, wenn die gesetzliche Ermächtigung die automatisierte Erfassung und Auswertung von Kraftfahrzeugkennzeichen ermöglicht, ohne dass konkrete Gefahrenlagen oder allgemein gesteigerte Risiken von Rechtsgutgefährdungen oder -verletzungen einen Anlass zur Einrichtung der Kennzeichenerfassung geben. Die stichprobenhafte Durchführung einer solchen Maßnahme kann gegebenenfalls zu Eingriffen von lediglich geringerer Intensität zulässig sein.

IV. Kommentar

In dem freiheitlichen Rechtsstaat Bundesrepublik Deutschland und auch in anderen freiheitlichen Rechtsstaaten zeigen die Gesetzgebungen zur Gefahrenabwehr und Sicherheit, dass der Staat mehr und mehr ein Vorbeugungs- oder Verhütungsstaat (ein Präventivstaat) wird. In Deutschland hat das Bundesverfassungsgericht zwar manche Gesetzgebungen als verfassungswidrig eingestuft und dem Gesetzgeber Schranken und die Bedeutung der informationellen Selbstbestimmung gezeigt, aber insgesamt sind die Sicherheitsgesetze schärfer und damit die Möglichkeiten zur Beobachtung und Erfassung größer geworden. Beispielsweise darf der Geheimdienst seit dem Jahr 2001 mehr polizeiliche Aufgaben wahrnehmen. Er darf ohne Staatsanwalt und ohne Richter mehr Telefone abhören und auf Daten der Post, der Banken und des Luftverkehrs zugreifen. Es gibt die Biometrik im Pass und im Personalausweis. Die Möglichkeiten der Telefon- und Video-Überwachung sind ausgeweitet worden. Eine Vorrats-

datenspeicherung haben wir auch – über sechs Monate wird gespeichert, wer mit wem von wo aus telefoniert, wer an einem Chat teilnimmt und wer welche Internetseiten aufruft. Damit werden zum Schutz der Freiheit Freiheitsrechte des Bürgers eingeschränkt. Das geltende Recht und die Rechtsprechung dazu sind teilweise präzise und teilweise ungenau. Die Rechtslage und auch die rechtspolitischen Diskussionen wirken undurchschaubar. Der Bürger, der nichts zu verbergen hat, sei von all dem – so wird oft behauptet – nicht betroffen; tatsächlich ist es aber so, dass viele, vielleicht sogar alle Bürger erstens verunsichert sind und zweitens etwas zu verbergen haben: ihre ganz normale private Sphäre. Wer möchte sich in dieser Sphäre beobachten und kontrollieren lassen? Wer möchte akzeptieren, dass die Grenzen zwischen Verdächtigen und Unverdächtigen und zwischen Unschuldigen und Schuldigen durchlässiger werden? Wer möchte akzeptieren, dass der Einzelne zunächst als Risikofaktor gilt und dass er es sich – ohne einen konkreten Anlass geliefert zu haben – gefallen lassen muss, dass er zur Sicherheit überwacht wird? Wer möchte akzeptieren, dass der Einzelne als potentiell verdächtig gilt, bis sich durch Maßnahmen der Überwachung und Kontrollen seine Entlastung ergibt? Wenn das akzeptiert wird, dann wird das bisherige Prinzip umgekehrt: Der Bürger wurde in Ruhe gelassen, wenn er keinen Anlass für staatliches Eingreifen gegeben hatte. Er konnte durch sein eigenes Verhalten Distanz zum Staat begründen. Die „neue Logik“ ist anders und kann – wenn wir sie zu Ende denken – zur Vorbeugehaft führen. Viele Bürger werden angesichts dieser Entwicklungen unruhig; jedenfalls zeigt die Tatsache, dass die Verfassungsbeschwerde gegen die Vorratsdatenspeicherung von 30.000 Bürgern eingereicht wurde, dass es in der Bevölkerung ein Unbehagen gegen politische Planungen gibt, in denen Recht in diffuser Weise zum Kampf gegen „das Böse“ instrumentalisiert wird, und dass es zugleich ein gewisses Vertrauen in das Bundesverfassungsgericht gibt.

