Sarah Thomé

# Massenhafte Datensammlungen vor Gericht*

Schon mehrmals mussten sich deutsche und europäische Gerichte mit der Frage beschäftigen, ob bestimmte Praktiken der Sicherheitsbehörden mit den Grundrechten vereinbar sind. Hierzu zählt insbesondere die massenhafte und größtenteils anlasslose Erhebung von personenbezogenen Daten. Der folgende Beitrag von Sarah Thomé skizziert und vergleicht die Rechtsprechung des Bundesverfassungsgerichts und des Europäischen Gerichtshofs (EuGH) in diesem Bereich.

## 1. Überwachung: Vom Mittel zum Selbstzweck

In der aktuellen politischen Diskussion um den gesetzgeberischen Handlungsbedarf zur wirksamen Bekämpfung des internationalen Terrorismus lässt sich teilweise schwer ausmachen, ob die zahlreichen geforderten Maßnahmen noch einem legitimen Zweck dienen. So steht selbst bei der von der NSA praktizierten Massenüberwachung nicht wirklich fest, ob die gespeicherten Daten überhaupt einen nennenswerten Beitrag zur Aufklärung oder Verhinderung von Straftaten oder gar terroristischen Anschlägen beitragen können. Laut einer Studie der *New America Foundation*[1] ist der Nutzen dieser Daten im Vergleich zu traditionellen Ermittlungsmethoden von geringer Bedeutung. Teilweise entsteht der Eindruck, dass die Möglichkeit der besseren Kontrolle als Selbstzweck verstanden wird. Dieser Haltung entspringt letztlich auch die Massenüberwachung durch amerikanische Geheimdienste. Hier hat sich der Glaube manifestiert, dass allein die Möglichkeit, auf sämtliche Kommunikationsdaten zuzugreifen, einen Mehrwert schafft.

Bei der juristischen Bewertung massenhafter Datensammlungen stoßen die Gerichte auf erhebliche dogmatische Schwierigkeiten, insbesondere wenn sie die Verhältnismäßigkeit derartiger Datenerhebungen beurteilen sollen. Dieser Aufsatz soll beispielhaft anhand verschiedener Urteile des Bundesverfassungsgerichts und des Europäischen Gerichtshofs (EuGH) zeigen, wie diese Gerichte auf derartige Herausforderungen reagiert haben. Dabei wird sich zeigen, dass ein effektiver Grundrechtsschutz nur dann gewährleistet wird, wenn erstens die Eingriffsvoraussetzungen schon bei der Er-

* Sarah Thomé ist Referentin bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit. Der Aufsatz gibt ausschließlich ihre eigene Meinung wieder. Rosemarie Will dankt sie für die wertvollen Erklärungen zur Rechtsprechung des Bundesverfassungsgerichts zu anlasslosen Datenerhebungen.

hebung der Daten und nicht erst bei ihrem Abruf vorliegen müssen und zweitens geprüft wird, ob zwischen dem Zweck und den zu erhebenden Daten tatsächlich ein enger Zusammenhang im Sinne einer „Notwendigkeit" besteht.

## 2. Rechtsprechung des Bundesverfassungsgerichts

In der Rechtsprechung des Bundesverfassungsgerichts zur Frage der Zulässigkeit staatlicher Überwachungsmaßnahmen zeigt sich, dass das Gericht einige Anstrengungen unternommen hat, um die Verhältnismäßigkeit neuer staatlicher Befugnisse zur Datenerhebung bestimmen zu können. Die Verhältnismäßigkeitsprüfung[2] wurde hinsichtlich der Bestimmung der Schwere des Eingriffs immer wieder um Kriterien ergänzt, die den Besonderheiten staatlicher Überwachungsmaßnahmen im Kontext der Terrorismusbekämpfung gerecht werden sollten. Es zeigen sich aber gravierende dogmatische Probleme, die letztlich zu einer Schwächung des Grundrechtsschutzes und zu einer teilweisen Rechtfertigung von anlasslosen Datenspeicherungen geführt haben.

