Das aktuelle Thema

Rainer Erd
Bundesverfassungsgericht versus Politik

Eine kommentierende Dokumentation der jüngsten Entscheidungen zu drei Sicherheitsgesetzen

Der gezielte Angriff von zwei Flugzeugen auf die beiden Türme des New Yorker World Trade Center am 11. September 2001 hatte entscheidende Folgen für die Rechtsstaats-Diskussion in der Bundesrepublik. Schon immer waren die Interpreten des Grundgesetzes mit der Aufgabe befasst, zwischen Freiheit und Sicherheit eine Balance zu finden. Doch mit dem New Yorker Ereignis haben die für freiheitsbegrenzende Sicherheit argumentierenden Politiker mehr Aufmerksamkeit und normatives Gewicht beansprucht. Als Repräsentanten einer solchen Politik stehen zwei Innenminister: der ehemalige Bürgerrechtler und nach einer Mitgliedschaft bei den GRÜNEN ins konservative Lager der Sozialdemokratie abgewanderte Otto Schily und der gegenwärtige CDU-Innenminister Wolfgang Schäuble. Beide Politiker setzten im Parlament rechtliche Regelungen durch, die der Sicherheit der Bürger dienen sollten (wie die gesetzliche Regelung zur Rasterfahndung und das Luftsicherheitsgesetz), von denen Kritiker aber behaupteten, sie höhlten zunehmend die Grundlagen des Rechtsstaats aus. Viele dieser Gesetze oder Gesetzesvorlagen hatten die Erhebung und Kontrolle personenbezogener Daten zum Ziel. Das ist in einer Gesellschaft, in der Informationen zu einer zentralen Ressource geworden sind, nicht überraschend. Mit der Verbreitung drahtloser Kommunikation vorwiegend durch das Internet und den Mobilfunk sind diese Medien auch von denen genutzt worden, die terroristische Aktivitäten vorbereiten oder betreiben. Kein Wunder also, dass sicherheitsorientierte Politiker von der Kontrolle und Überwachung dieser Medien Wunder im Kampf gegen den internationalen Terrorismus erwarteten.

Wenngleich es verschwörungstheoretischem Denken entspräche, wollte man mehrere gesetzgeberische und administrative Aktivitäten auf Bundes- und auf Länderebene als eine konzertierte Aktion betrachten, lässt sich doch nicht übersehen, dass die Grundgedanken vieler Initiativen identisch oder ähnlich waren. Einem als stets präsent dargestellten Feind, dem internationalen Terrorismus, stellte man ein neues rechtliches Instrumentarium gegenüber, das vorwiegend auf die Erhebung und Verwertung personenbezogener Daten zielte. Für die auf diese Weise erzielbare *Sicherheit* für den Bürger vor dem allgegenwärtigen Feind, so suggerierte man, sei die *Einschränkung von Freiheitsrechten* ein kleines, wenn nicht gar vernachlässigbares Übel. So entwickelte sich in der BRD seit Ende 2001 ein politisches Klima, das von jedem Bürger eine auf Dauer gestellte

Sicherheitslast einforderte, die dazu dienen sollte, die »Freiheit in Sicherheit« zu verteidigen.[1]

Nun führen in der Regel Verschiebungen von politischen und rechtlichen Diskussionen zu extrem konservativen Konzeptionen zu Reaktionen, die die Ursprungsidee des Rechtsstaats gegen seine Kritiker verteidigen. In der links-liberalen publizistischen und juristischen Öffentlichkeit entwickelte sich so eine Gegenposition gegen den maßlosen Konservatismus, die darauf zielte, vorbereitete oder bereits verabschiedete Gesetze, die auf drastische Weise in die Freiheitsrechte der Bürger eingriffen oder eingreifen sollten, als wirkungslose Beruhigungsmanöver eines autoritären Staates darzustellen. Heribert Prantl[2] schildert in seinem jüngsten Buch die Themen und Mechanismen dieser Politik. Neben Journalisten und Politikern, die diese Kontroversen über eine rechtsstaatlich orientierte Sicherheitspolitik in den vergangenen Jahren führten, trat im Frühjahr dieses Jahres eine Institution, ohne die die Sicherheitspolitik der kommenden Jahre eine andere Richtung einnehmen würde: das Bundesverfassungsgericht. Schon in den Urteilen zur Rasterfahndung[3] und zum Luftsicherheitsgesetz[4] gegenüber dem Gesetzgeber eine eher klassische rechtsstaatliche Konzeption vertretend, machte sich das höchste deutsche Gericht zum Fürsprecher einer freiheitlich orientierten Sicherheitspolitik, die einem immer maßloser werdenden Gesetzgeber deutliche Grenzen definierte. Im Zentrum der juristischen Diskussionen standen der Datenschutz und die Grundrechte der Persönlichkeitsentfaltung (Art. 2 Abs. 1 GG) und Menschenwürde (Art. 1 Abs. 1 GG).

Das Datenschutzrecht gehört zu den verhältnismäßig jungen Rechtsgebieten. Es gibt bislang wenig höchstrichterliche Rechtsprechung, die meisten Urteile und Beschlüsse hingegen sind von dogmatischer und rechtspolitischer Brisanz. Ob es das Volkszählungsurteil vom 15.12.1983,[5] das Urteil zum Großen Lauschangriff vom 3.3.2004[6] oder der Beschluss zur Rasterfahndung vom 4.4.2006[7] ist, in allen drei Fällen standen schwerwiegende Eingriffe in das Persönlichkeitsrecht einzelner Personen zur Diskussion, die das Bundesverfassungsgericht zu dogmatischen Neubestimmungen anregten. Hatte das Gericht seine Grundsätze zum Datenschutz, insbesondere zum *Recht auf informationelle Selbstbestimmung*, in einer nunmehr 25-jährigen Rechtsprechung eher gemächlich entwickelt, so legte es im Februar/März diesen Jahres geradezu sprunghaft gleich drei Leitentscheidungen vor, in denen es um folgende Themen ging. Die

- *Online-Durchsuchung*, mit der ein Landesgesetzgeber sich die gesetzliche Legitimation für eine Kontroll- und Überwachungspolitik des Bürgers bis in seine intimsten Bereiche hinein verschaffen wollte;
- *Vorratsdatenspeicherung*, die ein besorgtes Parlament aufgrund einer EU-Richtlinie verabschiedet hatte und die jeden Bürger zum potentiell Verdächtigen machte, bis seine Unschuld bewiesen werden konnte und

1 Zu dieser Problematik vgl. folgende Beiträge in der Kritischen Justiz: Markus Krajewski, Terroranschläge in den USA, 4/2001, 363 ff.; Thomas Groß, Terrorismus und Grundrechte, 1/2002, 1 ff.; Henner Hess, Terrorismus und globale Staatsbildung, 4/2002, 450 ff.; Reinhard Marx, »Globaler Krieg gegen Terrorismus« und territorial gebrochene Menschenrechte, 2/2006, 151 ff.; Andreas Fischer-Lescano, Paradoxien deutscher Sicherheitspolitik, 1/2004, 67 ff.; Bernhard Haffke, Vom Rechtsstaat zum Sicherheitsstaat, 1/2005, 17 ff.

