Prof. em. Dr. Dres. h.c.
Hans-Jürgen Papier

Mitterfeld 5 A
82327 Tutzing

hans-jürgen@prof-
papier.de

Gutachtliche Stellungnahme

Beweisbeschluss SV-2 des ersten Untersuchungsausschusses des Deutschen Bundestages der 18. Wahlperiode

von

Hans-Jürgen Papier

München, im Mai 2014

I.

1. Nach der Rechtsprechung des Bundesverfassungsgerichts verstößt eine flächendeckende vorsorglich anlasslose Speicherung aller Telekommunikationsverkehrsdaten, die für die Strafverfolgung oder Gefahrenprävention nützlich sein könnten, gegen deutsches Verfassungsrecht (vgl. BVerfGE 125, 260, 323 f.). Die Wahrung der Freiheitsrechte der Bürger darf nicht total erfasst und registriert werden. Dieses Verbot gehört sogar zur „verfassungsrechtlichen Identität der Bundesrepublik Deutschland", das die staatlichen Organe der Bundesrepublik nicht nur unmittelbar bindet, sondern für dessen Wahrung sich Deutschland auch „in europäischen und internationalen Zusammenhängen einsetzen muss" (vgl. BVerfGE 125, 260, 324). Eine vom Staat vorgenommene oder durch staatliche Regelungen veranlasste Sammlung von personenbezogenen Daten auf Vorrat zu unbestimmten oder (noch) nicht hinreichend bestimmbaren Zwecken ist nach der Rechtsprechung des Bundesverfassungsgerichts strikt untersagt (BVerfGE 65, 1, 46; 100, 313, 360; 115, 320, 350; 118, 168, 187; 125, 260, 321).

2. Allerdings ist damit noch nicht jede vorsorglich anlasslose Speicherung der Telekommunikationsverkehrsdaten von vorne herein rechtlich ausgeschlossen. Das Bundesverfassungsgericht hat es für verfassungsrechtlich möglich erachtet, dass eine zeitlich eng befristete anlasslose Speicherung der Telekommunikationsverkehrsdaten für qualifizierte Verwendungen im Rahmen der Strafverfolgung, der Gefahrenabwehr und der Aufgaben der Nachrichtendienste in einer den verfassungsrechtlichen Verhältnismäßigkeitsanforderungen genügenden Weise gesetzlich ausgestaltet werden 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" (BVerfGE 125, 260, 316

ff., unter Hinweis auf BVerfGE 65, 1, 46 f. – Volkszählung; 115, 320, 350 – Rasterfahndung; 118, 168, 187 – Kontostammdaten).

3. Bei der Telekommunikation, vor deren Kenntnisnahme durch die öffentliche Gewalt Art.10 Abs. 1 GG schützt, geht es um alle Vorgänge der unkörperlichen Übermittlung von Informationen an virtuelle Empfänger mit Hilfe des Telekommunikationsverkehrs. Der grundrechtliche Schutz bezieht sich nicht nur auf die Inhalte der Kommunikation, sondern auch auf die Vertraulichkeit der näheren Umstände der Kommunikationsvorgänge. Zu den geschützten Aspekten zählt also auch, „ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr statt gefunden hat oder versucht worden ist" (BVerfGE 125, 260, 309). Einen Eingriff in das Telekommunikationsgeheimnis stellt auch die Speicherung der den Internetzugang betreffenden Daten dar, selbst wenn sie Angaben über aufgerufene Internetseiten nicht enthalten (vgl. BVerfGE 125, 260, 311). 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 Art. 10 GG erlangten Daten (BVerfGE 100, 313, 319; 125, 260, 309 f.). In der Erfassung der Daten, der Speicherung, dem Abgleich mit anderen Daten, der Auswertung, der Selektierung zur weiteren Verwendung sowie der Übermittlung an Dritte liegen „je eigene Eingriffe in das Telekommunikationsgeheimnis" (BVerfGE 125, 260, 310). Dieser Grundsatz des fortbestehenden Schutzes durch Art.10 GG verlangt auch eine Kennzeichnung der durch einen ersten Eingriff in das Telekommunikationsgeheimnis erlangten Daten.