Zunächst begegnet man bei der Prüfung massenhafter Datenerhebungen zwangsläufig den strukturellen Problemen des Verhältnismäßigkeitsgrundsatzes: Dieser vermag angesichts terroristischer Gefahren vieles zu rechtfertigen, denn die Geeignetheit einer Maßnahme wird schon dann bejaht, wenn der Zweck auf eine bestimmte Art und Weise gefördert wird. Es muss aber nicht belegt sein, dass der Zweck erreicht wird. So überstand etwa die Vorratsdatenspeicherung diesen Test, obwohl ihr Nutzen immer noch nicht belegt werden konnte.[3] Darüber hinaus sind Entwicklungen dahingehend zu beobachten, dass bestimmte Datenerhebungen gar nicht mehr als Eingriffe gewertet werden und dass das Verbot der anlasslosen Speicherung von Daten auf Vorrat ausgehebelt wurde. Schließlich verliert auch der Zweckbindungsgrundsatz immer mehr an Substanz.

All dies kommt dem Ansinnen entgegen, dass massenhafte Datensammlungen, wie sie beispielsweise die NSA praktiziert, nicht mehr als rechtfertigungsbedürftige Eingriffe in Grundrechte gewertet werden. Auch in der Rechtsprechung des Bundesverfassungsgerichts finden sich Tendenzen dahingehend, dass das ursprüngliche Verbot der anlasslosen Speicherung von Daten auf Vorrat verwässert oder übergangen wird, indem bei der Prüfung nunmehr der Fokus auf die anschließende Verwendung, also den Abruf der Daten, abgestellt wird. Diese Entwicklung soll hier beispielhaft anhand dreier Entscheidungen verdeutlicht werden.

### 2.1. Telekommunikationsüberwachung I (1999)

In seiner Entscheidung zur Telekommunikationsüberwachung I[4] aus dem Jahr 1999 hat das Bundesverfassungsgericht die rechtlichen Grenzen nachrichtendienstlicher Befugnisse zur Telekommunikationsüberwachung noch klar benannt: „Beschränkungen des Fernmeldegeheimnisses sind zwar gemäß Art. 10 Abs. 2 GG möglich. Sie be-

dürfen aber nicht nur, wie jede Grundrechtsbeschränkung, einer gesetzlichen Regelung, die einen legitimen Gemeinwohlzweck verfolgt und im Übrigen den Grundsatz der Verhältnismäßigkeit wahrt. (...) Insbesondere muß der Zweck, zu dem Eingriffe in das Fernmeldegeheimnis vorgenommen werden dürfen, bereichsspezifisch und präzise bestimmt werden, und das erhobene Datenmaterial muß für diesen Zweck geeignet und erforderlich sein. Eine Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken wäre damit unvereinbar. Speicherung und Verwendung erlangter Daten sind daher grundsätzlich an den Zweck gebunden, den das zur Kenntnisnahme ermächtigende Gesetz festgelegt hat."[5]

Der letzte Absatz dieses Zitats beinhaltet drei Kriterien: (1) Der Zweck, zu dem die Daten erhoben werden, muss genau bestimmt sein. (2) Die erhobenen Daten müssen für diesen Zweck geeignet und erforderlich sein. (3) Es gilt ein Verbot der Sammlung von Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken. Hier wird deutlich, dass das Gericht auf die Erhebung der Daten abstellt und nicht auf die spätere Verwendung. Für die Frage der Verhältnismäßigkeit einer derartigen Befugnis zur Telekommunikationsüberwachung komme es darüber hinaus darauf an, wie viele Personen betroffen seien, wie schwer der Eingriff für die Einzelnen wiege und wie der Gesetzgeber die Einschreitschwellen[6] ausgestaltet habe.[7]