2 Heribert Prantl, Der Terrorist als Gesetzgeber. Wie man mit Angst Politik macht, München 2008.

3 Boris A. Bischof, Europäische Rasterfahndung, KJ 4/2004, 361 ff.

4 Wolfgang Harke, Die Entscheidung des Bundesverfassungsgerichts zum Luftsicherheitsgesetz, KJ 2/2006, 179 ff.

5 BVerfG, Urt. v. 15. Dezember 1983 – 1 BvR 209/83 u. a. –, BVerfGE 65, 1.

6 BVerfG, Urt. v. 3. März 2004 – 1 BvR 2378/98, 1 BvR 1084/99 -, BVerfGE 109, 279.

7 BVerfG, Beschl. v. 4. April 2006 – 1 BvR 518/02 –, BVerfGE 115, 320.

- *automatisierte Kennzeichenerfassung von PKW* in zwei Bundesländern, die von dem Gedanken getragen war, eine umfassende Überwachung und Kontrolle des mobilen Verhaltens aller Bürger könne Aufschluss über mögliche terroristische Aktivitäten geben.

Was als breit angelegte gesetzgeberische Aktivität begann, ist nach den Entscheidungen des Bundesverfassungsgerichts, das sich wie einer Konzeption folgend an der Idee der »Balance zwischen Freiheit und Sicherheit« orientierte,[8] wieder an den Gesetzgeber zurückverwiesen worden mit dem Hinweis, bei einer Neufassung der für nichtig erklärten Gesetzesteile den Freiheitsgedanken und das Verhältnismäßigkeitsprinzip, vor allem nach einer neu entwickelten Dogmatik im Persönlichkeitsrecht strikter zu beachten. Dass die Rechtsprechung bereits politische Konsequenzen hatte, wird in der Entscheidung der Bundesregierung sichtbar, die Möglichkeit der Online-Durchsuchung im Gesetz über das Bundeskriminalamt (BKAG) – im Gegensatz zum vorherigen Entwurf des Innenministers – nun streng nach den Regeln zu gestalten, die das Bundesverfassungsgericht in seinem Urteil entwickelt hat.[9]

1. Online-Durchsuchung

Das Urteil zur Online-Durchsuchung wird wie die Entscheidung zur Volkszählung von 1983 in die Geschichte der Verfassungsrechtsprechung eingehen.[10] Vor allem deshalb, weil es einer Politik, die seit den dramatischen Ereignissen am 11. September 2001 in New York nichts unversucht ließ, im Namen der Sicherheit der Bürger Freiheitsrechte einzuschränken, beachtliche Schranken zu setzen versucht. Langfristig wird das Urteil deshalb von allergrößter Bedeutung sein, weil es mit dem neu entwickelten Grundrecht auf *»Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme«* einen Begriff geschaffen hat, der zukünftig alle leichtfertigen Versuche abbremsen sollte, in Computer von Personen einzudringen, um dort gespeicherte Daten zu durchsuchen. In geradezu peniblen empirischen Schritten geht das Gericht auf die technischen Möglichkeiten von Personalcomputern ein (die es mit anderen technischen Geräten, die vergleichbare Datenmengen speichern, wie Handy und elektronischem Terminkalender gleichsetzt), interpretiert diese auf ihre Bedeutung für die Persönlichkeitsentwicklung des Bürgers, um sodann in differenzierten Argumentationen das 1983 entwickelte »Recht auf informationelle Selbstbestimmung« auf die technischen Gegebenheiten des 21. Jahrhunderts anzuwenden und zu erweitern.

Mit dem *»Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme«*, das das Bundesverfassungsgericht aus dem *»Recht auf informationelle Selbstbestimmung«* herleitet, passt es das Persönlichkeitsrecht an die neuen technischen Entwicklungen der vergangenen Jahre an. Im Gegensatz zum Gesetzgeber, dem das Persönlichkeitsrecht des Grundgesetzes immer wieder zur lästigen Schranke hoheitlichen Handelns zu werden scheint, argumentiert das Bundesverfassungsgericht konsequent im Interesse des Schutzes der Persönlichkeit und seiner Freiheitsbewahrung angesichts einer umfassender werdenden Technik, die es erlaubt, Daten aus den intimsten Berei-

8 So der Berichterstatter des für die drei Entscheidungen zuständigen Ersten Senats, Wolfgang Hoffmann-Riem, in der Süddeutschen Zeitung vom 12./13. April 2008.
9 Frankfurter Allgemeine Zeitung vom 16. April 2008.
10 BVerfG, Urt. v. 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07 –, NJW 2008, 822.

chen der Bürger zu speichern und damit für einen informationshungrigen Staat greifbar zu machen. Man muss dem Bundesverfassungsgericht bescheinigen, dass es die Bürger der Bundesrepublik vor dem unersättlichen Datenhunger eines Staates bewahren will, der meint, die beste Garantie für die Freiheit der Bürger sei deren Aushöhlung. Dass solche Befürchtungen zur Zeit geringer geworden sind, ist dem Bundesverfassungsgericht zu verdanken, das Einschränkungen des Persönlichkeitsrechts an relativ strenge Bedingungen geknüpft hat, die präzise gesetzlich zu definieren sind, dem Grundsatz der Verhältnismäßigkeit genügen müssen und letztlich von Richtern zu kontrollieren sind.

Im Online-Durchsuchung-Fall stand eine Norm des nordrhein-westfälischen Verfassungsschutzgesetzes (NRW-VSG) zur Entscheidung. Die gesetzliche Möglichkeit für die Polizei, einen Computer für längere Zeit ohne Kenntnis des Betroffenen heimlich zu beobachten und seine Internetaktivitäten zu verfolgen, hatte der Landesgesetzgeber in § 5 NRW-VSG geschaffen. Dort hieß es in Absatz 2:

> (2) Die Verfassungsschutzbehörde darf nach Maßgabe des § 7 zur Informationsbeschaffung als nachrichtendienstliche Mittel die folgenden Maßnahmen anwenden:
>
> (…)
>
> Nr. 11. heimliches Beobachten und sonstiges Aufklären des Internet, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen, sowie der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel. Soweit solche Maßnahmen einen Eingriff in das Brief-, Post- und Fernmeldegeheimnis darstellen bzw. in Art und Schwere diesem gleichkommen, ist dieser nur unter den Voraussetzungen des Gesetzes zu Artikel 10 Grundgesetz zulässig (…).

§ 5 Abs. 2 Nr. 11 NRW-VSG blieb in seiner datenschutz- und verfassungsrechtlichen Brisanz zunächst wenig beachtet. In den Focus öffentlichen Interesses rückte das NRW-VSG durch die Initiative von Bundesinnenminister Wolfgang Schäuble, der, weit über die nordrhein-westfälische Regelung hinausgehend, sein Ministerium einen Entwurf für die Neufassung des BKAG ausarbeiten und darin einen eigenständigen, hochkomplexen Paragrafen zur Bekämpfung des internationalen Terrorismus einfügen ließ. Der sog. Schäuble-Entwurf vom 11. Juli 2007 gelangte durch eine Indiskretion an die Öffentlichkeit, lenkte nunmehr die Aufmerksamkeit auf die Regelung in Nordrhein-Westfalen und führte in kürzester Zeit zu einer öffentlichen Diskussion und zu Kontroversen innerhalb der Bundesregierung.