4. In einer gesetzlich angeordneten Speicherung der Telekommunikationsverkehrsdaten hat das Bundesverfassungsgericht einen „besonders schweren Eingriff" gesehen, wie ihn „die Rechtsordnung bisher

nicht kennt“ (BVerfGE 125, 260). Für die besondere Eingriffsschwere werden unter anderem angeführt:

- Erfassung sämtlicher Verkehrsdaten aller Bürgerinnen und Bürger ohne Anknüpfung an ein zurechenbares vorwerfbares Verhalten, ohne eine auch nur abstrakte Gefährlichkeit oder eine sonstige qualifizierte Situation;
- weitreichende Aussagekraft der Daten und Möglichkeiten der Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile;
- erhebliche Missbrauchsmöglichkeiten, die mit solchen Datensammlungen verbunden sind. Diese werden dadurch gesteigert, dass eine Vielzahl verschiedener Anbieter existiert, die von dieser Speicherungspflicht betroffen sind;
- Entstehung eines „diffus bedrohlichen Gefühls des Beobachtetseins“ beim Bürger, „das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann“ (BVerfGE 125, 260, 320).

5. Andererseits hat das Bundesverfassungsgericht in dieser Form der Datenspeicherung noch nicht per se einen unverhältnismäßigen Freiheitseingriff gesehen bzw. einen Eingriff, der den Menschenwürdekern des Grundrechts (Art. 10 Abs.1 in Verbindung mit Art.1 Abs.1 GG) oder seinen Wesensgehalt (Art.19 Abs. 2 GG) verletzt. Als maßgeblich erachtet das Bundesverfassungsgericht insofern folgende Aspekte:

- Speicherung erstreckt sich nur auf die Verkehrsdaten und erfasst nicht die Inhalte der Telekommunikation;
- Speicherung ist zeitlich limitiert, wobei die Speicherungsdauer von sechs Monaten „an der Obergrenze dessen“ liege, „was unter Verhältnismäßigkeitserwägungen rechtfertigungsfähig“ sei (BVerfGE 125, 260, 322);
- Speicherung der Vekehrsdaten erfolgt nicht direkt durch den Staat. Dieser hat keinen direkten Zugriff auf die Daten. Der Abruf seitens staatlicher Stellen erfolgt erst in einem zweiten Schritt und anlassbezogen nach gesetzlich näher festgelegten Kriterien.

6. Eine Speicherung der Telekommunikationsverkehrsdaten kann nur dann als noch verhältnismäßig im Sinne des Verfassungsrechts angesehen werden, wenn der Gesetzgeber einen besonders hohen Standard der Datensicherheit gewährleistet. Der Gesetzgeber muss einen Standard der Datensicherheit verordnen, der im Hinblick auf die besonderen Gefährdungspotentiale der durch eine vorsorgliche Telekommunikationsverkehrsdatenspeicherung geschaffenen Datenbanken ein entsprechend hohes Maß an Sicherheit gewährleistet (zum Beispiel: getrennte Speicherung, anspruchsvolle Verschlüsselung, gesichertes Zugriffsregime, revisionssichere Protokollierung. Siehe: BVerfGE 125, 260, 325 ff.).

7. Die Verfassungsmäßigkeit einer Speicherung von Telekommunikationsverkehrsdaten hängt überdies entscheidend von den gesetzlichen Regelungen der Verwendung der Daten ab (BVerfGE 125, 260, 327 ff.). Der Grundsatz der Verhältnismäßigkeit verlangt, dass die Verwendung dieser Daten ausschließlich für überragend wichtige Aufgaben des Rechtsgüterschutzes erfolgt. Es darf insoweit allein um die Ahndung von Straftaten, die überragend wichtige Rechtsgüter bedrohen, oder um die Abwehr von Gefahren für solche Rechtsgüter gehen (BVerfGE 125, 260, 328).

Eine Verwendung der Daten zu Zwecken der Strafverfolgung setzt danach voraus, dass zumindest ein durch bestimmte Tatsachen begründeter Verdacht einer schweren Straftat besteht.

Soweit der Abruf zur Gefahrenabwehr erfolgen soll, muss es um die Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder um die Abwehr einer gemeinen Gefahr gehen. Es müssen „zumindest tatsächliche Anhaltspunkte einer konkreten Gefahr für die zu schützenden Rechtsgüter“ bestehen (BVerfGE 125, 260, 330). Vermutungen oder allgemeine Erfahrungssätze reichen nicht aus.