## 2.2. Rasterfahndung (2006)

In der Entscheidung zur Rasterfahndung[8] prüfte das Bundesverfassungsgericht eine staatliche Befugnis, die im Kontext der Terrorismusbekämpfung steht und es erlaubte, Daten, die bei anderen Stellen vorhanden waren, zusammenzuführen und nach bestimmten Kriterien zu filtern, um dadurch „Schläfer" aufdecken zu können. In dieser Entscheidung zeigt sich zunächst die Schwäche, die der Verhältnismäßigkeitsprüfung innewohnt, wenn es um die Prüfung der Geeignetheit und Erforderlichkeit von Maßnahmen im Kontext der Terrorismusbekämpfung geht. So heißt es zu diesen Prüfungspunkten in der Entscheidung lediglich:

„Mit der Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person verfolgt die Regelung einen legitimen Zweck. Das Mittel der Rasterfahndung ist zur Verfolgung dieses Zweckes auch geeignet. Ein Gesetz ist zur Zweckerreichung geeignet, wenn mit seiner Hilfe der erstrebte Erfolg gefördert werden kann (...) Das ist vorliegend der Fall. Die Eignung scheitert nicht etwa an der großen Streubreite der Erfassungsmethode, die nur in vergleichsweise wenigen Fällen Erkenntnisse verspricht (vgl. BVerfGE 100, 313 [373]). Der Eingriff ist auch erforderlich zur Verfolgung des gesetzgeberischen Zweckes. Dieser lässt sich nicht durch mildere Mittel ebenso wirksam erreichen."[9]

Das Gericht kommt an dieser Stelle jedweder Kritik zuvor, indem es selbst darauf hinweist, dass es für die Geeignetheit einer Maßnahme unerheblich ist, wenn sie nur in sehr wenigen Fällen zum Erfolg führt. Es genügt, wenn ein irgendwie gearteter Zusammenhang zwischen Mittel und Zweck besteht. Betrifft die Rasterfahndung etwa 80 Millionen Menschen und führt potenziell zu einem Treffer, so ist sie bereits geeignet. Das Bundesverfassungsgericht versucht diesen Umstand durch eine besonders stren-

ge Verhältnismäßigkeitsprüfung auszugleichen, indem es die zu Art. 10 Abs. 1 und Art. 13 Abs. 1 GG definierten Kriterien auch auf das Recht auf informationelle Selbstbestimmung anwendet, das bei der Rasterfahndung betroffen ist. Es macht außerdem deutlich, dass zumindest eine hinreichend konkrete Gefahr für die bedrohten Rechtsgüter bestehen muss. Die Schwere des Eingriffs bemisst sich außerdem nach dem Inhalt der Kommunikation, der Verknüpfungsmöglichkeit der Daten und danach, ob es sich um sensible und besonders geschützte Arten personenbezogener Daten handelt. Die Nachteile, die sich aus der Maßnahme ergeben, bestimmen sich danach, ob sie falsche Verdächtigungen oder eine Stigmatisierung der Betroffenen nach sich ziehen kann. Weniger Schwierigkeiten hat das Gericht mit dem Umstand, dass die Daten ursprünglich zu vollkommen anderen Zwecken erhoben wurden. Es setzt sich zwar damit auseinander, dass eine derartige Zweckänderung auch eine anlasslose Speicherung von Daten auf Vorrat ermöglichen kann. Soweit aber eine konkrete Gefahr besteht, hat es keine Bedenken gegen diese Zweckänderung. Problematisch ist, dass der Zweck vor der Erhebung der Daten bestimmt sein sollte. Es wäre hier also nicht auf die Ermächtigung zur Rasterfahndung abzustellen, sondern auf die ursprüngliche Erhebung der Daten. Denn nur so würde dem Umstand Rechnung getragen, dass aus einer derartigen Maßnahme auch gravierende Nachteile für die Betroffenen resultieren können, wie zum Beispiel falsche Verdächtigungen. Fordert man diesen Zusammenhang nicht, so akzeptiert man, dass jede Person ständig damit rechnen muss, dass über sie gespeicherte Daten in der Zukunft einmal anderweitig, etwa im Rahmen polizeilicher Ermittlungsmaßnahmen, genutzt werden können. Dies gilt auch dann, wenn man selbst keinerlei Anlass dazu gegeben hat, in den Fokus derartiger Ermittlungen zu gelangen.

