Vorratsdatenspeicherung und Grundgesetz#

Hans-Jürgen PAPIER*

I. Das Grundrecht auf informationelle Selbstbestimmung

Mit seinem Urteil vom 15. Dezember 1983 zur Verfassungsmäßigkeit der Volkszählung hatte das Bundesverfassungsgericht ein Grundrecht auf informationelle Selbstbestimmung anerkannt und dieses Grundrecht im Mittelpunkt der grundgesetzlichen Ordnung, nämlich im Wert und der Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt, verankert.[1)] Ihrem Schutz dient das allgemeine Persönlichkeitsrecht, und zwar neben den speziellen Freiheitsverbürgungen wie dem Grundrecht auf Unverletzlichkeit der Wohnung und auf Schutz des Brief-, Post- und Fernmeldegeheimnisses (Art. 13, Art. 10 GG). Neu war im „Volkszählungsurteil", dass das Bundesverfassungsgericht die Vorgaben des allgemeinen Persönlichkeitsrechts[2)] an die modernen Bedingungen der automatischen Datenverarbeitung angepasst hat. Die freie Entfaltung der Persönlichkeit setzt insoweit den Schutz des Einzelnen gegen unbegrenzte Erhebungen, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Das Grundrecht auf informationelle Selbstbestimmung gewährleistet dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[3)]

Eingriffe in das Recht auf informationelle Selbstbestimmung bedürfen einer hinreichend bestimmten gesetzlichen Grundlage.[4)] Dabei muss der Gesetzgeber den Verwendungszweck der zu erhebenden Daten bereichsspezifisch und präzise festlegen.[5)] Eine Weitergabe von Daten kommt grundsätzlich nur zu dem gleichen Zweck in Betracht, zu dem die Daten erhoben wurden. Die öffentliche Verwaltung ist keine „Informationseinheit", innerhalb derer im Wege der Amtshilfe jede Information beschafft und zwischen den unterschiedlichen Behörden beliebig ausgetauscht werden dürfte. Diese Zweckbindung erhobener Daten schließt

* Prof. Dr. Dres. h.c. Hans-Jürgen Papier ist emeritierter Professor der Ludwig-Maximilians-Universität München und ehemaliger Präsident des Bundesverfassungsgerichts.

This paper was supported by a grant-in-aid from the Japan Society for the Promotion of Science.

1) BVerfGE 65, 1 (41 ff.) – Volkszählung.

2) Vgl. zum allgemeinen Persönlichkeitsrecht BGHZ 13, 334 (338) – Schacht-Leserbrief; BVerfGE 34, 269 (281 f.) – Soraya.

3) BVerfGE 65, 1 (42 f.) – Volkszählung.

4) BVerfGE 65, 1 (44) – Volkszählung.

5) BVerfGE 65, 1 (46) – Volkszählung.

zwar eine Zweckänderung nicht grundsätzlich aus. Diese bedarf jedoch ihrerseits einer verfassungsgemäßen gesetzlichen Grundlage. Erforderlich sind außerdem verfahrensrechtliche Schutzvorkehrungen, wie beispielsweise Aufklärungs-, Auskunfts- und Löschungspflichten sowie im Interesse eines vorgezogenen Rechtsschutzes die Beteiligung eines unabhängigen Datenschutzbeauftragten.[6)]

II. Vorratsdatenspeicherung und Telekommunikationsgeheimnis

Bei der Vorratsdatenspeicherung geht es um Vorgänge der Telekommunikation. Bezogen auf die Telekommunikation enthält der Art. 10 GG eine spezielle Garantie, die das allgemeine Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG verdrängt und aus der sich besondere Anforderungen für die Daten ergeben, die durch Eingriffe in das Fernmeldegeheimnis erlangt werden. Insoweit lassen sich allerdings die Maßgaben, die das Bundesverfassungsgericht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG entwickelt hat, weitgehend auf die speziellere Garantie des Art. 10 GG übertragen.