Diese Anforderungen gelten für alle Datenabrufe mit präventiver Zielsetzung, also auch für solche durch die Nachrichtendienste. Eine Verwendung der vorsorglich gesicherten Daten durch die Nachrichtendienste dürfte daher in vielen Fällen ausscheiden, wenn und weil diese vorrangig im Bereich der Vorfeldaufklärung tätig sind. Nach der Rechtsprechung des Bundesverfassungsgerichts stellt dies keinen Rechtfertigungsgrund dafür dar, Abstriche an den verfassungsrechtlichen Anforderungen für Eingriffe in das Telekommunikationsgeheimnis mit präventiver Zielsetzung zu machen.

8. Eine vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten und deren Verwendung ist überdies nur dann mit dem Grundsatz der Verhältnismäßigkeit vereinbar, wenn der Gesetzgeber hinreichende Vorkehrungen zur Transparenz der Datenverwendung sowie zur Gewährleistung eines effektiven Rechtsschutzes sowie effektive Sanktionen bei Verletzungshandlungen vorsieht (BVerfGE 125, 260, 334).

Soweit die Verwendung der Daten heimlich erfolgt, ist eine gesetzliche Pflicht der nachträglichen Benachrichtigung vorzusehen. Ausnahmen aus zwingenden Gründen bedürfen der richterlichen Bestätigung.

Die Abrufe oder Übermittlungen der Daten bedürfen grundsätzlich der richterlichen Anordnung. Der richterliche Anordnungsbeschluss muss „gehaltvoll begründet werden" (BVerfGE 125, 260, 338).

Die abrufberechtigten Behörden dürfen keinen „Durchgriff" auf die Daten haben.

Es muss eine nachträgliche richterliche Kontrolle der Datenverwertung eröffnet sein.

Es müssen wirksame Sanktionen bei Rechtsverletzungen vorgesehen sein. Verletzungen des Telekommunikationsgeheimnisses dürfen im Ergebnis

nicht sanktionslos bleiben, der Persönlichkeitsschutz des Einzelnen darf „angesichts der immateriellen Natur dieses Rechts“ nicht „verkümmern“ (BVerfGE 125, 260, 339). Der Staat hat den Einzelnen vor Persönlichkeitsrechtsverletzungen und Persönlichkeitsrechtsgefährdungen auch durch Dritte angemessen zu schützen (BVerfGE 125, 260, 339).

9. Da die mit Gesetz vom 21. Dezember 2007 (BGBl. I, S.3198) eingeführte Regelung der Vorratsdatenspeicherung zum Abruf dieser Daten alle diese Voraussetzungen eines den Grundsatz der Verhältnismäßigkeit wahrenden Eingriffs in das Telekommunikationsgeheimnis nicht erfüllten, sind die Regelungen vom Bundesverfassungsgericht mit Urteil vom 2. März 2010 (BVerfGE 125, 260) für verfassungswidrig und nichtig erklärt worden. Sie waren damit zu keinem Zeitpunkt geltendes deutsches Recht. Eine flächendeckende, vorsorglich anlasslose und verdachtsunabhängige Speicherung von Telekommunikationsverkehrsdaten, sei es beim privaten Diensteanbiete, sei es beim Staat, durften und dürfen nach deutschem Verfassungsrecht also nicht erfolgen. Damit entfällt selbstverständlich auch jede rechtliche Möglichkeit des Abrufs solcher Daten durch staatliche Behörden. Das gilt erst recht für die Inhalte der Telekommunikation.

II.

10. Die Grundrechte des Grundgesetzes binden nach Art. 1 Abs. 3 GG Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht. Diese unmittelbare Bindungswirkung gilt allerdings nur für die vom Grundgesetz konstituierte deutsche öffentliche Gewalt. Auch Art. 10 GG entfaltet seinen unmittelbaren freiheitsrechtlichen Schutz also nur gegenüber Eingriffen, die der deutschen öffentlichen Gewalt zurechenbar sind. Der Schutzbereich der Grundrechte des Grundgesetzes endet dort, „wo ein Vorgang in seinem wesentlichen Verlauf von einem fremden Staat, nach seinem, von der Bundesrepublik Deutschland unabhängigen Willen gestaltet wird“ (BVerfGE 66, 39, 62).