Das Urteil zur Online-Durchsuchung hat Bedeutung für die gesamte Gesetzgebung in Deutschland. Es hat erneut deutlich gemacht, dass Gesetze nicht so „weit“ gefasst werden dürfen, wie manche Sicherheitspolitiker es gern hätten; es hat erneut deutlich gemacht, dass der Staat Grundrechte nicht gewährt, sondern die Freiheitssphäre der Bürger aktiv schützen muss. Die Richter haben die Online-Durchsuchung aber nicht als verfassungswidrig beurteilt, sondern aufgezeigt, ob und in welchem Umfang Online-Durchsuchungen möglich werden können. Das Ausspähen der Festplatte eines Computers ist nur noch zulässig, wenn „tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen“. Das ist einerseits ein Fortschritt. Andererseits ist aber schon absehbar, dass es um die Auslegung des Begriffes „wichtiges Rechtsgut“ Streit geben wird. Es ist auch die grundsätzliche Frage zu stellen, ob ein solch heimliches Vorgehen des Staates mit Grundprinzipien unserer Verfassung wirklich vereinbar ist. So ist nur wenige Tage nach der Einigung der Bundesregierung auf Online-Durchsuchungen ein neuer Streit über den Anti-Terror-Kampf ausgebrochen: Die Pläne zur Videoüberwachung von Wohnungen Unverdächtiger im neuen BKA-Gesetz lösten erhebliche Bedenken in der SPD und Proteste der Opposition aus. Die Grünen sprachen von „Überwachungswahn“. Der frühere Innenminister Gerhart Baum – der zu den Klägern gegen die On-

line-Durchsuchung gehört – drohte mit einer neuen Klage vor dem Bundesverfassungsgericht. Er sieht den „Inbegriff der Privatheit“ gefährdet.

Die Entscheidung über die Vorratsdatenspeicherung ist noch nicht endgültig. Die verfügte Beschränkung der Weitergabe der Daten auf die Verfolgung schwerer Straftaten zeigt, dass die Richter hier einen gravierenden Grundrechtseingriff sehen. Die Investitionskosten für die Vorratsdatenspeicherung betragen übrigens nach Angaben des Verbandes der deutschen Internetwirtschaft (eco) ca. 330 Millionen Euro. Hinzu kommen jährliche Unterhaltskosten von ca. 50 Millionen Euro. Sie wären wohl von den Kunden zu tragen. Interessant ist dazu eine 500 Seiten umfassende Studie „Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO“ des Max-Planck-Instituts für Strafrecht. Die Wissenschaftler kommen zu dem Schluss, dass durch die Speicherung der Verbindungsdaten für sechs Monate die Aufklärungsquote von Verbrechen nur um 0,002 Prozent gesteigert würde. Die Studie ist hier veröffentlicht: http://www.vorratsdatenspeicherung.de/images/ mpi-gutachten.pdf

Das Urteil zur automatischen Erfassung von Kfz-Kennzeichen war für Fachleute keine Überraschung. Es war auch von denen erwartet worden, die für mehr Befugnisse der Polizei eintreten. Aus der Begründung des Urteils kann der Schluss gezogen werden, dass das Bundesverfassungsgericht bei Fragen mit Grundrechtsrelevanz das Verhältnis zwischen EU-Vorgaben und deutscher Rechtsprechung genauer betrachten wird. Dies könnte damit zusammenhängen, dass es ein Missfallen der Richter gibt, wenn versucht wird, mit einem verfahrenstechnischen Trick – auf dem Umweg über EU-Richtlinien – den vergleichsweise hohen Datenschutz-Standard in Deutschland zu reduzieren. In Großbritannien wird die Erfassung der Kennzeichen unter dem Titel „automatic number plate recognition“ (ANPR) flächendeckend angewendet. In Frankreich wird die allgegenwärtige automatisierte Kontrolle der Fahrzeuge ebenfalls eingesetzt. Vermutlich würde das Bundesverfassungsgericht deutsche Politiker korrigieren, wenn die britischen oder französischen Standards der Polizeigesetze zum Maßstab europäischen Rechts gemacht würden und deutsche Politiker dann meinen, dass sie auch im deutschen Recht umgesetzt werden müssen.

Angesichts der Problemlagen bei der Gefahrenabwehr und Sicherheit stellt sich für alle Bürger die Frage, wie eine Politik aussehen kann, die Sicherheit und Recht und Freiheit sichert und die dem Bürger eben auch Sicherheit im Recht gibt. Für die politische Bildung ist dazu die Streitschrift eines fachlich (juristisch) kompetenten engagierten Journalisten nützlich: Heribert Prantl: Der Terrorist als Gesetzgeber (München 2008). Prantl argumentiert manchmal dramatisch – aber er verteidigt immer die bürgerlichen Freiheiten. Das ist auch eine Hauptaufgabe der politischen Bildung.

Anmerkungen

1 Az.: 1 BvR 209/83;
2 Az.: 1 BvR 370/07; 1 BvR 595/07
3 Az.: 1 BvR 256/08
4 Az.: 1 BvR 2074/05