Die Entscheidung zur Rasterfahndung verdeutlicht einerseits die weitere Ausdifferenzierung des Verhältnismäßigkeitsgrundsatzes und die Besorgnis des Gerichts, dass mit dem technologischen Fortschritt tiefere Eingriffe in die Privatsphäre ermöglicht werden. In den Fokus der Verhältnismäßigkeitsprüfung geraten so die Nachteile, die unbeteiligte Dritte erleiden können, wenn sie fälschlicherweise verdächtigt werden. Gleichzeitig wird aber deutlich, dass der Weg für einen massenhaften Abgleich vorgehaltener Daten geebnet wird, weil die Zweckbindung unterlaufen wird. Dadurch wird auch das Risiko falscher Verdächtigungen zum notwendigen Kollateralschaden degradiert.

### 2.3. Vorratsdatenspeicherung (2010)

Mit der Einführung der Vorratsdatenspeicherung sahen viele bereits den Punkt erreicht, an dem vom Fernmeldegeheimnis „nichts mehr übrig bleiben würde“, denn diese erlaubte zum damaligen Zeitpunkt die anlasslose Speicherung der Verkehrsdaten sämtlicher Kommunikationsteilnehmer für einen Zeitraum von sechs Monaten.[10] Das Bundesverfassungsgericht teilte diese Auffassung nicht, weil die staatlichen Stellen nicht vom Inhalt der Kommunikation Kenntnis erlangen. Es hält die Einführung der Speicherung von Daten auf Vorrat „ausnahmsweise“ für verhältnismäßig und daher zulässig: „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 (...). Dabei liegt eine illegitime, das Freiheitsprinzip des Art. 10 Abs. 1 GG selbst aufhebende Zielsetzung nicht schon darin, dass die Telekommunikationsverkehrsdaten anlasslos vorsorglich gesichert werden sollen. Art. 10 Abs. 1 GG verbietet nicht jede vorsorgliche Erhebung und Speicherung von Daten überhaupt, sondern schützt vor einer unverhältnismäßigen Gestaltung solcher Datensammlungen und hierbei insbesondere vor entgrenzenden Zwecksetzungen. Strikt verboten ist lediglich die Speicherung von personenbezogenen Daten auf Vorrat zu unbestimmten und noch nicht bestimmbaren Zwecken (vgl. BVerfGE 65, 1 [46]; 100, 313 [360]).“[11]

Das Bundesverfassungsgericht beruft sich bei seiner Verhältnismäßigkeitsprüfung darauf, dass die Vorratsdatenspeicherung zwar anlasslos, aber zu möglicherweise bestimmten Zwecken erfolgt. So heißt es: „Allerdings entspricht es der ständigen Rechtsprechung des BVerfG, dass dem Staat eine Sammlung von personenbezogenen Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken verfassungsrechtlich strikt untersagt ist (...). Um eine solche von vornherein verbotene Form der Datensammlung handelt es sich bei einer vorsorglich anlasslosen Speicherung der TK-Verbindungsdaten nicht in jedem Fall. Erfolgt sie zu bestimmten Zwecken, kann eine solche Speicherung eingebunden in eine dem Eingriff adäquate gesetzliche Ausgestaltung (s. unten V) vielmehr auch den Verhältnismäßigkeitsanforderungen im engeren Sinne genügen.“[12] Hier wird also in gewisser Weise nur unterstellt, dass diese Zwecke vorliegen. Erst recht geht das Gericht nicht mehr auf die Frage ein, ob die Speicherung zu unbestimmten Zwecken erfolgt, denn es verweist dann nur auf den Abruf der Daten: „Der Abruf der Daten seitens staatlicher Stellen erfolgt erst in einem zweiten Schritt und nunmehr anlassbezogen nach rechtlich näher festgelegten Kriterien. Die Ausgestaltung der zum Abruf und zur weiteren Verwendung der gespeicherten Daten ermächtigenden Bestimmungen kann dabei sicherstellen, dass die Speicherung nicht zu unbestimmten oder noch nicht bestimmbaren Zwecken erfolgt.“[13]