11. Deutsche Behörden, einschließlich der Nachrichtendienste, sind an Art. 10 GG auch dann gebunden, wenn und soweit sie die grenzenüberschreitende Telekommunikation überwachen. Art. 10 GG schützt als Menschenrecht und damit gemäß seinem weiten personellen Schutzbereich nicht nur Deutsche, sondern auch Ausländer. Das gilt uneingeschränkt für die Telekommunikationsverkehre von Deutschen und Ausländern im deutschen Staatsgebiet, aber auch für solche, bei denen ein Endpunkt im Ausland, der andere im Inland liegt. Sofern beide Endpunkte des Telekommunikationsverkehrs im Ausland liegen, sind die den Eingriff in das Telekommunikationsgeheimnis vornehmenden deutschen Behörden grundsätzlich ebenfalls an Art. 10 GG gebunden; der räumliche Schutzumfang des Fernmeldegeheimnisses ist also nicht auf das Inland begrenzt (BVerfGE 100, 313). Das gilt nach der Rechtsprechung des Bundesverfassungsgerichts jedenfalls dann, wenn „eine im Ausland stattfindende Telekommunikation durch Erfassung und Auswertung im Inland hinreichend mit inländischem staatlichen Handeln verknüpft ist" (BVerfGE 100, 313 ff.).

12. Eingriffe in das Telekommunikationsgeheimnis, auch in das von Ausländern, unterliegen dagegen nicht dem grundrechtlichen Schutzbereich, wenn und soweit diese Eingriffe von ausländischen Behörden vorgenommen werden. Die aus den Grundrechten des Grundgesetzes folgenden freiheitsrechtlichen Eingriffsverbote sind an die deutsche öffentliche Gewalt adressiert. Eine Zurechenbarkeit solcher Eingriffe auch an die deutsche öffentliche Gewalt ist allerdings dann geboten, wenn und soweit diese Eingriffe von deutschem Boden mit Billigung und Duldung deutscher Behörden erfolgen. Die jeweils zuständigen deutschen Behörden haben das Recht und die Möglichkeit, Eingriffe ausländischer Mächte in das Telekommunikationsgeheimnis, die von deutschem Boden aus vorgenommen werden, zu verhindern bzw. zu unterbinden. Sie sind dazu auch verpflichtet. Eingriffe ausländischer Stellen, die von deutschem Boden aus vorgenommen werden und die mit Billigung oder Duldung deutscher Stellen erfolgen, sind auch der deutschen öffentlichen Gewalt zuzurechnen. Es geht dann nicht mehr um Vorgänge, die in ihrem wesentlichen Verlauf

ausschließlich von einem fremden Staat nach seinem, von der Bundesrepublik Deutschland unabhängigen Willen gestaltet werden (vgl. BVerfGE 66, 39, 62).

13. Es ist bereits dargelegt worden, dass der sachliche Schutzbereich des Art. 10 GG nicht auf den ersten Zugriff begrenzt ist, mit dem die öffentliche Gewalt von Telekommunikationsvorgängen und Telekommunikationsinhalten Kenntnis nimmt (vgl. BVerfGE 125, 260, 309). Auch die weiteren Vorgänge der Speicherung, Weiterleitung und Verarbeitung, die sich an die Kenntnisnahme von geschützten Vorgängen oder Daten anschließen, sowie jeder Gebrauch, der von der Kenntnis gemacht wird, stellen je eigene Eingriffe in das Grundrecht des Art. 10 GG dar. Damit ist auch eine Verwendung oder ein Gebrauchmachen von Kommunikationsvorgängen durch deutsche Stellen, die zwar von ausländischen Behörden erstmals erhoben, dann aber an deutsche Stellen weitergeleitet werden, ein der deutschen öffentlichen Gewalt zurechenbarer – selbstständiger – Eingriff in das Grundrecht des Art.10 GG und muss dessen Vorgaben und Eingriffsschranken genügen sowie auf einer bereichsspezifischen und normenklaren (Verwendungs-)Ermächtigung des deutschen Gesetzgebers basieren. Entsprechen die ersten Zugriffe auf die durch Art.10 GG geschützten Fernmeldevorgänge und Telekommunikationsinhalte seitens der ausländischen Stellen nicht den Anforderungen, die Art. 10 GG an Einschränkungen des Telekommunikationsgeheimnisses stellt, so haftet dieser Makel auch den nachfolgenden Informations- und Datenverarbeitungsprozessen an. Erfolgen diese durch grundrechtsgebundene Träger deutscher öffentlicher Gewalt, so handeln diese Träger grundrechtswidrig.