1. Schutz des Telekommunikationsgeheimnisses

Art. 10 Abs. 1 des Grundgesetzes schützt das Telekommunikationsgeheimnis. Bei der Telekommunikation geht es um alle Vorgänge der unkörperlichen Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs. Diese Vorgänge sollen vor einer Kenntnisnahme durch die öffentliche Gewalt geschützt sein,[7)] und zwar nicht nur im Hinblick auf die Inhalte der Kommunikation, sondern auch in Bezug auf die Vertraulichkeit der näheren Umstände der Kommunikationsvorgänge. Zu diesen von Art. 10 des Grundgesetzes ebenfalls geschützten Aspekten zählt das Bundesverfassungsgericht ausdrücklich, „ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist“.[8)]

Das Grundrecht des Art. 10 GG schützt das Telekommunikationsgeheimnis zum einen vor dem ersten Zugriff der öffentlichen Gewalt zum Zwecke der Kenntnisnahme von Telekommunikationsvorgängen und Telekommunikationsinhalten. Das Grundrecht entfaltet seinen Schutz zum anderen auch im Hinblick auf sich anschließende Maßnahmen des Gebrauchs und der Verwendung der durch einen Eingriff in das Telekommunikationsgeheimnis erlangten Daten.[9)] „Ein Grundrechtseingriff ist jede Kenntnisnahme, Aufzeichnung und

6) BVerfGE 65, 1 (49) – Volkszählung.
7) Vgl. dazu und zum Folgenden BVerfGE 125, 260 (309 ff.) – Vorratsdatenspeicherung; BVerfGE 120, 274 (306 f.) – Online-Durchsuchung; BVerfGE 106, 28 (35 f.) – Mithörvorrichtung.
8) BVerfGE 125, 260 (309) – Vorratsdatenspeicherung, mit weiteren Nachweisen aus der Rechtsprechung.
9) BVerfGE 100, 313 (319) – Telekommunikationsüberwachung; 125, 260 (309 f.) – Vorratsdatenspeicherung.

Verwertung von Kommunikationsdaten sowie jede Auswertung ihres Inhalts oder die sonstige Verwendung durch die öffentliche Gewalt“.[10] Folglich liegt in der durch Gesetz oder auf Grund eines Gesetzes erfolgenden Anordnung gegenüber Kommunikationsunternehmen, Telekommunikationsdaten zu erheben, zu speichern und an staatliche Stellen zu übermitteln, ein Eingriff in das Grundrecht auf Schutz des Telekommunikationsgeheimnisses aus Art. 10 Abs. 1 GG.

2. Verfassungsrechtliche Anforderungen an die Vorratsdatenspeicherung

Verfassungsgemäß sind die Eingriffe in das Telekommunikationsgeheimnis, „wenn sie legitimen Gemeinwohlzwecken dienen und im Übrigen dem Grundsatz der Verhältnismäßigkeit genügen“. Sie müssen mithin zur Erreichung der Zwecke geeignet, erforderlich und angemessen sein.[11]

a) Das Bundesverfassungsgericht hat es für verfassungsrechtlich möglich angesehen, dass der Gesetzgeber eine sechsmonatige anlasslose Speicherung von Telekommunikationsverkehrsdaten für qualifizierte Verwendungen im Rahmen der Strafverfolgung, der Gefahrenabwehr und der Aufgaben der Nachrichtendienste vorsieht[12]. Eine solche Regelung verfolgt verfassungslegitime Zwecke, für deren Erreichung eine sechsmonatige anlasslose Speicherung geeignet, erforderlich und auch verhältnismäßig im engeren Sinne sein kann. „Bei einer Ausgestaltung, die dem besonderen Gewicht des hierin liegenden Eingriffs hinreichend Rechnung trägt, unterfällt eine anlasslose Speicherung der Telekommunikationsverkehrsdaten nicht schon als solche dem strikten Verbot einer Speicherung von Daten auf Vorrat im Sinne der Rechtsprechung des Bundesverfassungsgerichts“.[13]