Mit der Zulässigkeit der anlasslosen Erfassung von Daten wird auch das Kriterium der „Ausgestaltung der Eingriffsschwelle“ zumindest für die Speicherung (nicht für den Abruf) der Daten aufgegeben. Weiterhin werden trotz der hohen Streubreite und der Anlasslosigkeit der Vorratsdatenspeicherung keine gesteigerten Anforderungen an deren Geeignetheit oder Erforderlichkeit gestellt. Problematisch erscheint darüber hinaus, dass die Verhältnismäßigkeit mit Bedingungen verknüpft wird, die im Prinzip in der Zukunft liegen: „Die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten setzt vielmehr voraus, dass diese eine Ausnahme bleibt.“[14] Das Gericht verpflichtet den Gesetzgeber „(...) bei der Erwägung neuer Speicherungspflichten oder -berechtigungen in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen zu größerer Zurückhaltung.“[15] Die Verhältnismäßigkeit der Vorratsdatenspeicherung bemisst sich somit danach, ob der Gesetzgeber die „Überwachungsgesamtrechnung“[16] klein hält. Bei zukünftigen Maßnahmen soll nunmehr eine doppelte Verhältnismäßigkeitsprüfung durchgeführt werden: „Zum einen ist auf der Grundlage der Wirkungen eines Überwachungsinstruments dessen verhältnismäßiger Einsatz zu bewerten. Zum anderen ist aber zusätzlich auf der Basis einer Gesamtbetrachtung aller verfügbaren staat-

lichen Überwachungsmaßnahmen die Verhältnismäßigkeit der Gesamtbelastungen bürgerlicher Freiheiten zu prüfen. Danach kann der Gesetzgeber Überwachungsmaßnahmen eventuell nur austauschen, aber nicht kombinieren."[17] Positiv an diesem Gedanken ist, dass Überwachungsmaßnahmen nicht isoliert, sondern in einem gesamtgesellschaftlichen Kontext gesehen werden. In der Praxis scheint dieses Konzept, das auf eine Selbstbeschränkung des Gesetzgebers setzt, aber wenig erfolgversprechend.

Ein weiterer kritikwürdiger Punkt besteht darin, dass das Bundesverfassungsgericht die Vorratsdatenspeicherung als weniger belastend für die Bürger ansieht, weil die Daten bei den privaten Anbietern und nicht von staatlichen Stellen erhoben werden: „Maßgeblich ist hierfür zunächst, dass die vorgesehene Speicherung der TK-Verkehrsdaten nicht direkt durch den Staat, sondern durch eine Verpflichtung der privaten Diensteanbieter verwirklicht wird. Die Daten werden damit bei der Speicherung selbst noch nicht zusammengeführt, sondern bleiben verteilt auf viele Einzelunternehmen und stehen dem Staat unmittelbar als Gesamtheit nicht zur Verfügung." Diese Aussage muss angesichts der Snowden-Enthüllungen angezweifelt werden.

## 3. Rechtsprechung des Europäischen Gerichtshofs

### 3.1. Vorratsdatenspeicherung (2014)

Datenschutz wurde auf Ebene der Europäischen Union lange Zeit allein unter dem Blickwinkel des freien Warenverkehrs diskutiert. Inwieweit die Union in der Lage sein würde, den in der Grundrechte-Charta verbürgten Schutz der Privatsphäre und der persönlichen Daten zu garantieren, stellten viele in Frage. Schon in der Entscheidung des EuGH zur Vorratsdatenspeicherung[18] hat sich jedoch gezeigt, dass das Gericht sehr strenge Voraussetzungen an die Zulässigkeit von Eingriffen in die Privatsphäre stellt.[19] Zwar sah auch der EuGH den Wesensgehalt der betroffenen Grundrechte nicht als verletzt an, da nicht auf den Inhalt der Kommunikation zugegriffen wurde,[20] er stellte jedoch die Erforderlichkeit der anlasslosen Speicherung in Frage. Das Unionsrecht verlange, dass staatliche Eingriffe auf das Notwendigste begrenzt blieben. Im Kontext der Vorratsdatenspeicherung sei dieses Kriterium nicht eingehalten worden, da die Speicherpflicht unterschiedslos sämtliche Personen betreffe, unabhängig davon, ob diese durch ihr Verhalten Anlass zu einer staatlichen Überwachungsmaßnahme gegeben haben oder nicht.[21] Darüber hinaus kritisierte der EuGH, dass es keinen unmittelbaren Zusammenhang zwischen der Auswahl der zu erhebenden Daten und dem Zweck der Richtlinie gebe: „(D)ie Richtlinie (soll) zwar zur Bekämpfung schwerer Kriminalität beitragen, verlangt aber keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit; insbesondere beschränkt sie die Vorratsspeicherung weder auf die Daten eines bestimmten Zeitraums und/oder eines bestimmten geografischen Gebiets und/oder eines bestimmten Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte

Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten."[22] Der EuGH macht an dieser Stelle deutlich, dass es nicht genügt, einen legitimen Zweck für die Einführung staatlicher Überwachungsmaßnahmen zu nennen, es muss auch einen konkreten Zusammenhang zwischen den zu erhebenden Daten sowie den Betroffenen und diesem Zweck geben. Somit sind seine Anforderungen an die Verhältnismäßigkeit wesentlich strenger als die des Bundesverfassungsgerichts, das erst beim Zugriff auf die Daten einen konkreten Anlass fordert, wie dies am Beispiel der Vorratsdatenspeicherung beschrieben wurde. Der EuGH prüft folglich strikt, ob die Daten für den angestrebten Zweck notwendig sind. Eine anlasslose Erhebung von Daten, die später zu Zwecken der Strafverfolgung genutzt werden können, erachtet er als unzulässig.[23]

## 3.2. Safe Harbor (2015)

Das *Safe Harbor*-Urteil des EuGH betrifft die Übermittlung von personenbezogenen Daten in die USA. Gegenstand des Urteils war eine Entscheidung der Europäischen Kommission, die die Datenübermittlung in die USA unter den im *Safe Harbor*-Abkommen festgelegten Grundsätzen für zulässig erklärte. Anlass für das Verfahren bot die Tatsache, dass amerikanische Unternehmen sich zwar gemäß des *Safe Harbor*-Abkommens zu bestimmten Maßnahmen verpflichteten, um personenbezogene Daten von Europäern zu schützen, amerikanische Behörden jedoch trotz dieser Zusicherungen ungehindert auf die personenbezogenen Daten von Europäern zugreifen konnten, die bei amerikanischen Unternehmen gespeichert waren. Da die amerikanischen Behörden auf diesem Weg auch Zugriff auf den Inhalt der Kommunikation erhielten, sah der EuGH den Wesensgehalt der Privatsphäre als verletzt an: „Insbesondere verletzt eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des durch Art. 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens (...)."[24]

An der Entscheidung des EuGH ist besonders bemerkenswert, dass sie die Verletzung des Wesensgehalts nicht daran festmacht, ob eine staatliche Befugnis zur Erhebung bestimmter Daten das Recht auf Privatsphäre verletzt, sondern daran, dass eine Regelung eingeführt wurde, die im Ergebnis dazu führt, dass personenbezogene Daten unbeschränkt den staatlichen Stellen eines anderen Landes zugänglich gemacht werden. In dieser Konstellation geht es nicht darum, dass sich die Europäische Kommission oder die Mitgliedsstaaten selbst Zugriff auf die Kommunikation der EU-Bürger verschafft haben, sondern die Kommission hat eine Regelung eingeführt, die EU-Bürger gegenüber dem Zugriff amerikanischer Geheimdienste schutzlos stellt. Dieser Aspekt fand in der Rechtsprechung zu Eingriffen in die Privatsphäre und bei der Prüfung der Verhältnismäßigkeit bislang wenig Beachtung.