Das BKAG regelt bislang die Erhebung personenbezogener Daten durch Behörden in Übereinstimmung mit dem Bundesdatenschutzgesetz und dem Grundgesetz in folgender Weise:

> *§ 20 Datenspeicherung für Zwecke künftiger Strafverfahren*
>
> Unter den Voraussetzungen des § 8 kann das Bundeskriminalamt personenbezogene Daten, die es bei der Wahrnehmung seiner Aufgaben auf dem Gebiet der Strafverfolgung erlangt hat, für Zwecke künftiger Strafverfahren in Dateien speichern, verändern oder nutzen.
>
> *§ 8 Dateien der Zentralstelle*
>
> (1) Das Bundeskriminalamt kann zur Erfüllung seiner Aufgaben nach § 2 Abs. 1 bis 3
> 1. die Personendaten von Beschuldigten und, soweit erforderlich, andere zur Identifizierung geeignete Merkmale,
> 2. die kriminalaktenführende Polizeidienststelle und die Kriminalaktennummer,
> 3. die Tatzeiten und Tatorte und
> 4. die Tatvorwürfe, die Angabe der gesetzlichen Vorschriften und die Bezeichnung der Straftaten
>
> in Dateien speichern, verändern und nutzen.
>
> (…)

Nach § 23 Abs. 1 BKAG sind Datenerhebungen bei solchen Personen erlaubt, die eine Straftat gegen Leib, Leben oder Freiheit einer zu schützenden Person oder eine gemeingefährliche Straftat gegen ein Verfassungsorgan verüben wollen sowie gegen deren Kontakt- und Begleitpersonen. Die Mittel, die eine solche Datenerhebung ermöglichen, regelt § 23 Abs. 2 BKAG im Einzelnen. Im Vergleich zu dem, was der Schäuble-Entwurf vorsieht, muten die gegenwärtig zulässigen Maßnahmen geradezu harmlos an. Das noch gültige BKAG sieht drei besondere Formen der Datenerhebung vor:

1. die längerfristige Observation (mehr als zwei Tage),
2. der heimliche Einsatz technischer Mittel außerhalb der Wohnung durch Bild- und Tonaufnahmen und
3. der Einsatz von Personen außerhalb des Bundeskriminalamts, deren Zusammenarbeit mit dem BKA Dritten unbekannt ist.

Der Einsatz besonderer Mittel wird durch den Leiter der Abteilung Personenschutz beim BKA angeordnet, ist aktenkundig zu machen und auf einen Monat beschränkt. Eine darüber hinausgehende Verlängerung muss richterlich angeordnet werden. Die erhobenen Daten sind unverzüglich zu löschen, wenn der Zweck der Überwachungsmaßnahme erreicht ist. Der Überwachte ist davon zu unterrichten, sofern dies ohne Gefährdung des Zwecks der Maßnahme oder der öffentlichen Sicherheit möglich ist, § 23 Abs. 3, 4 BKAG.

Gegenüber diesem Gesetz sah der Schäuble-Entwurf qualitativ neue Formen der Überwachung vor, indem er einen neuen Tatbestand einführt: die »Abwehr von Gefahren des internationalen Terrorismus«.[11] Wann eine solche Gefahr vorliegt, definiert der Gesetzentwurf nicht, er führt beispielhaft, aber nicht abschließend, § 129a StGB an. Neben der Unbestimmtheit des Tatbestandsmerkmals »Gefahr des internationalen Terrorismus« enthielt der Entwurf in § 20 eine Fülle von Eingriffstatbeständen in die verfassungsrechtlich geschützte Privatsphäre von Verdächtigen.

Der bislang knappe § 20 sollte nach dem Papier vom 11. Juli 2007 durch 25 hochkomplexe Vorschriften geändert werden (§§ 20a–20y). Allein die Fülle neu vorgesehener Möglichkeiten für das Bundeskriminalamt, von denen zwanzig erweiterte Eingriffskompetenzen für den Staat und fünf Schutzregelungen für die Betroffenen enthielten, zeigte, dass dem Entwurf die Idee zugrunde lag, eine lückenlose Überwachung von Personen sei erforderlich, um in Zukunft terroristische Anschläge zu verhindern. Die Anmerkungen der Sachbearbeiter des Entwurfs zu den Folgen der neuen gesetzlichen Regelungen ließen ein gering ausgebildetes Problembewusstsein von den Missbrauchsmöglichkeiten erkennen, die der Gesetzentwurf enthält. So fanden sich unter der Rubrik Folgen für »Bürgerinnen und Bürger« die beiden lapidaren Worte: »keine Auswirkungen«.[12] Die in der Geschichte der Bundesrepublik umfassendste Planung der Erhebung und Weiterverarbeitung personenbezogener Daten von Bürgern bis in ihre intimsten Bereiche hatte aus Sicht der Beamten des Innenministeriums »keine« Auswirkungen. Der den Entwurf öffentlich vertretende Bundesinnenminister Schäuble sollte bald nach seinem Bekanntwerden erfahren, dass viele Bürgerinnen und Bürger und auch Mitglieder des Bundeskabinetts wie insbesondere die Justizministerin Brigitte Zypries dies vollständig anders sahen.

Die vielfältigen kritischen Stimmen, die sich gegen den Entwurf eines neuen BKA-Gesetzes richteten, konzentrierten sich vorwiegend auf die Regelungen,

11 § 4a Entwurf.
12 Entwurf vom 11. Juli 2007, S. 2.

die einen Einsatz technischer Mittel zur Überwachung von Computern vorsehen. Einschlägig dafür war in dem Entwurf § 20k, der die Möglichkeit vorsah, ohne Wissen des Betroffenen Daten von dessen Computer zu erheben. Im Zweifel sollte die Anordnung dieser Maßnahme ohne richterliche Entscheidung durch den Präsidenten des Bundeskriminalamts oder seinen Stellvertreter getroffen werden können.[13]

§ 20k Heimlicher/Verdeckter Zugriff auf informationstechnische Systeme

(1) Das Bundeskriminalamt darf ohne Wissen des Betroffenen durch den automatisierten Einsatz technischer Mittel aus informationstechnischen Systemen Daten erheben, soweit die Abwehr der dringenden Gefahr oder die Verhütung von Straftaten gemäß § 4a Abs. 1 Satz 2 auf andere Weise aussichtslos ist oder wesentlich erschwert wäre. Die Maßnahme darf sich richten gegen:

1. den entsprechend § 17 oder 18 des Bundespolizeigesetzes Verantwortlichen (Gefahrverursacher, R. E.)
2. eine Person, die für den Verantwortlichen bestimmte der von diesem herrührende Informationen entgegennimmt oder weitergibt, oder
3. eine Person, deren informationstechnisches System ein Verantwortlicher nutzt.

Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

Diese Regelung zielte nicht nur auf mutmaßliche Terroristen, sondern auch auf die Empfänger von Informationen. Das können die unterschiedlichsten Personen sein, für die gesetzliche Verschwiegenheitspflichten gelten: Journalisten, Rechtsanwälte, Geistliche, Ärzte oder Therapeuten. Mag man bei der Formulierung »die für den Verantwortlichen bestimmte Informationen entgegennimmt oder weitergibt« noch einen Zusammenhang zwischen vermutetem Terrorist und Empfänger annehmen können, so schließt der Begriff »herrührende Informationen« jeden intentionalen Zusammenhang aus. Denn Informationen erhalten Personen auch unerwünscht, die sodann vom BKA heimlich online überwacht werden könnten.

Der inhaltliche Zusammenhang zwischen § 20k des Schäuble-Entwurfs und § 5 NRW-VSG ist offensichtlich. In beiden Regelungen wird einer staatlichen Stelle der Zugriff auf den Computer (»*informationstechnisches System*«) einer Person erlaubt. Aus diesem Grund war für alle Beteiligten des Verfahrens vor dem Bundesverfassungsgericht zum nordrhein-westfälischen VSG offensichtlich, dass das Urteil des Gerichts zugleich auch die zulässigen Möglichkeiten der geplanten bundesweiten Veränderung polizeilicher Überwachungsmöglichkeiten präjudizieren würde.