b) Es gehört zu den legitimen Aufgaben und Zwecken des Staates, die auch einen Eingriff in das Telekommunikationsgeheimnis grundsätzlich rechtfertigen können, wenn die Strafverfolgung, die Abwehr von Gefahren für die öffentliche Sicherheit sowie die Aufgabenerfüllung der Nachrichtendienste effektiver ausgestaltet werden sollen. Dies gilt auch dann, wenn die Telekommunikationsverkehrsdaten anlasslos vorsorglich gesichert werden. Nicht jede vorsorgliche Erhebung und Speicherung von Daten überhaupt, sondern nur die unverhältnismäßige Ausgestaltung solcher Datensammlungen und insbesondere entgrenzende Zwecksetzungen werden durch das Grundrecht des Art. 10 des Grundgesetzes verboten. Als grundrechtswidrig erweist sich also eine Speicherung von personenbezogenen Daten auf

10) BVerfGE 125, 260 (310) – Vorratsdatenspeicherung.

11) BVerfGE 125, 260 (316) – Vorratsdatenspeicherung, mit weiteren Nachweisen aus der bisherigen Rechtsprechung.

12) BVerfGE 125, 260 (316 ff.) – Vorratsdatenspeicherung.

13) BVerfGE 125, 260 (316) – Vorratsdatenspeicherung, unter Hinweis auf BVerfGE 65, 1 (46 f.) – Volkszählung; 115, 320 (350) – Rasterfahndung II; 118, 168 (187) – Kontostammdaten.

Vorrat insbesondere dann, wenn sie zu unbestimmten und noch nicht bestimmbaren Zwecken erfolgt. Eine vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten zur späteren anlassbezogenen Übermittlung an die für die Strafverfolgung oder Gefahrenabwehr zuständigen Behörden oder an die Nachrichtendienste ist dagegen nicht von vornherein unverhältnismäßig und damit grundrechtswidrig. Die Ausgestaltung einer solchen vorsorglichen Telekommunikationsverkehrsdatenspeicherung unterliegt allerdings besonderen verfassungsrechtlichen Anforderungen. Dies gilt nach der Rechtsprechung des Bundesverfassungsgerichts insbesondere im Hinblick auf die Datensicherheit, die Voraussetzungen und den Umfang der Datenverwendungen sowie die Transparenz und den Rechtsschutz.[14)]

c) Eine Speicherung der Telekommunikationsverkehrsdaten kann nur dann verfassungsgemäß sein, wenn der Gesetzgeber zugleich einen besonders hohen Standard der Datensicherheit gewährleistet. Der Datensicherheit kommt für die Verhältnismäßigkeit der Vorratsdatenspeicherung große Bedeutung zu, weil die so geschaffenen Datenbestände einen immensen Umfang und eine erhebliche potenzielle Aussagekraft erlangen. In diesem Zusammenhang ist auch zu berücksichtigen, dass die Daten bei privaten Diensteanbietern gespeichert werden, die den Anforderungen der Wirtschaftlichkeit unterliegen und unter Kostendruck handeln. Für sie gibt es nur in begrenztem Maße Anreize zur Gewährleistung von Datensicherheit. Zwar kann die Verfassung nicht im Einzelnen vorgeben, welche Sicherheitsmaßnahmen im Detail geboten sind. Im Ergebnis muss jedoch ein Standard gewährleistet sein, der im Hinblick auf die besonderen Gefährdungspotenziale der durch eine vorsorgliche Telekommunikationsverkehrsdatenspeicherung geschaffenen Datenbestände ein entsprechend hohes Maß an Sicherheit gewährleistet. Dieser Standard muss an dem Entwicklungsstand der Fachdiskussion orientiert sein und neue Erkenntnisse und Einsichten fortlaufend aufnehmen. Das Gefährdungspotenzial, das von solchen Datenbeständen ausgeht, gestattet es nicht, die Sicherheitsanforderungen unter Abwägung mit allgemeinen wirtschaftlichen Belangen zu relativieren. Man wird daher wohl beispielsweise eine getrennte Speicherung der Daten, eine anspruchsvolle Verschlüsselung, ein gesichertes Zugriffsregime unter Nutzung etwa des Vier-Augen-Prinzips sowie eine revisionssichere Protokollierung verlangen müssen, um die Sicherheit der Daten verfassungsrechtlich hinreichend zu gewährleisten.[15)]

d) Die Verfassungsmäßigkeit einer Speicherung von Telekommunikationsverkehrsdaten hängt überdies von gesetzlichen Regelungen zur Verwendung dieser Daten ab.[16)] Dabei müssen die „Voraussetzungen für die Datenverwendung und deren Umfang in den betreffenden