14. Von Verfassungs wegen dürfen der Verwendungszweck, zu dem die Erhebung (rechtmäßigerweise) erfolgt ist, und ein veränderter Verwendungszweck, der insbesondere mit einer Übermittlung der Daten an andere Behörden verfolgt wird, nicht miteinander unvereinbar sein (BVerfGE 65, 1, 51, 62; 100, 313, 360). Eine solche Unvereinbarkeit läge vor, wenn grundrechtsgebotene Beschränkungen, etwa der Einsatz

bestimmter Erhebungsmethoden, dadurch umgangen würden, dass Daten, die rechtmäßigerweise zu bestimmten Verwendungszwecken erhoben worden sind, in gleicher Weise auch für Zwecke zugänglich gemacht werden, die einen derartigen Methodeneinsatz oder eine derartige Erhebung nicht rechtfertigen würden. Damit wird zwar nicht jegliche Übermittlung an Behörden ausgeschlossen, denen entsprechende Überwachungsmethoden nicht zustehen. Jedoch setzen solche Übermittlungen bereichsspezifische und normenklare gesetzliche Ermächtigungen voraus. Sie bedürfen ferner einer besonders genauen Überprüfung anhand des Übermaßverbotes (vgl. BVerfGE 100, 313, 390 ff.). Für Übermittlungen von Daten, die durch Eingriffe deutscher Behörden in das Telekommunikationsgeheimnis erlangt worden sind, an ausländische öffentliche Stellen ist deshalb eine bereichsspezifische normenklare gesetzliche Ermächtigung im deutschen Recht zu verlangen. Diese muss auch voraussetzen, dass die weiteren Verwendungen der so erlangten Daten durch die ausländischen Behörden in einer adäquaten rechtsstaatlichen Art und Weise erfolgen.

15. Die Grundrechte des Grundgesetzes verpflichten den Staat nicht nur dazu, sich selbst grundrechtsverletzender Eingriffe zu enthalten, sondern auch einen angemessenen Schutz zu schaffen und durchzusetzen sowie sich auf internationaler und unionsrechtlicher Ebene für ein solches effizientes Schutzregime einzusetzen. Der Grundrechtsschutz allgemein und der des Art.10 GG im Besonderen erschöpft sich auch nach der ständigen Rechtsprechung des Bundesverfassungsgerichts nicht in seinem historischen Gehalt im Sinne subjektiver Abwehrrechte gegenüber staatlichen Eingriffen. Aus den Grundrechten folgen auch Schutzpflichten des Staates für das grundrechtlich geschützte Rechtsgut, deren „Vernächlässigung" von den Betroffenen mit der Verfassungsbeschwerde geltend gemacht werden kann (BVerfGE 125, 39, 78 mit weiteren Nachweisen).

16. Der Staat muss seiner grundrechtlichen Schutzpflicht durch hinreichende Vorkehrungen genügen (BVerfGE 125, 39, 78). Allerdings kann aus dem Verfassungsrecht regelmäßig keine „bestimmte Handlungsvorgabe"

