Mit Europarecht gegen die amerikanischen und britischen Abhöraktionen? Teil 2: GCHQ

Franz C. Mayer

18.11.2013 doi: 10.17176/20171006-143709

Neben der amerikanischen NSA, aber wohl teilweise in Absprache und Zusammenarbeit mit den USA, sammelt offenbar auch der britische technische Nachrichtendienst Government Communications Headquarters (GCHQ) in großem Stil flächendeckend und anlasslos Verbindungsdaten und Kommunikationsinhalte aus allen Formen moderner Telekommunikation. Bekannt geworden sind insbesondere die Aktivitäten unter dem Projektnamen Tempora durch Veröffentlichungen der Washington Post und des Guardian nach Informationen durch vormals für die NSA tätigen Edward Snowden. Es geht dabei zuvörderst um das Ausleiten von Daten aus den Datenkabeln die auf britischem Hoheitsgebiet oder auf dem Meeresboden verlaufen.

Anders als bei den USA erscheint hier der Konnex zum Europarecht nicht sonderlich fernliegend. Großbritannien ist seit 1973 Mitglied der EWG bzw. heute der EU. Die verdeckte, systematische, großflächige und anlasslose Sammlung von personenbezogenen Daten von Unionsbürgern durch einen Mitgliedstaat berührt Garantien, wie sie in Art. 8 Charta der Grundrechte sowie in Art. 16 AEUV und im geltenden Sekundärrecht niedergelegt sind, siehe zu letzterem nur die Datenschutz-Richtlinien 95/46/EG und 2002/58/EG. Dass hier Kerngewährleistungen des Unionsrechts berührt sind ergibt sich bereits aus folgender Testfrage: Würde man einen Beitrittskandidaten in die EU aufnehmen, der einen solchen Datenstaubsauger wie die GCHQ betreibt? Die Antwort ist ziemlich klar: Nein. Die Mitgliedschaft in der EU setzt das Einhalten bestimmter Grundrechtsschutz- und Rechtsstaatsstandards voraus (Kopenhagener Kriterien).

Für die bereits beigetretenen Staaten, die aktuellen 28 Mitgliedstaaten, darunter Großbritannien, kann man das Einhalten der Rechtsstaats- und Grundrechtsstandards des Art. 2 EUV mit einem Verfahren nach Art. 7 EUV erzwingen. Das ist das größte rechtliche Kaliber, die Folgen reichen bis zum Entzug von Stimmrechten. Der Mechanismus hat sich aber bisher als wenig effektiv erwiesen, vielleicht weil die erforderlichen Quoren doch zu hoch sind und sicherlich der politische Wille für den Einsatz des Instruments bisher gefehlt hat, der Fall Ungarn zeigt dies ganz deutlich.

Wendet man sich konkreten Datenschutzgewährleistungen zu, wie sie in Art. 8 GRCh, 16 AEUV sowie im Sekundärrecht niedergelegt sind, dann stößt man durchgehend auf das Problem, dass all diese Gewährleistungen nicht ohne weiteres die Mitgliedstaaten binden. Die Probleme beginnen mit der Bereichsausnahme der Datenschutz-Richtlinie. Wörtlich heißt es in Art. 3 Abs. 2 Datenschutz-Richtlinie 95/46/EG zum Anwendungsbereich (Hervorhebung hinzugefügt):

> *Diese Richtlinie findet keine Anwendung auf die Verarbeitung personenbezogener Daten,– die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und* ***auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt)*** *und die Tätigkeiten des Staates im strafrechtlichen Bereich;– (…)*

Siehe auch den Erwägungsgrund 43 zur Richtlinie:

> *„Die Mitgliedstaaten können Beschränkungen des Auskunfts- und Informationsrechts sowie bestimmter Pflichten des für die Verarbeitung Verantwortlichen vorsehen, soweit dies beispiels-*