Aufsehen erregend waren nicht nur das Verfahren, sondern auch die Entscheidungsgründe. Das Bundesverfassungsgericht kreierte, wie bereits im Volkszählungsurteil von 1983, ein neues Recht: das »*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.*« Indem es § 5 Abs. 2 Nr. 11 NRW-VSG wegen Verstoßes gegen Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, Art. 10 Abs. 1 und Art. 19 Abs. 1 Satz 2 GG für nichtig erklärte, entschied es implizit über das Schicksal des Schäuble-Entwurfs.

Im Urteil vom 27.2.2008 entwickelt das Bundesverfassungsgericht, ganz auf der Höhe der Zeit, aus dem Persönlichkeitsrecht das »*Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme*«, umgangssprachlich »Computer-Grundrecht«[14] genannt. Wie schon im Volkszählungsurteil leitet auch hier das Bundesverfassungsgericht das neue Grund-

13 § 20k Abs. 2 S. 2 Entwurf.
14 Heribert Prantl, Süddeutsche Zeitung vom 27.2.2008.

recht aus gesellschaftlichen und technischen Veränderungen her. Waren 1983 im Volkszählungsurteil die »Bedingungen der modernen Datenverarbeitung« das entscheidende Argument für die Begründung des »*Rechts auf informationelle Selbstbestimmung*«, so heißt es nun, einer Lücken schließenden Gewährleistung des allgemeinen Persönlichkeitsrechts bedürfe es,

> »um neuartigen Gefährdungen zu begegnen, zu denen es im Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse kommen kann.«[15]

Um ein *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* zu begründen, muss das Gericht einen Zusammenhang zwischen allgemeinem Persönlichkeitsrecht und der Nutzung informationstechnischer Systeme herstellen. Es tut dies, indem es zeigt, dass moderne Informationstechniken dazu geführt haben, dass der Personalcomputer, in der Mehrheit aller deutschen Haushalte mittlerweile vorhanden, für die Persönlichkeitsentfaltung zunehmend Bedeutung erlangt hat. Sowohl Verbreitung und Leistungsfähigkeit von Personalcomputern sowie ihre Vernetzung eröffnen dem Nutzer – insbesondere durch das Internet –

> »eine unübersehbare Fülle von Informationen, die von anderen Netzrechnern zum Abruf bereit gehalten werden. Es stellt ihm daneben zahlreiche neuartige Kommunikationsdienste zur Verfügung, mit deren Hilfe er aktiv soziale Verbindungen aufbauen und pflegen kann.«[16]

Anerkennt man ein *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, dann muss man es verfassungsrechtlich vor Gefährdungen schützen. Dies tut das Bundesverfassungsgericht, indem es darlegt, welche datenschutzrechtlichen Probleme die Nutzung eines Personalcomputers (PC) zur Folge haben kann. Es sind nicht allein die vom Nutzer erzeugten und gespeicherten Daten, die von anderen abgerufen werden können. Der PC generiert auch eigenständig Daten, die das Verhalten und die Eigenschaften des Nutzers festhalten (z. B. cookies). Auf diese Weise

> »können sich im Arbeitsspeicher und auf den Speichermedien solcher Systeme eine Vielzahl von Daten mit Bezug zu den persönlichen Verhältnissen, den sozialen Kontakten und den ausgeübten Tätigkeiten des Nutzers finden. Werden diese Daten von Dritten erhoben und ausgewertet, so kann dies weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen.«[17]

Vertieft werden diese Gefährdungen bei vernetzten Systemen. Solche Systeme erlauben die Erzeugung, Verarbeitung und Speicherung von noch mehr Daten, sie erhöhen die Möglichkeiten der Erstellung von Persönlichkeitsprofilen eines Nutzers. Die bedeutendste Gefahr, die das Bundesverfassungsgericht sieht, liegt im Ausspähen und Manipulieren von Daten. Aus der Bedeutung informationstechnischer Systeme für die Persönlichkeitsentfaltung und aus ihren Gefährdungen folgert das Gericht, dass ein erheblicher grundrechtlicher Schutzbedarf besteht. Das Telekommunikationsgeheimnis des Art. 10 GG und die Unverletzlichkeit der Wohnung (Art. 13 GG) genügen diesem Schutzbedürfnis nicht hinreichend. Der Regelungsbedarf entsteht daraus, dass Art. 10 GG zwar Inhalte und Umstände der laufenden Kommunikation im Rechnernetz schützt, nicht hingegen die gespeicherten Daten vor einem heimlichen Zugriff. Ebenso enthält Art. 13 Abs. 1 GG Schutzlücken gegenüber Zugriffen auf informationstechnische Systeme, da die Garantie der Unverletzlichkeit der Wohnung nicht die Fälle erfasst, in denen der Eingriff von einem Ort außerhalb der Wohnung erfolgt.

15 BVerfG (Fn. 10), C I 1 a (Rz. 169).
16 BVerfG (Fn. 10), C I 1 b bb (Rz. 176).
17 BVerfG (Fn. 10), C I 1 b cc (1) (Rz. 178).

Auch die Erhebung von Daten eines informationstechnischen Systems durch Infiltration ist nicht durch Art. 13 GG geschützt.

Gewähren weder Art. 10 GG noch Art. 13 GG einen hinreichenden Schutz vor dem heimlichen Zugriff auf informationstechnische Systeme, so ist auch das Recht auf informationelle Selbstbestimmung nicht ausreichend, Bedrohungen des Persönlichkeitsrechts durch Online-Durchsuchungen dogmatisch ausreichend zu bewerten. Deshalb muss es um den bislang in der Rechtsprechung nicht bekannten Grundsatz der »*Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme*« erweitert werden. Wie das *Recht auf informationelle Selbstbestimmung* leitet das Gericht das Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme aus den Art. 2 Abs. 1 i.V.m. Art 1 Abs. 1 GG ab.

Anzuwenden ist das Grundrecht dann,

> »wenn die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Weise enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten. Eine solche Möglichkeit besteht etwa beim Zugriff auf Personalcomputer (...). Der spezifische Grundrechtsschutz erstreckt sich ferner beispielsweise auf solche Mobiltelefone oder elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können.«[18]

Der Grundrechtsschutz umfasst die auf dem Arbeitsspeicher sowie die auf dauerhaften Speichermedien abgelegten Daten.

Doch keine Grundrechtsgewährung ohne Schranken. Eingriffe in das *Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme* zu präventiven wie zu Zwecken der Strafverfolgung hält das Gericht für grundsätzlich zulässig. Der Eingriff muss allerdings auf einer verfassungsmäßigen gesetzlichen Grundlage beruhen. An dieser fehle es aber im zur Entscheidung stehenden Fall, weil die angegriffene Norm des NRW-VSG nicht den Geboten der Normklarheit, Normbestimmtheit und Verhältnismäßigkeit entspreche. § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 NRW-VSG sei folglich verfassungswidrig, weil sich die tatbestandlichen Voraussetzungen der vorgesehenen Maßnahmen dem Gesetz nicht hinreichend entnehmen lassen. Neuartige Ermittlungsmaßnahmen können nicht durch einen schlichten Verweis auf eine andere Norm gerechtfertigt werden, sie müssen vom Gesetzgeber konkret festgelegt werden.