## 4. Vergleich

Das Bundesverfassungsgericht hat in den vergangenen Jahren wieder und wieder versucht, staatlichen Überwachungsmaßnahmen durch zusätzliche Kriterien und strengere Prüfungsmaßstäbe im Rahmen der Verhältnismäßigkeitsprüfung Grenzen zu setzen. In der Entscheidung zur Vorratsdatenspeicherung hat sich gezeigt, dass die Grenze dessen erreicht wurde, was das Gericht, wenn auch nur „ausnahmsweise", für zulässig erachten konnte. Mit der Verdopplung der Verhältnismäßigkeitsprüfung im Rahmen der „Überwachungsgesamtrechnung" zeigte das Gericht, dass ein Niveau erreicht wurde, das mit einer einfachen Prüfung nicht mehr angemessen beurteilt werden konnte. Darüber hinaus deutet sich an, dass das Gericht weder einen sehr strengen Zusammenhang zwischen dem Zweck der Maßnahme und den erhobenen Daten fordert, noch den Zweckbindungsgrundsatz streng prüft. Das eine oder das andere wäre aber notwendig, um eine Erosion des Grundrechtsschutzes angesichts massenhafter Datenerhebungen zu verhindern. Nach diesen Kriterien ist der Weg geebnet für die Zulässigkeit massenhafter Datensammlungen auf Vorrat.

Der EuGH ist einige Zeit später einen anderen Weg gegangen. Zur Vorratsdatenspeicherung hat er deutlich gemacht, dass die undifferenzierte, anlasslose Erhebung von personenbezogenen Daten nicht auf das Notwendigste beschränkt und daher unzulässig ist. Der EuGH prüft hier wesentlich strenger als das Bundesverfassungsgericht, ob schon die Daten, die erhoben werden, dem Zweck der Maßnahme dienen. Damit scheinen zum einen anlasslose Datenerhebungen auf Vorrat europarechtlich unzulässig, zum anderen zeigt der EuGH deutlich, dass schon das Bereithalten der Daten einen Eingriff darstellt, über den man bei der Prüfung nicht mit dem Verweis hinweg gehen kann, dass der Anlass in der zweiten Stufe, nämlich beim Abruf der Daten geregelt sein muss. Damit kommt der EuGH all denjenigen zuvor, die davon ausgehen, dass das alleinige „Vorhalten" der Daten keinen Grundrechtseingriff darstelle.

Das Safe Harbor-Abkommen hat der EuGH kurz und knapp für mit dem Wesensgehalt der Privatsphäre und dem Recht auf Datenschutz unvereinbar erklärt, weil es den staatlichen Stellen eines Drittstaates den ungehinderten Zugriff auf personenbezogene Daten von Europäern ermöglicht. Der EuGH hat hier staatlichen Überwachungsmaßnahmen eine klare Grenze gesetzt. Weitere Grenzen setzen der Kernbereich privater Lebensgestaltung und das Verbot der Totalüberwachung[25]. Darüber hinaus zeigt diese Entscheidung, dass es nicht darauf ankommt, dass der Staat die Daten selbst erhebt. Es genügt vielmehr, wenn er eine Regelung schafft, die anderen Stellen den unbegrenzten Zugriff auf personenbezogene Daten ermöglicht.

Massenhafte Datenerhebungen vor Gericht: Das Bundesverfassungsgericht und der EuGH kommen hier gegenwärtig zu unterschiedlichen Ergebnissen. Im Sinne des Grundrechtsschutzes zu überzeugen vermag derzeit in dieser Frage nur der EuGH, denn dieser hat in seiner Rechtsprechung deutlich gemacht, dass massenhafte anlasslose Datenerhebungen mit den Grundrechten unvereinbar sind.

**DR. SARAH THOMÈ** Jahrgang 1982, studierte Rechtswissenschaften in Berlin und Oslo. Von 2012 bis 2014 war sie Referentin für Telekommunikationspolitik beim BITKOM e.V. 2014 promovierte sie mit einer Arbeit zur „Reform der Datenschutzaufsicht“; 2014/15 lehrte sie als Gastdozentin Staatsrecht an der Berliner Hochschule für Wirtschaft und Recht. Seit diesem Jahr ist sie Referentin bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit. Thomé gehört dem Bundesvorstand der Humanistischen Union an, wo sie für Datenschutzrecht und Netzpolitik zuständig ist.