> *weise für die **Sicherheit des Staates**, die Landesverteidigung, die **öffentliche Sicherheit**, für **zwingende wirtschaftliche oder finanzielle Interessen eines Mitgliedstaats** oder der Union oder für die Ermittlung und Verfolgung von Straftaten oder von Verstößen gegen Standesregeln bei reglementierten Berufen erforderlich ist. Als Ausnahmen und Beschränkungen sind Kontroll-, Überwachungs- und Ordnungsfunktionen zu nennen, die in den drei letztgenannten Bereichen in bezug auf öffentliche Sicherheit, wirtschaftliches oder finanzielles Interesse und Strafverfolgung erforderlich sind. Die Erwähnung der Aufgaben in diesen drei Bereichen läßt die Zulässigkeit von Ausnahmen und Einschränkungen aus Gründen der Sicherheit des Staates und der Landesverteidigung unberührt.*

Und schließlich Art. 13 Abs. 1 der Richtlinie zu Ausnahmen und Einschränkungen (Hervorhebungen hinzugefügt):

> *Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Pflichten und Rechte gemäß Artikel 6 Absatz 1, Artikel 10, Artikel 11 Absatz 1, Artikel 12 und Artikel 21 beschränken, sofern eine solche Beschränkung notwendig ist füra) die **Sicherheit des Staates**;b) die Landesverteidigung;c) die **öffentliche Sicherheit**;d) die **Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten** oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen;e) ein **wichtiges wirtschaftliches oder finanzielles Interesse eines Mitgliedstaats** oder der Europäischen Union einschließlich Währungs-, Haushalts- und Steuerangelegenheiten;f) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben c), d) und e) genannten Zwecke verbunden sind;g) den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen.*

In der englischen Sprachfassung der Richtlinie sind die einschlägigen Stichworte: „public security“, „State security“, „defence“ , „important economic or financial interests“, „economic well-being of the State“. Die Rechtsgrundlagen für die elektronischen Abhörprogramme in Großbritannien enthalten genau die gleichen Stichworte. In Art. 8 (4) und (5) i.V.m. Art. 5 (3) RIPA (Regulation of Investigatory Powers Act) von 2000: „interests of national security“, „purpose of preventing or detecting serious crime“, „purpose of safeguarding the **economic well-being** of the United Kingdom“, (…)

Es scheint also, dass man mit dem Sekundärrecht nicht weiter kommt. Wie sieht es mit dem Primärrecht, dem Vertragsrecht aus?

In Betracht kommen die primärrechtlichen Garantien zum Datenschutz in der Grundrechte-Charta und Art. 16 AEUV, daneben das Grundrecht auf effektiven Grundrechtsschutz (Art. 47 GRCh, dazu jüngst EuGH in der Rs. C-300/11, ZZ, vom 4. Juni 2013).

Diese Garantien können gegenüber Mitgliedstaaten indessen nur dann geltend gemacht werden, wenn der Anwendungsbereich des Unionsrechts eröffnet ist. Dies gilt auch für den etwas ferner liegenden Art. 18 AEUV, der von einer NGO Privacy International in einer Klage in Großbritannien vorgebracht wird.

Selbst wenn es gelingt, den Anwendungsbereich des Unionsrechts zu begründen, so begegnet man wiederum dem rechtlichen Einwand, die Programme dienten der nationalen Sicherheit. Dazu führt nämlich Art. 4 Abs. 2 EUV Folgendes aus (Hervorhebung hinzugefügt):

> *Die Union achtet die Gleichheit der Mitgliedstaaten vor den Verträgen und ihre jeweilige nationale Identität […]. Sie achtet die grundlegenden Funktionen des Staates, insbesondere die Wahrung der territorialen Unversehrtheit, die Aufrechterhaltung der öffentlichen Ordnung und den Schutz der nationalen Sicherheit. **Insbesondere die nationale Sicherheit fällt weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten.***

Auf Ebene des Primärrechts, also auf der gleichen Rangstufe wie Art. 16 AEUV oder die Charta, wird nationale Sicherheit damit schlicht aus dem Europarecht herausgenommen.