14) BVerfGE 125, 260 (325 ff.) – Vorratsdatenspeicherung.
15) BVerfGE 125, 260 (325 f.) – Vorratsdatenspeicherung.
16) BVerfGE 125, 260 (327 ff.) – Vorratsdatenspeicherung.

Rechtsgrundlagen umso enger begrenzt werden, je schwerer der in der Speicherung liegende Eingriff liegt. Anlass, Zweck und Umfang des jeweiligen Eingriffs sowie die entsprechenden Eingriffsschwellen sind dabei durch den Gesetzgeber bereichsspezifisch, präzise und normenklar zu regeln".[17)]

Sollen Daten oder Datenbestände verwendet werden, die durch eine anlasslose systematische Speicherung praktisch aller Telekommunikationsverkehrsdaten gewonnen worden sind, verlangt der Grundsatz der Verhältnismäßigkeit, dass diese Verwendung besonders hochrangigen Gemeinwohlbelangen dient. Sie darf nur für überragend wichtige Aufgaben des Rechtsgüterschutzes eingesetzt werden. Es muss mit anderen Worten um die Ahndung von Straftaten, die überragend wichtige Rechtsgüter bedrohen oder um die Abwehr von Gefahren für solche Rechtsgüter gehen.[18)]

(1) Eine Datenverwendung zu Zwecken der Strafverfolgung setzt demgemäß voraus, dass zumindest ein durch bestimmte Tatsachen begründeter Verdacht einer schweren Straftat besteht. Welche Straftatbestände im Einzelnen zu diesem Kreis der „schweren Straftaten" gehören sollen, hat der Gesetzgeber zusammen mit der Regelung zur Datenspeicherung abschließend festzulegen. Die Einstufung als „schwere Straftat" muss sich in der jeweiligen Strafvorschrift objektiv widerspiegeln, etwa in ihrem besonderen Strafrahmen. Der Gesetzgeber hat also abstrakt einen entsprechenden Straftatenkatalog festzulegen, darüber hinaus hat er aber auch sicherzustellen, dass ein Abruf auf die vorsorglich gespeicherten Telekommunikationsverkehrsdaten nur dann erfolgen darf, wenn es um die Verfolgung einer auch im Einzelfall schwerwiegenden Straftat geht.[19)]

(2) Für die Gefahrenabwehr gelten folgende verfassungsrechtliche Grenzen des Abrufs der vorsorglich gespeicherten Telekommunikationsverkehrsdaten: Er ist nur zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr zulässig.[20)] Das folgt aus der Abwägung zwischen dem Gewicht des in der Datenspeicherung und Datenverwendung liegenden Eingriffs und der Bedeutung einer wirksamen Gefahrenabwehr. Die gesetzliche Ermächtigungsgrundlage muss außerdem „zumindest tatsächliche Anhaltspunkte einer konkreten Gefahr für die zu schützenden Rechtsgüter" voraussetzen.[21)] Vermutungen oder allgemeine Erfahrungssätze reichen nicht aus, um den Zugriff auf die Daten zum Zwecke der Gefahrenabwehr zu rechtfertigen. Es müssen vielmehr bestimmte Tatsachen festgestellt sein,

17) BVerfGE 125, 260 (328) – Vorratsdatenspeicherung, mit weiteren Nachweisen aus der Rechtsprechung.
18) BVerfGE 125, 260 (328) – Vorratsdatenspeicherung.
19) BVerfGE 125, 260 (329) – Vorratsdatenspeicherung.
20) BVerfGE 125, 260 (330) – Vorratsdatenspeicherung.
21) BVerfGE 125, 260 (330) – Vorratsdatenspeicherung.