Das Gesetz entsprach weiterhin nicht dem *Grundsatz der Verhältnismäßigkeit*. Zwar ist der heimliche Zugriff auf ein informationstechnisches System geeignet für staatliche Ermittlungsmaßnahmen und er ist auch erforderlich, um Daten von einem System zu erheben. Die *Verhältnismäßigkeit im engeren Sinne* sieht das Bundesverfassungsgericht jedoch deshalb als verletzt an, weil § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 NRW-VSG Grundrechtseingriffe vorsieht, die

> »zu dem öffentlichen Ermittlungsinteresse, das sich aus dem geregelten Eingriffsanlass ergibt, außer Verhältnis stehen. Zudem bedarf es ergänzender verfahrensrechtlicher Vorgaben, um dem grundrechtlich geschützten Interesse des Betroffenen Rechnung zu tragen; auch an ihnen fehlt es.«[19]

Die Entscheidung, Teile des NRW-VSG für verfassungswidrig zu erklären, bedeutet für das Bundsverfassungsgericht aber nicht – hierin zeigt es, wie es die

18 BVerfG (Fn. 10), C I 1 d aa (Rz. 203).
19 BVerfG (Fn. 10), C I 2 b dd. (Rz. 227).

Balance zwischen Freiheit und Sicherheit auszutarieren gedenkt –, Online-Durchsuchungen generell für unzulässig zu halten. Das heimliche Ausspähen eines Computers soll dann zulässig sein, 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.«[20]

Um eine rechtsstaatliche Online-Durchsuchung zu gewährleisten, müssen – das wird für die weitere Diskussion zur gesetzlichen Regelung der Online-Durchsuchung von allergrößter Bedeutung sein – geeignete *verfahrensrechtliche Regelungen* geschaffen werden. Wie solche Verfahrensregelungen auszusehen haben, schreibt das Gericht dem Gesetzgeber vor. Der Verhältnismäßigkeitsgrundsatz erfordert zunächst, dass besondere Anforderungen an den *Anlass des Eingriffs* zu stellen sind. Nicht jede Rechtsgutverletzung erlaubt einen schwerwiegenden Eingriff, sondern dies ist nur dann zulässig, wenn

> »tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen. Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Hierzu zählt etwa auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen. Zum Schutz sonstiger Rechtsgüter Einzelner oder der Allgemeinheit in Situationen, in denen eine existenzielle Bedrohungslage nicht besteht, ist eine staatliche Maßnahme grundsätzlich nicht angemessen, durch die (...) die Persönlichkeit des Betroffenen einer weitgehenden Ausspähung durch die Ermittlungsbehörde preisgegeben wird. Zum Schutz solcher Rechtsgüter hat sich der Staat auf andere Ermittlungsbefugnisse zu beschränken, die ihm das jeweils anwendbare Fachrecht im präventiven Bereich einräumt«.[21]

Ohne tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr will das Gericht einen Eingriff nicht zulassen. Im Einzelnen bedeutet das: Es muss dargetan werden, dass es sich um einen Einzelfall handelt, eine zeitliche Nähe des Umschlagens der Gefahr in einen Schaden besteht und der Verursacher eine individuelle Person ist. Zu den verfahrensrechtlichen Erfordernissen für die Überwachung gehört auch die *richterliche Anordnung*, weil nur diese eine unabhängige und neutrale Kontrolle gewährleistet. Deren Fehlen im nordrhein-westfälischen Gesetz war ein weiterer Grund für die Verfassungswidrigkeit.

Schließlich moniert das Gericht, dass im nordrhein-westfälischen VSG kein Schutzkonzept erkennbar sei, das es ermöglicht, »*kernbereichsrelevante Daten*« nicht zu erheben bzw. – wenn dies technisch nicht möglich ist – ihre sofortige Löschung zu veranlassen. Ein solches »*zweistufiges Schutzkonzept*« sei Voraussetzung für die Verfassungsmäßigkeit einer Online-Durchsuchung. Hier freilich wird sich der Bundesgesetzgeber viel einfallen lassen müssen. Denn auch das Bundesverfassungsgericht hat nicht dargelegt, wie man auf ein informationstechnisches System heimlich zugreifen und zugleich gewährleisten kann, dass keine Daten erhoben und gespeichert werden, die zum Kernbereich der Persönlichkeit gehören. Und wer gewährleistet, dass für den Fall der unzulässigen Erhebung kernbereichsrelevanter Daten diese auch umgehend gelöscht werden?

Nach ausführlichen Begründungen für die Verfassungswidrigkeit der § 5 Abs. 2 Nr. 11 Satz 1 2. Alternative NRW-VSG (»heimlicher Zugriff auf informationstechnische Systeme«) erklärte das Gericht auch die 1. Alternative für verfassungswidrig (»heimliches Aufklären des Internet«). Das ist konsequent, weil damit die Folge eines verfassungswidrigen Zugriffs erfasst wird. Hier sieht das Gericht Art. 10 GG (Telekommunikationsgeheimnis) dann als verletzt an, wenn

20 BVerfG (Fn. 10), C I 2 b dd 2 (Rz. 242).
21 BVerfG (Fn. 10), C I 2 b dd 2 c aa (Rz. 248)

bereits der Eingriff nicht gerechtfertigt war. Weiterhin stellt das Gericht – wie bereits in der Argumentation zur Verfassungswidrigkeit der 2. Alternative – einen Verstoß gegen den Grundsatz der Verhältnismäßigkeit und gegen die Erforderlichkeit von Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung fest. Wie im Falle der verfassungsrechtlichen Prüfung der 2. Alternative hält auch bei der 1. Alternative das Gericht ein »heimliches Aufklären« dann für zulässig, wenn diese nicht in Grundrechte eingreift.
§ 5 Abs. 2 Nr. 11 NRW-VSG, so das Resümee des Gerichts, ist insgesamt verfassungswidrig.

2. *Vorratsdatenspeicherung*

Im Vergleich zur Online-Durchsuchung ist die Vorratsdatenspeicherung ein weniger umfangreicher Eingriff in Datenschutzrechte von Bürgern. Die vom Gesetzgeber im neuen § 113b Satz 1 Nr. 1 Telekommunikationsgesetz (TKG) geschaffene sechsmonatige Vorratsdatenspeicherung ist nicht neu. Vorratsdatenspeicherung gibt es in §§ 96, 97 TKG und in § 15 Abs. 4 Telemediengesetz (TMG).[22] Neu ist, dass alle Betreiber öffentlich zugänglicher Telekommunikationsdienste die entstandenen Verkehrsdaten für einen Zeitraum von *sechs Monaten* speichern müssen und dass die Daten für Zwecke verwendet werden dürfen, für die sie nicht erhoben wurden. Bislang wurde die Speicherdauer von der Zweckverwendung der Daten abhängig gemacht. Waren beispielsweise die Abrechnungen mit Verbindungsnachweis erfolgt, so entfiel der Speicherungszweck. Die neue Regelung des TKG,[23] zurückgehend auf die EG-Richtlinie 2006/24 vom 21. Dezember 2007, hat die Speicherungsdauer demgegenüber anlassunabhängig auf sechs Monate festgelegt und die Verwendungszwecke der Daten erweitert.

> *§ 113a TKG Speicherungspflichten für Daten*
>
> (1) Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ist verpflichtet, von ihm bei der Nutzung seines Dienstes erzeugte oder verarbeitete Verkehrsdaten nach Maßgabe der Absätze 2 bis 5 sechs Monate im Inland oder in einem anderen Mitgliedsstaat der Europäischen Union zu speichern (...).
>
> (2) Die Anbieter von öffentlich zugänglichen Telefondiensten speichern:
>
> 1. die Rufnummer oder andere Kennung des anrufenden und des angerufenen Anschlusses sowie im Falle von Um- und Weiterschaltungen jedes weiteren beteiligten Anschlusses,
> 2. den Beginn und das Ende der Verbindung nach Datum und Uhrzeit unter Angabe der zugrundeliegenden Zeitzone,
>
> (…)
>
> (3) Die Anbieter von Diensten der elektronischen Post speichern:
>
> (...)
>
> (4) Die Anbieter von Internetzugangsdiensten speichern:
>
> (...)