Damit ergibt sich als Zwischenbefund , dass das Europarecht nicht weiter zu helfen scheint. Das Euro-

parecht kommt offenbar schlicht nicht an die hier in Rede stehenden Vorgänge heran.

Kann das schon alles sein?

Nein. Schon mit Blick darauf, dass man kaum gegenüber den USA strikte Beachtung von Datenschutzstandards einfordern kann und gleichzeitig einen Mitgliedstaat unbehelligt lässt, muss das britische Handeln auf den Prüfstand des Unionsrechts.

Letztlich ist die europarechtliche Frage, die sich hier stellt, auch nicht schwer zu identifizieren. Es geht um eine Abwägung. Auf der einen Seite stehen die Gewährleistungen des Europarechts, seien es die grundrechtlichen Gehalte zum Datenschutz und der Privatsphäre oder die grundfreiheitlichen Gewährleistungen von Warenverkehrsfreiheit oder Dienstleistungsfreiheit. Auf der anderen Seite stehen mitgliedstaatliche Belange, die als Bereichsausnahme oder Rechtfertigungselemente daherkommen und sich auf nationale Sicherheit oder – allgemeiner – öffentliche Sicherheit berufen.

Am Beispiel der Auslegung der Bereichsausnahme in Art. 3 Abs. 2 der Datenschutz-Richtlinie lässt sich illustrieren, worum es geht. Nach Art. 3 Abs. 2 bezieht sich die Richtlinie „auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich; […]“.

Gestattet dies wirklich eine anlasslose flächendeckende Datenerhebung? Zu bedenken ist dabei Folgendes: Die Richtlinie stammt aus dem Jahre 1995, also aus einer Zeit, in der schon technisch eine derartig flächendeckende Datenerhebung, wie sie jetzt in Rede steht, nicht in Sicht war. Zudem sind Ausnahmen von den Gewährleistungen des Unionsrechts grundsätzlich eng auszulegen. Deswegen wird man wohl doch einen konkreten Anlass, vielleicht sogar einen konkreten Angriff verlangen müssen, um die Ausnahme als gegeben ansehen zu können. Die Ausnahme kann in dieser Logik eigentlich auch nur Behörden der nationalen Sicherheit zugute kommen. Sie kann demnach also keine Anwendung finden, wenn private Telekommunikations-Unternehmen für den Staat aktiv werden. Art. 3 Abs. 2 ist danach kein Freibrief für anlasslose flächendeckende Datenerhebung. Und auch Art. 4 Abs. 2 EUV wird in diesem Sinne eng auszulegen sein und im Ergebnis eine anlasslose flächendeckende Datenerhebung durch einen Mitgliedstaat nicht ermöglichen können.

Der EuGH wird letztlich die Institution sein, die letztverbindlich über die Reichweite und Auslegung der Ausnahmen von den Gewährleistungen des Unionsrechts im vorliegenden Kontext befindet. Der EuGH lässt sich vom Argument der nationalen Sicherheit nur mäßig beeindrucken und überprüft entsprechende Argumente. Es genügt also nicht, als Mitgliedstaat schlicht in allgemeiner Form und unüberprüfbar auf angebliche Belange der nationalen Sicherheit zu verweisen, siehe dazu etwa EuGH in der Rs. C-300/11, ZZ, vom 4. Juni 2013, Rn. 38:

> *„Außerdem ist es zwar Sache der Mitgliedstaaten, die geeigneten Maßnahmen zur Gewährleistung ihrer inneren und äußeren Sicherheit zu ergreifen, doch kann der Umstand, dass eine Entscheidung die Sicherheit des Staates betrifft, für sich allein genommen nicht zur Unanwendbarkeit des Rechts der Union führen.“*

Es kommt letztlich auf eine Güterabwägung im Rahmen einer Verhältnismäßigkeitsprüfung an. Es werden demnach die Argumente der nationalen Sicherheit oder öffentlichen Sicherheit durch den EuGH allesamt unter dem Aspekt der Verhältnismäßigkeit und des Übermaßverbotes überprüft.