die die Prognose einer konkreten Gefahr tragen. Der Abruf der Daten stellt einen gewichtigen Grundrechtseingriff dar. Daher darf der tatsächliche Eingriffsanlass nicht weitgehend in das Vorfeld einer im Einzelnen noch nicht absehbaren konkreten Gefahr vorverlegt werden. Es müssen bestimmte Tatsachen festgestellt sein, die die Prognose einer konkreten Gefahr tragfähig und plausibel erscheinen lassen.

(3) Was zur Verwendung der Daten zur polizeilichen Gefahrenabwehr gesagt ist, gilt grundsätzlich für alle Eingriffsermächtigungen mit präventiver Zielsetzung. Auch im Hinblick auf die Verwendung der Daten durch die Nachrichtendienste sind die erwähnten verfassungsrechtlichen Anforderungen und Grenzen zu beachten.[22] Es besteht keine Möglichkeit zu behördenbezogenen Differenzierungen, also beispielsweise zwischen Polizeibehörden einerseits und anderen mit präventiven Aufgaben betrauten Behörden wie den Behörden des Verfassungsschutzes auf der anderen Seite. Eine Verwendung der vorsorglich gespeicherten Telekommunikationsverkehrsdaten von Seiten der Nachrichtendienste dürfte daher in vielen Fällen ausscheiden. Das folgt aus der Art der Aufgabenstellung der Nachrichtendienste, die vorrangig im Bereich der Vorfeldaufklärung tätig sind. Dies stellt keinen Rechtfertigungsgrund dafür dar, an den verfassungsrechtlichen Voraussetzungen für einen Eingriff der hier vorliegenden Art Abstriche zu machen.

e) Der Gesetzgeber hat schließlich hinreichende Vorkehrungen zur Transparenz der Datenverwendung sowie zur Gewährleistung eines effektiven Rechtsschutzes und effektiver Sanktionen zu treffen.[23] Nur unter diesen weiteren Voraussetzungen entspricht eine vorsorgliche anlasslose Speicherung von Telekommunikationsverkehrsdaten und deren Verwendung dem Grundsatz der Verhältnismäßigkeit. Im Hinblick auf die gebotene Transparenz muss, soweit dies möglich ist, die Verwendung der Daten offen erfolgen. Kommt eine solche nach Lage der Dinge nicht in Betracht, bedarf es grundsätzlich zumindest nachträglich einer Benachrichtigung des Betroffenen. Scheidet ausnahmsweise auch eine solche nachträgliche Benachrichtigung aus, hat ein Richter über die Nichtbenachrichtigung zu entscheiden.

(1) Eine Verwendung der Daten ohne Wissen des Betroffenen ist verfassungsrechtlich nur zulässig, „wenn andernfalls der Zweck der Untersuchung, dem der Datenabruf dient, vereitelt wird“.[24] Soweit es um Gefahrenabwehr geht, wird dies grundsätzlich der Fall sein. Im Rahmen der Strafverfolgung können indes die Daten vielfach auch offen erhoben und genutzt werden. Eine heimliche Verwendung darf hier nur erfolgen, wenn und soweit dies im Einzelfall erforderlich und richterlich angeordnet ist.

---

22) BVerfGE 125, 260 (331) – Vorratsdatenspeicherung.
23) BVerfGE 125, 260 (334) – Vorratsdatenspeicherung.
24) BVerfGE 125, 260 (336) – Vorratsdatenspeicherung.