abgeleitet werden (BVerfG a.a.O.). Wie die grundrechtlichen Schutzpflichten erfüllt werden sollen, haben die zuständigen staatlichen Organe, insbesondere der Gesetzgeber, grundsätzlich in eigener Verantwortung zu entscheiden. Der Gesetzgeber hat unter Ausübung seines weiten Einschätzungs-, Wertungs- und Gestaltungsspielraums ein Schutzkonzept aufzustellen und normativ auszugestalten, die rechtsanwendenden Organen der zweiten und dritten Gewalt sind gehalten, dieses effizient umzusetzen. Das Bundesverfassungsgericht wird eine Verletzung von grundrechtlichen Schutzpflichten allerdings nur feststellen können, „wenn Schutzvorkehrungen entweder überhaupt nicht getroffen sind, wenn die getroffenen Regelungen und Maßnahmen offensichtlich ungeeignet oder völlig unzulänglich sind, das gebotene Schutzziel zu erreichen, oder wenn sie erheblich hinter dem Schutzziel zurückbleiben“ (BVerfGE 125, 39, 78/9; vgl. auch BVerfGE 92, 26, 46, mit weiteren Nachweisen). So wird der grundrechtsverpflichtete Staat auch für wirksame Sanktionen bei Verletzungen des Telekommunikationsgeheimnisses Sorge tragen müssen. „Würden auch schwere Verletzungen des Telekommunikationsgeheimnisses im Ergebnis sanktionslos bleiben mit der Folge, dass der Schutz des Persönlichkeitsrechts, auch soweit er in Art. 10 Abs. 1 GG eine spezielle Ausprägung gefunden hat, angesichts der immateriellen Natur dieses Rechts verkümmern würde ... , widerspräche dies der Verpflichtung der staatlichen Gewalt, dem Einzelnen die Entfaltung seiner Persönlichkeit zu ermöglichen ... und ihn vor Persönlichkeitsgefährdungen durch Dritte zu schützen“ (BVerfGE 125, 260, 339 mit weiteren Nachweisen).

Der Gesetzgeber hat hier allerdings – wie gesagt – einen weiten Gestaltungsspielraum. Er kann von Verfassungs wegen auch nicht zu etwas rechtlich und tatsächlich Unmöglichem verpflichtet sein. Bei Grundrechtsverletzungen und Grundrechtsgefährdungen, die von ausländischen Mächten oder international agierenden ausländischen Unternehmen ausgehen, werden die territorialen Grenzen der deutschen öffentlichen Gewalt in Rechnung zu stellen sein. Immerhin könnte hier eine Verschärfung der strafrechtlichen Sanktionierung von unbefugter Datenausspähung und unbefugtem Datenabfangen und auch für diese

Delikte – wie in den Fällen der §§ 5 und 6 StGB – eine gesetzliche Umstellung vom Tatort- auf das Schutzprinzip in Betracht kommen, sodass das deutsche Strafrecht insoweit auch für Taten gelten würde, die im Ausland gegen Deutsche begangen werden, selbst wenn diese Taten am Tatort nicht mit Strafe bedroht sind. Auf nationaler und unionsrechtlicher Ebene sind überdies verschärfte Vorschriften zur Datensicherung bei den Telekommunikationsdienstleistungen anbietenden Unternehmen zu erlassen, und zwar auch für Unternehmen, die zwar ihren Sitz außerhalb Deutschlands bzw. der Europäischen Union haben, aber ihre Dienstleistungen in Deutschland bzw. in der Europäischen Union anbieten.

Schließlich wird man vom deutschen Staat verlangen müssen, dass er sich energisch für bilaterale oder unilaterale Datenschutzabkommen einsetzt, in denen ein Standard rechtlicher Regeln entwickelt und normiert wird, die auf einem gemeinsamen Wertekanon gründen, einem Wertekanon, der den im Wesentlichen übereinstimmenden grundrechtlichen Wertentscheidungen unseres Grundgesetzes, der Grundrechtecharta der Union und den menschenrechtlichen Verbürgungen der Europäischen Menschenrechtskonvention in Fragen des Persönlichkeitsschutzes und des Telekommunikationsgeheimnisses entspricht.

17. Die Schutzpflichten des Staates, die aus dem Telekommunikationsgeheimnis (Art. 10 GG), dem Grundrecht auf informationelle Selbstbestimmung und auf Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) folgen, begründen eine Staatsaufgabe bzw. eine staatliche Verpflichtung zur Gewährleistung von nicht nur funktionsfähigen, sondern auch grundrechtswahrenden informationstechnischen Infrastrukturen, vergleichbar der Gewährleistungsverantwortung für eine flächendeckende angemessene und ausreichende Telekommunikation nach Art. 87 f Abs. 1 GG (vgl. auch *Hoffmann-Riem,* Grundrechts- und Funktionsschutz für elektronisch vernetzte Kommunikation, in: AöR 134 (2009), S. 513, 538 ff.). An eine entsprechende ausdrückliche Verankerung dieses Grundsatzes im Grundgesetz wäre zu denken.

III.