Mit der Neufassung von § 113a TGK hat der Gesetzgeber die Absicht verfolgt, zwar nicht die Inhalte von Kommunikationen, aber sämtliche möglichen *Verbindungsdaten* der telefonischen (einschließlich Mobil- und Internettelefonie) und der Internetkommunikation zu erfassen. Ein vergleichbares Interesse wie bei der Online-Durchsuchung wird erkennbar, mit einem wesentlichen Unter-

22 Vgl. Maximilian Warntjen, Telekommunikationsüberwachung, KJ 3/2005, 276 ff.
23 BGBl I S. 3198.

schied: Nicht die *Kommunikationsinhalte* sind Gegenstand der gesetzlichen Regelung, sondern die *Kommunikationsformen* sollen lückenlos erfasst werden. Für die verfassungsrechtliche Prüfung des Gesetzes wurde nun wichtig, welchen Zwecken diese Daten zugeführt werden sollten.

> *§ 113b Verwendung der nach § 113a gespeicherten Daten*
>
> Der nach § 113a Verpflichtete darf die allein auf Grund der Speicherungsverpflichtung nach § 113a gespeicherten Daten
>
> 1. zur Verfolgung von Straftaten,
> 2. zur Abwehr erheblicher Gefahren für die öffentliche Sicherheit oder
> 3. zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes
>
> an die zuständigen Stellen auf deren Verlangen übermitteln, soweit dies in den jeweiligen gesetzlichen Bestimmungen unter Bezugnahme auf § 113a vorgesehen und die Übermittlung im Einzelfall angeordnet ist; für andere Zwecke mit Ausnahme einer Auskunftserteilung nach § 113 darf er die Daten nicht verwenden. § 113 Abs. 1 Satz 4 gilt entsprechend.

Auch dieser Form der Datenerhebung und -verwertung hat das Bundesverfassungsgericht in seinem Beschluss zur Vorratsdatenspeicherung, der im Rahmen eines Verfahrens einstweiliger Anordnung erging, einen – hier nur vorläufigen – Riegel vorgeschoben.[24] Vorangegangen waren dem Urteil Demonstrationen und Internetproteste gegen die Vorratsdatenspeicherung, wie es sie seit der großen Protestbewegung gegen die Volkszählung 1983 wegen einer Datenschutzfrage nicht mehr gegeben hatte. Wie schon im Urteil zur Online-Durchsuchung legte das Gericht einen strengen Prüfungsmaßstab an und entschied, dass § 113b Satz 1 Nr. 1 TKG bis zur Entscheidung im Hauptsacheverfahren nur eingeschränkt Anwendung finden kann: Es dürfen zwar Daten aufgrund eines Abrufersuchens einer Strafverfolgungsbehörde nach § 100g Abs. 1 StPO von einer Person *erhoben* werden. Die *Übermittlung* dieser Daten an die ersuchende Behörde ist jedoch nur dann zulässig, wenn Gegenstand des Ermittlungsverfahrens eine Katalogtat nach § 100a Abs. 2 StPO ist und die Voraussetzungen des § 100a Abs. 1 StPO vorliegen. In den Fällen des § 100g Abs. 1 StPO ist einstweilen von einer Übermittlung der Daten abzusehen. Darüber hinaus wird die Bundesregierung verpflichtet, dem Bundesverfassungsgericht bis zum 1. September 2008 über die praktischen Auswirkungen der Datenspeicherungen nach § 113a TKG zu berichten.
Konkret bedeutet die Entscheidung, dass die nach § 113a TKG für sechs Monate zu speichernden personenbezogenen Daten nicht für alle Anlässe der Strafverfolgung verwendet werden dürfen, sondern auf bestimmte beschränkt bleiben. Die in § 113b Satz 1 Nr. 1 TKG vorgesehene Datennutzung »zur Verfolgung von Straftaten« wird bis zur Entscheidung über die Verfassungsbeschwerde teilweise ausgesetzt. Die Nachteile der Nutzung solcher Daten sieht das Gericht darin, dass sie

> »Erkenntnisse über das Kommunikationsverhalten und die sozialen Kontakte des Betroffenen (...), gegebenenfalls sogar begrenzte Rückschlüsse auf die Gesprächsinhalte zu ziehen« erlauben, die einen nicht mehr rückgängig zu machenden Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG darstellen. Die demgegenüber möglicherweise entstehenden Nachteile für den Staat an effektiver Strafverfolgung »wiegen allerdings teilweise weniger schwer und sind angesichts des Gewichts der dem Einzelnen und der Allgemeinheit durch den Vollzug des § 113b Satz 1 Nr. 1 TKG drohenden Nachteile hinzunehmen (...).«[25]

Das engagierte Plädoyer des Bundesverfassungsgerichts für die Grundrechte der Bürger und die Entscheidung gegen umfangreiche Möglichkeiten des Staates zur

24 BVerfG, Beschluss v. 11. März 2008 – 1 BvR 256/08 –, DVBl. 2008, 569.
25 BVerfG (Fn. 24), B II 2 b aa 2 (Rz. 156).

Datennutzung resultiert aus einem verfassungsrechtlichen Verständnis, das bereits im Urteil zur Online-Durchsuchung dargetan wurde und sich so beschreiben lässt: Bei der Abwägung zwischen staatlichen Überwachungs- und Kontrollwünschen zur Gewährleistung von Sicherheit und Freiheitsrechten des Bürgers können Freiheitsrechte nur unter exakt definierten Bedingungen eingeschränkt werden.
Welche Datennutzung bleibt nach der einstweiligen Anordnung erlaubt und welche ist unzulässig? Weitergegeben werden dürfen Daten, wenn es um die Verfolgung schwerer Straftaten im Sinne des § 100a Abs. 2 StPO geht (das sind gegen staatliche Institutionen gerichtete Taten, Verstöße gegen das Kinderpornografieverbot, Mord und Totschlag etc.). Einstweilen nicht an Verfolgungsbehörden weitergeleitet werden können Daten, die unterhalb dieser Schwelle liegen (einfache Straftaten). Geschützt vor der Verwertung routinemäßig gespeicherter Daten sind nun Bürger, die in Verdacht stehen, Straftaten begangen zu haben, die rechtlich als nicht »schwer« eingestuft werden. In diesen Fällen, vermutlich der Mehrheit potentieller Datenübermittlungen, hat das Bundesverfassungsgericht das Schutzinteresse des Bürgers gegenüber dem Verfolgungsinteresse des Staates höher bewertet – auch dies ein rechtlicher Sieg der Skeptiker umfassender staatlicher Überwachung.