(2) Eine vorsorgliche Speicherung der Telekommunikationsverkehrsdaten und ihre Verwendung können schließlich nur dann dem Verhältnismäßigkeitsprinzip genügen, wenn ein effektiver Rechtsschutz und adäquate Sanktionen im Falle einer Rechtsverletzung gewährleistet sind. Zu diesem Zweck ist eine Abfrage oder Übermittlung der Daten grundsätzlich unter einen Richtervorbehalt zu stellen.[25] Bei Eingriffsmaßnahmen, die einen schwerwiegenden Grundrechtseingriff bewirken, ist allgemein von Verfassungs wegen eine vorbeugende Kontrolle durch eine unabhängige Instanz geboten. Dies gilt in besonderem Maße, wenn der Grundrechtseingriff heimlich erfolgt und für den Betroffenen unmittelbar nicht wahrnehmbar ist. Das bedeutet, dass solche Maßnahmen grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen sind. Denn nur Richter können „auf Grund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer ausschließlichen Bindung an das Gesetz die Rechte des Betroffenen im Einzelfall am besten und sichersten wahren“.[26]

Es muss im Übrigen auch ein Rechtsschutzverfahren zur nachträglichen Kontrolle der Datenverwendung geben. Konnten sich Betroffene vor Durchführung der Maßnahme nicht vor den Gerichten gegen die Verwendung ihrer Telekommunikationsverkehrsdaten zur Wehr setzen, muss ihnen eine nachträgliche gerichtliche Kontrolle eröffnet sein.[27]

(3) Schließlich muss der Gesetzgeber wirksame Sanktionen im Falle rechtswidriger Datenverwendungen vorsehen. Der besonderen Schwere der Persönlichkeitsverletzung, die in der unberechtigten Erlangung oder Verwendung der hier in Frage stehenden Daten regelmäßig liegt, muss im Strafrecht, im Strafverfahrensrecht sowie im zivilrechtlichen Schadenersatzrecht hinreichend Rechnung getragen werden. Denkbar sind hier strafrechtliche Verwertungsverbote sowie eine Haftung auf Schadenersatz auch für immaterielle Schäden.

3. Verfassungswidrigkeit der deutschen Gesetzesregelungen

Die gesetzlichen Vorgaben für die Datensicherheit sowie die Vorschriften zur Verwendung der Daten in den angefochtenen gesetzlichen Regelungen des deutschen Rechts genügten nach Auffassung des Bundesverfassungsgerichts den verfassungsrechtlichen Anforderungen nicht.[28] Damit fehlte es zugleich auch der Speicherungspflicht selbst an der verfassungsrechtlich erforderlichen Rechtfertigung. Daher waren die gesamten Vorschriften über die Vorratsdatenspeicherung mit dem Grundrecht auf Schutz des Telekommunikationsgeheimnisses nach Art. 10 Abs. 1 GG nicht vereinbar. Sie sind vom Bundesverfassungsgericht für nichtig erklärt worden. Auf der anderen Seite hat das Bundesverfassungsgericht nicht ausgeschlossen, dass bei Wahrung spezifischer strenger Anforderungen eine anlasslose Vorratsdatenspeicherung

25) BVerfGE 125, 260 (337) – Vorratsdatenspeicherung.
26) BVerfGE 125, 260 (338) – Vorratsdatenspeicherung.
27) BVerfGE 125, 260 (339) – Vorratsdatenspeicherung.
28) BVerfGE 125, 260 (347 ff.) – Vorratsdatenspeicherung.

im Hinblick auf die Telekommunikationsverkehrsdaten mit der Verfassung vereinbar sein kann. Der Gesetzgeber hat allerdings bis zum heutigen Tage noch keine Neuregelung getroffen. Das liegt vor allem daran, dass innerhalb der christlich-liberalen Koalition die Einführung einer Vorratsdatenspeicherung insgesamt umstritten ist.

Das Bundesverfassungsgericht hat mit seiner Entscheidung zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten einen verfassungsrechtlichen „Grenzpfahl" errichtet: Eine flächendeckende, vorsorgliche Erfassung und Speicherung von Daten, die praktisch alle Aktivitäten des Bürgers rekonstruierbar macht, ist mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar. Eine solche staatliche Datensammlung bedeutete vielleicht ein zusätzliches Maß an Sicherheit; dies darf aber nicht auf Kosten einer totalen Überwachung der Bürger gehen, die die Freiheitsausübung empfindlich einschränken würde.