## Anmerkungen:

1 MMR-Aktuell 2014, 355514.
2 Ob eine staatliche Maßnahme im Einzelfall verhältnismäßig ist, beurteilt sich danach, ob die einschränkende Maßnahme erforderlich, geeignet und angemessen ist. Im Wesentlichen gilt es zu überprüfen, ob eine gesetzliche Regelung, die Eingriffe in die Grundrechte erlaubt, einen legitimen Zweck fördert (Geeignetheit), ob es ein milderes gleich geeignetes Mittel gibt (Erforderlichkeit), und ob die Beschränkung im Verhältnis zum angestrebten Zweck angemessen ist (Verhältnismäßigkeit i.e.S.).
3 So weisen eine Studie des Max-Planck-Instituts und ein Gutachten des wissenschaftlichen Dienstes des Bundestages darauf hin, dass die Aufklärungsquote durch die Vorhaltung der Daten auf Vorrat nicht nachweisbar verbessert werden konnte, bzw. dass durch den Wegfall der Speicherpflicht keine Schutzlücke entsteht (s. MMR-Aktuell 2012, 328594). Auch nach „Angaben der EU-Kommission haben nur elf von 27 Mitgliedsstaaten Beweise für die Wirksamkeit im Einzelfall der Speicherung von Verkehrsdaten auf Vorrat zur Bekämpfung des Terrorismus, schwerer Kriminalität oder von mittels Telekommunikation begangenen Straftaten vorlegen können. Auch lässt sich den Aussagen der Bedarfsträger nicht entnehmen, ob die benötigten Verkehrsdaten bei den Providern auch ohne Verpflichtung zur Vorratsdatenspeicherung vorhanden sind.“ (MMR-Aktuell 2012, 327192).
4 BVerfGE 100, 313 ff.
5 BVerfGE 100, 313 (359 f.).
6 D.h. die tatbestandlichen Voraussetzungen, die für das Tätigwerden der staatlichen Stellen erfüllt sein müssen (im Polizeirecht i. d . R. das Vorliegen einer Gefahr).
7 BVerfGE 100, 313 (376 f.).
8 BVerfGE 115, 320.
9 BVerfGE 115, 320 (345).
10 So etwa die Einschätzungen des Bundesbeauftragten und des Berliner Beauftragten für Datenschutz und Informationsfreiheit in ihren jeweiligen Stellungnahmen zum Verfahren, vgl. BVerfGE 125, 260 (300 f.).
11 BVerfGE 125, 260 (360 f.).
12 BVerfGE 125, 260 (316 f.).
13 BVerfGE 125, 260 (361 f.)
14 BVerfGE 125, 260 (323 f).
15 BVerfGE 125, 260 (324 f).
16 Dazu ausführlich: Roßnagel: Die „Überwachungs-Gesamtrechnung” – Das BVerfG und die Vorratsdatenspeicherung, NJW 2010, S. 1238 ff.
17 Roßnagel NJW 2010, S. 1240.

18 EuGH, Entscheidung vom 8. April 2014, Digital Rights Ireland Ltd (C-293/12).
19 Vgl. Kühling: Der Fall der Vorratsdatenspeicherungsrichtlinie und der Aufstieg des EuGH zum Grundrechtsgericht, NVwZ 2014, S. 681 ff.
20 EuGH, A.a.O. Rn. 40.
21 A.a.O. Rn. 58.
22 A.a.O., Rn. 59.
23 Eine ausführliche Beschreibung der Auswirkungen des Urteils findet sich bei: Boehm/Cole: Data Retention after the Judgement of the Court of Justice of the European Union, 2014.
24 EuGH, Urteil vom 6. Oktober 2015 C-362/14, Rn. 94.
25 Dazu im Kontext der Vorratsdatenspeicherung durch TK und Fluggastdaten s. Knierim: Kumulation von Datensammlungen auf Vorrat - Vorratsspeicherung von TK- und Fluggastdaten und das Verbot umfassender Überwachung, ZD 2011, S. 17 ff.