3. Automatisierte Kennzeichenerfassung

Am selben Tag, an dem das Bundesverfassungsgericht die Vorratsdatenspeicherung begrenzte, erklärte es § 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) wegen Verstoßes gegen Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 des Grundgesetzes für nichtig.[26] Dass Regelungen von drei Landesgesetzen innerhalb von zwei Wochen vom Bundesverfassungsgericht für nichtig erklärt werden, regt zu kritischen Reflexionen über die verfassungsgemäße Verabschiedung von Gesetzen an. Es scheint, als habe die weitverbreitete Sorge vor terroristischen Anschlägen einigen Politikern den Blick auf das Grundgesetz verstellt. So mussten sich die Landesgesetzgeber von Nordrhein-Westfalen, Hessen und Schleswig-Holstein in der Zeit vom 27. Februar bis zum 11. März 2008 von den Karlsruher Richtern Unachtsamkeit in verfassungsrechtlichen Fragen attestieren lassen.
Die Erhebung von Fahrzeugkennzeichen ist nicht neu. In der Vergangenheit ist sie von der Polizei stichprobenartig oder einzelfallbezogen durchgeführt worden. Was es bislang in der Bundesrepublik, abgesehen von der Schleierfahndung, nicht gab, waren *systematische Massenkontrollen ohne konkreten Anlass*. Die hessische Polizei setzte seit Ende Januar 2007 aufgrund neuer gesetzlicher Regelungen im HSOG Kameras zur automatischen Kennzeichenerfassung ein und glich die Daten mit ihrem Fahndungsregister ab. Blieb der Abgleich erfolglos, wurden die Daten aus dem Speicher des Lesegeräts automatisch gelöscht. Im Trefferfall erschienen das erfasste Kennzeichen und das Foto des Fahrers auf einem Laptop der Polizei vor Ort, der diese Daten mit möglichen Fahndungsdaten abglich. Die dafür zur Verfügung stehenden Daten von INPOL und dem Schengener Informationssystem (SIS) betrugen mehr als zwei Millionen, die vorwiegend folgende Anlässe betrafen: »abhanden gekommen durch«, »ohne Haftpflichtversicherung«, »Amts-/Vollzugshilfe«. Gegen diese anlasslose Erhebung von Kfz-Kenn-

26 BVerfG, Beschl. v. 11. März 2008 – 1 BvR 2074/05, 1 BvR 1254/07 –, DVBl. 2008, 575.

zeichen beliebiger Personen (bis zu 3.000 Kennzeichen pro Stunde) richtete sich die Verfassungsbeschwerde, in der vorgetragen wurde, die Erstellung von »Bewegungsprofilen« verstoße gegen das Grundrecht auf informationelle Selbstbestimmung und gegen den Grundsatz der Verhältnismäßigkeit.
Beschränken wir uns auf den hessischen Fall, da er weitgehend dem schleswig-holsteinischen entspricht. § 14 Abs. 5 HSOG sah folgende Regelung vor:

> *§ 14 Datenerhebung und sonstige Datenverarbeitung an öffentlichen Orten und besonders gefährdeten Einrichtungen*
>
> (...)
>
> (5) Die Polizeibehörden können auf öffentlichen Straßen und Plätzen Daten von Kraftfahrzeugkennzeichen zum Zwecke des Abgleichs mit dem Fahndungsbestand automatisiert erheben. Daten, die im Fahndungsbestand nicht enthalten sind, sind unverzüglich zu löschen.

Das Bundesverfassungsgericht erklärte die hessische wie die schleswig-holsteinische automatisierte Datenerfassung für verfassungswidrig, weil sie das allgemeine Persönlichkeitsrecht in seiner Ausprägung als »*Grundrecht auf informationelle Selbstbestimmung*« verletzen. Der Leitlinie seiner bisherigen Rechtsprechung folgend, definiert das Gericht Gefährdungslagen, die bei der elektronischen Datenverarbeitung entstehen aus der unbegrenzbaren Speicher- und Abrufbarkeit von Daten sowie aus vielfältigen Nutzungs- und Verknüpfungsmöglichkeiten. Auf diese Weise könne das grundrechtlich geschützte Geheimhaltungsinteresse Betroffener und seine Verhaltensfreiheit beeinträchtigt werden. Dies geschehe durch das Erfassen des Kennzeichens eines PKW an einem bestimmten Ort. Sichtbar werde dies, wenn infolge der Datenerfassung eine Person von der Polizei angehalten und kontrolliert werde.
Auch bei der Überprüfung der Anforderungen an die Ermächtigungsgrundlage, die einen Eingriff in Form der automatisierten Datenerfassung rechtfertigen, folgt das Gericht seiner bisherigen Rechtsprechung. Die Anforderungen richten sich nach drei Kriterien: der Art und Intensität des Grundrechtseingriffs, der Normenbestimmtheit und Normenklarheit sowie dem Grundsatz der Verhältnismäßigkeit. Nachdem es ausgeführt hat, dass durch die angegriffenen gesetzlichen Regelungen »verbesserte Bedingungen für eine effektive und zudem heimliche Datenerfassung und –verarbeitung« geschaffen worden sind, also ein erheblicher Eingriff in das Recht auf informationelle Selbstbestimmung vorliegt, erklärt es die Verfassungswidrigkeit der Norm wegen mangelnder »*Bestimmtheit und Klarheit*«.[27] Weder sei der Verwendungszweck der erhobenen Daten eindeutig definiert noch der Umfang der erhebbaren Daten. Was das Bundesverfassungsgericht dazu ausführt, werden zukünftige Gesetzgeber zu beachten haben, wenn sie nicht erneut vor dem Verfassungsrecht scheitern wollen.
Das Gericht rügt, dass die Gesetzgeber keine »Präzisierung des Anwendungsbereichs der Ermächtigung durch Bezeichnung von Anlass und Zweck der Maßnahme durch die Verwendung der Begriffe des Fahndungstatbestands« vorgenommen haben. So könne jeder polizeiliche Datenbestand, in dem Fahrzeugkennzeichen enthalten sind, zum Fahndungstatbestand gezählt oder als Fahndungsnotierung betrachtet werden. Weiterhin sei ungeklärt, »ob und inwieweit der Einsatz der automatisierten Kennzeichenerfassung zur Erstellung von Bewegungsbildern im Rahmen einer polizeilichen Beobachtung oder längerfristigen Observation dienen soll und darf«.[28]

27 BVerfG (Fn. 26), C II 2 (Rz. 93 ff.).
28 BVerfG (Fn. 26), C II 2 b bb 4 (Rz. 105).

Das Argument, der Gesetzgeber habe seine Regelung so unbestimmt gefasst, dass mit Hilfe der automatisierten Kennzeichenerfassung auch andere Zwecke, wie z.B. die polizeiliche Beobachtung, durchgeführt werden könne, findet sich an mehreren Stellen des Urteils. Die Unbestimmtheit der gesetzlichen Regelung führe dazu, dass die Qualität der Kennzeichenerfassungen sich verändere und dadurch polizeiliche Maßnahmen einer darauf abgestimmten Ermächtigungsgrundlage bedürften. So sei den gesetzlichen Regelungen nicht zu entnehmen, ob die Erfassung der Kennzeichen auch für strafprozessuale Zwecke verwendet werden könne. Wohlwollend räumt das Bundesverfassungsgericht gegenüber den Landesgesetzgebern ein, dass möglicherweise einige Bestimmtheitsdefizite durch Auslegung zu beseitigen seien, stellt dann aber gleichsam resignativ und mahnend fest, dass auch in diesem Falle

> »die fehlende Bestimmtheit des Verwendungszweckes nicht insgesamt durch eine einengende verfassungskonforme Auslegung geheilt« wird.[29]

Das Bundesverfassungsgericht weist es von sich, verfassungswidrig weitgefasste Verwendungszwecke auf das verfassungsgemäße Maß herunter zu interpretieren. Heftige Kritik am Gesetzgeber ist aus der weiteren Formulierung des Gerichts zu hören, dass der Gesetzgeber »die Vorschrift bewusst unbestimmt gehalten und deshalb von einer Konkretisierung abgesehen hat.« Die exakte Befolgung des Bestimmtheitsgrundsatzes wird eine der wesentlichen Lehren sein, die zukünftige Gesetzgeber aus dem Urteil zu ziehen haben. Nachdem das Gericht das Fehlen einer Zweckbestimmung der automatisierten Kennzeichenerfassung festgestellt hat, folgert es daraus, dass auch die erhebbaren Informationen in den gesetzlichen Regelungen grundgesetzwidrig unbestimmt gehalten sind. Beide Gesetze enthalten keine Informationen darüber, ob neben der Ziffern- und Zeichenfolge des Kennzeichens weitere Informationen (wie z. B. der Insassen der PKW) erhoben werden dürfen.