III. Neue Herausforderungen für den Grundrechtsschutz

1. Neue Bedrohungen – neue Technologien

Das Recht auf informationelle Selbstbestimmung steht im Vergleich zur Zeit des Volkszählungsurteils vom 15. Dezember 1983 vor neuen Herausforderungen. Sie haben ihren Grund vor allem in der Art der drohenden Gefahren. Nach den Terroranschlägen vom 11. September 2001 in den USA und vom 11. März 2004 in Madrid wurden in Deutschland sowie auf EU-Ebene neuartige Maßnahmen durchgeführt oder beschlossen, wie die präventive polizeiliche Rasterfahndung[29] nach so genannten „Schläfern", die „Online-Durchsuchung"[30] oder die hier bereits angesprochene Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten.

Diese neuen Herausforderungen haben ihren Grund aber nicht nur in der Art der drohenden Gefahren, sondern auch in den geradezu revolutionären Veränderungen der Informations- und Kommunikationstechnologien. Der Staat darf einerseits – schon um seiner grundrechtlichen Pflicht zum Schutz von Leib, Leben oder Freiheit seiner Bürger zu genügen – diese technischen Veränderungen bei der Abwehr von Gefahren und der Verfolgung von Straftaten einerseits nicht unberücksichtigt lassen. Andererseits dürfen im Zuge der Ausbalancierung von Freiheit und Sicherheit die Gewichte nicht grundlegend zu Lasten der Freiheit verschoben werden.

2. Verhältnismäßigkeit und Schutz der Menschenwürde

Bei der verfassungsrechtlichen Beurteilung der neuartigen Eingriffe in das Recht auf

29) Vgl. dazu bereits BVerfGE 93, 181 (186 ff.) – Rasterfahndung I; BVerfGE 115, 320 (341 ff.) – Rasterfahndung II.

30) Vgl. BVerfGE 120, 274 (302 ff.) – Online-Durchsuchung.

informationelle Selbstbestimmung stellt der Verhältnismäßigkeitsgrundsatz Anforderungen an den Rang der zu schützenden Rechtsgüter sowie die Art und die Intensität ihrer Gefährdung. Darüber hinaus darf auch der Kernbereich privater Lebensgestaltung, der sich letztlich aus der Menschenwürde ableitet, durch staatliche Überwachungsmaßnahmen nicht angetastet werden.[31)] Die Menschenwürde und der Menschenwürdegehalt spezieller Freiheitsrechte sind nach der ständigen Judikatur des Bundesverfassungsgerichts nicht gegenüber anderen Freiheitsrechten und den aus ihnen folgenden Schutzpflichten des Staates abwägbar oder gar „wegwägbar". Freilich stellt sich in der Praxis häufig das Problem, dass vor einer Datenerhebung gar nicht geklärt werden kann, ob diese den Kernbereich privater Lebensgestaltung betreffen wird. Für diese Situationen gilt ein zweistufiges Schutzkonzept, das auf der Unterscheidung von Erhebungs- und Auswertungsphase besteht, auf das ich hier nicht im Einzelnen eingehen kann.

Als Fazit kann jedenfalls festgehalten werden, dass angesichts der grundrechtlichen Grenzen für die sicherheitsrechtliche Tätigkeit des Staates eine Wandlung des Staates in einen Überwachungsstaat „Orwellscher Prägung" eine sehr fern liegende Möglichkeit ist. Das rechtsstaatliche Gemeinwesen verfügt über rechtsstaatliche und demokratische Kontrollmechanismen, die es von totalitären Überwachungsstaaten unterscheidet, wie wir sie auch in Deutschland aus unserer jüngeren Geschichte kennen.