Wenn die Bereichsausnahmen des Europarechts aber nicht greifen, weil die britischen Maßnahmen zu breit, unbestimmt und ungezielt sind, dann kommen sämtliche Gewährleistungen des Sekundärrechts und des Primärrechts in den Blick.

Zu nennen sind dabei auch die Grundfreiheiten des Binnenmarktes, konkret die Warenverkehrs- oder die Dienstleistungsfreiheit. Die Grundfreiheiten im EU-Binnenmarkt handeln zwar im Kern von einer Marktzugangslogik. Und alleine das Absaugen von Daten hindert nicht die grenzüberschreitende Dienstleistung, die über das Internet abgewickelt wird, oder den Internetversandhandel. Diese ökonomischen Akti-

vitäten, so lässt sich argumentieren, bleiben weiterhin möglich. Allerdings enthält das Unionsrecht mit einem Beschränkungsverbot eine Gewährleistungsdimension, die schon seit längerem vom Marktzugangsparadigma abgekoppelt ist. In Betracht kommen hier wahrscheinlich am ehesten konkrete Fälle aus dem Bereich des Internetversandhandels und der Internetdienstleistungen.

Auch die Unionsbürgerschaft ist immer mehr vom Marktzugangsparadigma abgekoppelt. Aber dies wird man vorliegend nicht sinnvoll einsetzen können, es sei denn, man wollte die Datenschutzfrage im Kernbereich der Unionsbürgerschaft verorten.

Wenn das Argument nationale Sicherheit/öffentliche Sicherheit geklärt ist, dann werden vor allem die materiellen Gewährleistungen des europäischen Datenschutzrechts namentlich in der Grundrechte-Charta eine Rolle spielen können. Zwar bestehen jenseits des Argumentes von der Sperrwirkung der nationalen oder öffentlichen Sicherheit noch immer zwei Anfragen zur Anwendbarkeit der Charta, diese sind indessen wie folgt im Sinne des Grundrechtsschutzes der Unionsbürger zu beantworten.

Erstens: Das britische sogenannte Opt-out aus der Charta spielt vorliegend keine Rolle, das ergibt sich schon aus dem Wortlaut des einschlägigen Protokolls zum Vertrag von Lissabon, weil es genau besehen gar kein Opt-out gibt. Zweitens: Bei der Frage der Bindung der Mitgliedstaaten an die EU-Grundrechte – diese gelten vorrangig für die Unionsorgane – versperrt Art. 51 GRCh die Bindung eines Mitgliedstaats an die europäischen Grundrechte nicht, dies bestätigt die EuGH-Entscheidung in der Rs. Åkerberg Fransson, die im Sinne eines möglichst umfassenden Grundrechtsschutzes für die Unionsbürger eine restriktive Auslegung von Art. 51 GRCh und ein weites Verständnis von „Anwendungsbereich des Unionsrechts“ verfolgt. Es ist bedauerlich, dass der Erste Senat des BVerfG ausgerechnet in seiner Entscheidung zur Antiterrordatei vom April 2013, also in einem Kontext, der auch zur Rechtfertigung der NSA- und GCHQ-Maßnahmen vorgebracht wird, die Anwendbarkeit der Charta verneint und übrigens auch gleich ungefragt und nur begrenzt zuständig (wenn entscheidungserheblich muss eine solche Frage dem EuGH vorgelegt werden) die Bereichsausnahme des Art. 3 Datenschutz-Richtlinie (dazu bereits oben) interpretiert. Diese Argumentation wird sicherlich von den GCHQ-Juristen dankbar aufgenommen werden. Und dem BVerfG möchte man im vorliegenden Kontext die Einsicht wünschen, dass die aktuellsten und größten Bedrohungen für individuelle und kollektive Selbstbestimmung in Deutschland – was man als Kern der Souveränitätsargumente ernst nehmen kann – nicht vom EuGH oder der EZB ausgehen.