Als habe es dem Gesetzgeber noch nicht genug einen legeren Umgang mit Verfassungsgrundsätzen bescheinigt, attestiert das Gericht zum Schluss auch noch einen Verstoß gegen den Grundsatz der Verhältnismäßigkeit. Es kann nicht feststellen, dass die beiden Gesetzgeber einen legitimen Zweck mit Mitteln verfolgt haben, die geeignet, erforderlich und angemessen sind. Wenn das Gebot der Verhältnismäßigkeit im engeren Sinne verlangt, dass die Schwere einer gesetzgeberischen Grundrechtsbeschränkung bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der sie rechtfertigenden Gründe stehen darf, so wird deshalb dagegen verstoßen, weil die Vorschriften wegen ihrer weiten Formulierung anlasslose und flächendeckende Maßnahmen der automatisierten Erfassung und Auswertung von Kfz-Kennzeichen ermöglichen. Damit entstehe der Eindruck ständiger Kontrolle.[30]

Das Gericht lässt in seiner weiteren Argumentation erkennen, wie es sich eine verfassungsgemäße Kennzeichenerfassung vorstellt. Ginge es um die Abwehr einer konkreten Gefahr oder um eine stichprobenartige Erfassung an einer Örtlichkeit, bei der bestimmte Kriminalitätsschwerpunkte sich ausweisen lassen, und wäre die Verwendung der so erhobenen Daten auf konkrete Zwecke beschränkt, dann gäbe es keine verfassungsrechtlichen Einwände gegen eine automatisierte Datenerfassung. Diese Kriterien sollte der hessische und schleswig-holsteinische Gesetzgeber berücksichtigen, wenn er daran geht, polizeiliche

29 BVerfG (Fn. 26), C II 2 b ff (Rz. 153).
30 BVerfG (Fn. 26), C II 3 c bb (1) (Rz. 173).

Eingriffsbefugnisse bei der automatisierten Datenerfassung von PKW-Kennzeichen gesetzlich neu zu gestalten.

4. Konsequenzen

Welche Konsequenzen hat ein zukünftiger Gesetzgeber aus den drei Entscheidungen des Bundesverfassungsgerichts zu ziehen und wie ist die sicherheitspolitische Situation zu beurteilen? Wenn man die Entscheidungen des Bundesverfassungsgerichts in den Zusammenhang einer politischen Auseinandersetzung zwischen einer konservativen, rechtsstaatliche Garantien beschränkenden und einer liberalen, Freiheitsrechte trotz möglicher Bedrohungslagen bewahrenden Konzeption stellt, dann vertritt das Gericht unmissverständlich und argumentativ schwer widerlegbar ein klassisches freiheitsorientiertes Rechtsstaatsmodell. Die Entscheidungen verfolgen das rechtsstaatliche Anliegen, eine verfassungsrechtlich angemessene Balance zwischen Freiheit und Sicherheit zu finden. »Wir konnten die Entscheidungen Schritt für Schritt entwickeln. Zu den rechtsstaatlichen Anforderungen gehören hinreichende Anhaltspunkte der Wirksamkeit: Ist das neue Mittel geeignet und erforderlich und angemessen? (…) Wir haben nicht nur die Freiheit, sondern auch das Interesse an Gefahrenabwehr und Strafverfolgung sehr ernst genommen«.[31]
Dem gegenüber hatte der Gesetzgeber, dem das Gericht verfassungsrechtlich unwirksame Regelungen attestierte, keine exakten Anhaltspunkte für Gefährdungen von gewichtigen Rechtsgütern verlangt und staatliche Eingriffe in Freiheitsrechte erlaubt, ohne deren Angemessenheit zur Voraussetzung zu machen. So sind gesetzliche Regelungen entstanden oder sollten verabschiedet werden, die staatlichen Stellen einen breiten Interpretationsspielraum für Interventionen ließen, die in die intimsten Bereiche von Bürgern reichten. Dagegen hat das Gericht trotz Anerkennung potentieller Gefahrenlagen dafür plädiert, die Politik müsse »mit Augenmaß« reagieren.[32] Das Bundesverfassungsgericht ist von dem Anspruch ausgegangen, auch in diffusen Gefahrenlagen das Risiko, »Unverdächtige zu beinträchtigen oder die Bevölkerung insgesamt einzuschüchtern«, so gering wie möglich zu halten. Die Freiheit der Bürger, so manchem konservativen Politiker kein argumentationsweisender Maßstab, ist für das Bundesverfassungsgericht auch in bedrohlichen Situationen ein unverzichtbarer Wert. Es verlangt vom Gesetzgeber den exakten Nachweis, warum bisherige rechtliche Instrumente nicht ausreichend sind, neuen Gefahrenlagen zu begegnen. Mit dem Argument, frühere verfassungsrechtlich problematische Instrumente wie die Rasterfahndung hätten keine nachweisbaren Ergebnisse gebracht, ist das Gericht in einer guten argumentativen Lage.
Wer die Entscheidungen liest, dem wird neben dem emphatischen Plädoyer für Freiheitsrechte auffallen, dass das Gericht mit großer Sorgfalt die Wirkungsweise und die Folgen moderner Technik analysiert. Die Urteile zeigen, dass ein Jurist, der auf der Höhe der Zeit sein will, über weitaus mehr Kenntnisse als nur juristische verfügen muss. Da die Verfassungsrichter dies demonstrierten, machen sie es denen schwer, die mit technischen Argumenten traditionelle juristische Grundsätze außer Kraft setzen wollen. Das Gericht hat sich nicht nur als ein Bewahrer klassischer rechtsstaatlicher Grundsätze erwiesen, es hat auch

31 Wolfgang Hoffmann-Riem, Süddeutsche Zeitung vom 12./13. April 2008.
32 Hoffmann-Riem, ebd.

gezeigt, wie eine moderne Verfassungsrechtsprechung technisches Wissen zugunsten der Verteidigung von Freiheitsrechten nutzen kann. Wenn es dem zukünftigen Bundes- und Landesgesetzgeber Vorgaben für die Gestaltung von Gesetzen macht, dann verlangt es nicht mehr als das, was jeder Student im ersten Semester als tragende Grundsätze des Verfassungsrechts lernt: die Bestimmtheit und Klarheit von Normen und der Grundsatz der Verhältnismäßigkeit. Dem Gesetzgeber dies zu verdeutlichen, ist angesichts des zunehmend achtlosen Umgangs mit diesen Grundsätzen mehr als erforderlich. Dass er daraus lernt, dafür sprechen die aktuellen Diskussionen über eine verfassungskonforme Neufassung der Online-Durchsuchung.[33]

33 Süddeutsche Zeitung vom 16. April 2008.