3. Bedrohungen von privater Seite

a) Unsere Sorge sollte heute mehr darum gehen, dass wir uns möglicherweise zu einer privaten Überwachungsgesellschaft internationalen Ausmaßes verwandeln, was zu einem gewissen Teil auch noch freiwillig erfolgt. Durch den andauernden technischen Fortschritt der Informations- und Kommunikationstechnologien und die internationale Vernetzung der Informationswege haben die Bürger im Vergleich zur Zeit des Volkszählungsurteils unglaublich viele neue Handlungsmöglichkeiten hinzugewonnen. Würden allerdings alle die irgendwo auf der Welt über uns gespeicherten Informationen zusammengeführt, ließe sich unschwer ein „Persönlichkeitsprofil" von jedem von uns erstellen. Das allerdings wäre der „Super-Gau des Datenschutzes", allerdings herbeigeführt nicht durch den Staat, sondern durch die Hände Privater.

31) Vgl. dazu und zum Folgenden insbesondere etwa BVerfGE 109, 279 (311 ff.) – Großer Lauschangriff.

b) Die Grundrechte allgemein, das Grundrecht auf informationelle Selbstbestimmung im Besonderen fordern ein Mindestmaß staatlichen Schutzes zugunsten der Bürger.[32] Denn die Grundrechte verpflichten den Staat auch, im Ausgleich mit konkurrierenden Freiheitsrechten ein angemessenes Schutzregime und Schutzniveau zu schaffen und durchzusetzen, sowie sich auf internationaler Ebene für ein solches Regime einzusetzen.[33] Er muss mit anderen Worten einen effektiven Schutz gegen Eingriffe von privater Seite sicherstellen. Er wird sich dabei nicht mehr allein mit bloßen Selbstverpflichtungen Privater begnügen dürfen, sondern er wird selbst eine verbindliche Ordnung schaffen müssen, um der grundrechtlichen Wertordnung auch im Privatrechtsverkehr Geltung zu verschaffen. Man wird davon ausgehen können, dass der grundrechtliche Schutzauftrag des Rechts auf informationelle Selbstbestimmung angesichts des ständigen Fortschritts der Technik wohl nie wird abgeschlossen sein können.[34] Dies hat sich zuletzt wieder an der Diskussion um „Google Streetview" gezeigt – ein Internetprogramm, das für jeden frei zugänglich ist und eine detailgetreue, dreidimensionale Darstellung ganzer Städte ermöglicht.[35]

Ich möchte schließen mit einer Aussage aus dem bereits mehrfach zitierten Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983: „Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über einen weiß."

---

32) Vgl. zur Herleitung objektiver Schutzpflichten aus den Grundrechten etwa BVerfGE 39, 1 (36 ff.) – Schwangerschaftsabbruch; BVerfGE 115, 118 (152) – Luftsicherheitsgesetz.

33) Vgl. auch *Hoffmann-Riem*, JZ 2008, 1009 (1011 f., 1013); *ders.*, AöR 123 (1998), 513 (524 ff.); *Petri*, DuD 2008, 443 (446 f.); *Hassemer*, FAZ vom 5. Juli 2007, S. 6; *Ronellenfitsch*, RDV 2008, 55 (58).

34) Vgl. zum grundlegenden Reformbedarf des Datenschutzrechts etwa *Kutscha*, ZRP 2010, 112 ff.; *Kühling/Bohnen*, JZ 2010, 600, 601 (607 ff.).

35) Das Privatunternehmen Google hat sich zwar unter anderem dazu bereit erklärt, auf Widerspruch von Hauseigentümern und Mietern auf die Darstellung von deren Gebäuden zu verzichten, vgl. hierzu die Selbstverpflichtungserklärung „Zusagen von Google zum Internetdienst Google Street View", abrufbar unter http://www.hamburg.de/datenschutz/aktuelles/1569338/google-street-view-zusage.html. Es ist jedoch zumindest umstritten, ob nach der derzeitigen Rechtslage in Deutschland eine wirksame *rechtliche* Handhabe gegen eine Veröffentlichung der Bilder bestünde, vgl. dazu bspw. *Caspar*, DÖV 2009, 965 ff.; *Spiecker gen. Döhmann*, CR 2010, 311 ff.; *Lindner*, ZUM 2010, 292 ff.