18. Beschränkungen des Telekommunikationsgeheimnisses dürfen nach Art. 10 Abs.2 GG aufgrund Gesetzes angeordnet werden. Der Gesetzesvorbehalt gestattet auch Freiheitsbeschränkungen unmittelbar durch Gesetze. In materieller Hinsicht verlangt das Bundesverfassungsgericht in ständiger Rechtsprechung, dass diese Eingriffe durch Gesetz oder aufgrund Gesetzes legitimen Gemeinwohlzwecken dienen und dem Grundsatz der Verhältnismäßigkeit genügen (vgl. BVerfGE 100, 313, 359; 125, 260, 316). „Die Effektivierung der Strafverfolgung, der Gefahrenabwehr und der Erfüllung der Aufgaben der Nachrichtendienste sind legitime Zwecke, die einen Eingriff in das Telekommunikationsgeheimnis grundsätzlich rechtfertigen können" (BVerfGE 100, 313, 373, 383 f.; 125, 260, 316/7).

19. Der Schutz des Telekommunikationsgeheimnisses nach Art.10 GG enthält einen Menschenwürdekern, dessen Verletzung nicht im Wege der Abwägung mit anderen Rechtsgütern gerechtfertigt werden kann. Dieser Menschenwürdegehalt des Grundrechts führt zu einem absoluten – auch nicht mit hochrangigen Ermittlungsinteressen abwägbaren – Überwachungs- und Erhebungsverbot im Kernbereich privater Lebensgestaltung. Vom Gesetzgeber ist zu verlangen, dass er durch geeignete Vorschriften sicher stellt, dass die Kommunikationsinhalte des höchstpersönlichen Bereichs nicht gespeichert und nicht verwendet, sondern – wenn sie schon unvermeidbar erhoben sein sollten – unverzüglich gelöscht werden.

Es gibt mithin für den grundrechtsbeschränkenden Gesetzgeber im Wesentlichen zwei materiell-verfassungsrechtliche Schranken: eine – engere – Schranke folgt aus der Menschenwürdegarantie, sie gilt absolut und ist abwägungsfest, die andere – weitere – folgt aus dem Verhältnismäßigkeitsgrundsatz, sie unterliegt einer Abwägung und wirkt daher relativ.

20. Aus dem Gebot der Verhältnismäßigkeit im engeren Sinne kann unter bestimmten Voraussetzungen die vollständige Unzulässigkeit bestimmter Grundrechtseingriffe zu Zwecken persönlichkeitsbezogener Ermittlungen folgen. Ein Grundrechtseingriff von hoher Intensität kann bereits als solcher unverhältnismäßig sein, wenn der gesetzlich geregelte Eingriffsanlass kein hinreichendes Gewicht aufweist.

Auch wenn die Schutzgüter einer gesetzlichen Eingriffsermächtigung als solche hinreichend schwergewichtig erscheinen, begründet der Verhältnismäßigkeitsgrundsatz verfassungsrechtliche Anforderungen an die tatsächlichen Voraussetzungen des Eingriffs. Der Gesetzgeber hat insoweit die Ausgewogenheit zwischen der Art und Intensität der Grundrechtsbeeinträchtigung einerseits und den zum Eingriff berechtigenden Tatbestandsvoraussetzungen andererseits zu wahren. Die Anforderungen an den Wahrscheinlichkeitsgrad und an die Tatsachenbasis der Gefahrenprognose müssen in angemessenem Verhältnis zur Art und Schwere der Grundrechtsbeeinträchtigung stehen. Selbst bei höchstem Gewicht der drohenden Rechtsgutbeeinträchtigung kann auf das Erfordernis einer hinreichenden Eintrittswahrscheinlichkeit nicht verzichtet werden. Die gesetzliche Eingriffsgrundlage beispielsweise für einen heimlichen Zugriff auf informationstechnische System muss vorsehen, dass zumindest tatsächliche Anhaltspunkte einer konkreten Gefahr für die hinreichend gewichtigen Schutzgüter bestehen. Bloße Vermutungen oder allgemeine Erfahrungssätze allein reichen nicht aus, um diesen Zugriff zu rechfertigen. Vielmehr müssen bestimmte Tatsachen festgestellt werden, die eine Gefahrenprognose tragen. Dem Gewicht des Grundrechtseingriffs, der in dem heimlichen Zugriff liegt, wird nicht hinreichend Rechnung getragen, wenn der tatsächliche Eingriffsanlass noch weitgehend in das Vorfeld einer im Einzelnen noch nicht absehbaren konkreten Gefahr für die zu schützenden Rechtsgüter vorverlegt wird (vgl. BVerfGE 120, 274, 326 ff.).

21. Die strategischen Beschränkungen des Fernmeldegeheimnisses durch den Bundesnachrichtendienst finden auf der Grundlage der §§ 5 ff. G 10 statt. Sie dienen nicht der gezielten Erfassung bestimmter

Fernmeldeanschlüsse oder –beziehungen, sondern dienen in erster Linie der präventiven Aufklärung und Analyse von gesetzlich näher umschriebenen Gefahrenlagen (§ 5 Abs.1 Satz 3 G 10). Es geht insofern also auch um eine anlass- bzw. verdachtslose Überwachungsmaßnahme (siehe *Badura*, in: Bonner Kommentar, Art.10 GG, Rn.84) zur Früherkennung bestimmter aus dem Ausland drohender schwerer Gefahren für die Bundesrepublik Deutschland und zur Unterrichtung der Bundesregierung. Das Bundesverfassungsgericht hat die frühere Ermächtigungsnorm in § 3 G 10 a.F. (jetzt § 5 G 10) grundsätzlich für verfassungsgemäß erachtet. Der Verhältnismäßigkeitsgrundsatz wurde überwiegend als gewahrt erachtet, weil keine voraussetzungslose Erfassung sämtlicher Fernmeldekontakte bestimmter Grundrechtsträger erfolgt und Überwachung und Aufzeichnung des Fernmeldeverkehrs sowohl rechtlich als auch tatsächlich begrenzt seien (BVerfGE 100, 313, 376). In diesem Zusammenhang wurde darauf hingewiesen, dass allein der internationale nicht-leitungsgebundene Verkehr überwacht werden könne. Andererseits war zu berücksichtigen, dass die Gefahren, über die Erkenntnisse gewonnen werden sollen, sehr viel weiter gezogen worden waren und damit auch die Anonymität der Kommunikation nicht mehr in derselben Weise gewahrt werden konnte wie unter der alten Regelung. Aber auch der erweiterte Katalog der Gefahren fand prinzipiell die Billigung des Bundesverfassungsgerichts. Es handelt sich im Wesentlichen um schwerwiegende Gefahren, auch soweit es nicht nur um die Gefahren eines bewaffneten Angriffs, sondern beispielsweise auch um die des internationalen Terrorismus geht. Lediglich die Abwehr von Gefahren der im Ausland begangenden Geldfälschungen ist vom Bundesverfassungsgericht als nicht hinreichend gewichtig angesehen worden, um den schwerwiegenden Eingriff in das Telekommunikationsgeheimnis zu rechtfertigen.

22. Nur der begrenzte Verwendungszweck der strategischen Überwachung, die der Bundesnachrichtendienst vornehmen darf und die nicht auf Maßnahmen gegenüber bestimmten Personen abzielt, sondern internationale Gefahrenlagen betrifft, über die die Bundesregierung unterrichtet werden soll, rechtfertigt nach Auffassung des

Bundesverfassungsgerichts die Breite und Tiefe der Eingriffe in das Telekommunikationsgeheimnis. „Zielte sie von vorne herein auf Zwecke der Verhinderung oder Verfolgung von Straftaten, ließe sich die Befugnis dazu nicht mit Art.10 GG vereinbaren“ (BVerfGE 100, 313, 389). Deshalb müssen an die Übermittlung der auf diese Weise erlangten personenbezogenen Daten an andere Behörden, denen – wie den Strafverfolgungsbehörden und der Polizei – eine verdachtslose Telekommunikationsüberwachung nicht zusteht und auch nicht zugestanden werden darf, aus verfassungsrechtlichen Gründen besonders gesteigerte Anforderungen gestellt werden. Es muss ein Rechtsgut in Rede stehen, dem ein besonders hohes Gewicht zukommt. Zwingend geboten ist überdies eine „hinreichende Tatsachenbasis für den Verdacht, dass Straftaten geplant oder begangen werden“ (BVerfGE 100, 313, 329). Die früheren Übermittlungsvorschriften im G 10 genügten diesen gesteigerten Anforderungen nicht (vgl. jetzt § 7 G 10).