Die Frage, ob anlassloses flächendeckendes Ausspähen von Daten von Unionsbürgern im „Anwendungsbereich des Unionsrechts“ liegt oder nicht wird sich bei der geplanten EU-Datenschutzgrundverordnung ebenfalls stellen, weil dies das Kriterium für die Anwendbarkeit der Verordnung sein wird (Art. 2).

Die prozessualen Perspektiven zur Klärung dieser Fragen sind ein Vertragsverletzungsverfahren gegen Großbritannien vor dem EuGH, sowie vielleicht auch eine Vorlage an den EuGH aus einem Mitgliedstaat. Es gibt Hinweise, dass man in der Europäischen Kommission ein Vertragsverletzungsverfahren in Erwägung zieht. Wie auch im NSA-Kontext stellt sich aber die Frage, ob von einer am Ende ihres Mandats befindlichen Kommission mit einem Kommissions-Präsidenten, der die Vorstellung einer weiteren Amtszeit noch nicht aufgegeben hat, ein derartiger Schritt gegen einen großen Mitgliedstaat wirklich zu erwarten ist.

Von den Mitgliedstaaten wird man in Sachen Vertragsverletzungsverfahren aus verschiedenen Gründen wenig erwarten können. Die Bundesrepublik hat aus integrationspolitischen Gründen noch nie ein Vertragsverletzungsverfahren gegen einen anderen Mitgliedstaat eingeleitet, daher wird dies auch im Hinblick auf Großbritannien jedenfalls nicht freiwillig passieren.

Es ist aber nicht nur die traditionelle Linie, gegen andere Mitgliedstaaten nicht den EuGH anzurufen, die eine Zurückhaltung der Bundesregierung im Vorgehen gegen Großbritannien erklären würde. Hier kommt abschließend ein Aspekt in den Blick, der in der deutschen Diskussion vielfach ausgeblendet wird. Gerade aus anderen Mitgliedstaaten wird die Rolle des BND in

der NSA-GCHQ-Angelegenheit durchaus kritisch gesehen. Die Nähe der USA bei der Gründung des BND wird dabei in Erinnerung gerufen. Daneben muss gefragt werden, ob die Geheimdienste womöglich einen munteren Informationsringtausch betreiben, bei dem jeweils das, was man zu Hause aus rechtlichen Gründen bei den eigenen Bürgern nicht ausforschen darf, dann eben auf der Grundlage mehr oder weniger ebenbürtiger Gegenseitigkeit von einem anderen Geheimdienst zur Verfügung gestellt wird.

Auch an dieser Stelle sind wahrscheinlich auf nationaler Ebene, auch und gerade in Deutschland, rechtliche Klarstellungen erforderlich. Insbesondere die „strategische Fernmeldeüberwachung", ein Relikt aus dem Kalten Krieg auf Grundlage der §§ 5 und 8 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G 10), gehört eineinhalb Jahrzehnte nach der letzten Äußerung des BVerfG dazu auf den verfassungsrechtlichen Prüfstand. Auch die Zivilgesellschaft kann die Dinge hier in Bewegung bringen, wie das Beispiel Polen zeigt.

Zugleich wird man auch sehen müssen, dass andere Mitgliedstaaten, namentlich diejenigen, die unmittelbarer als Deutschland in ihrer jüngeren Vergangenheit Terroranschlägen ausgesetzt waren, die verfassungsrechtliche Abwägung zwischen Sicherheit und Grundrechten anders treffen als Deutschland mit einer seit 1949 gewachsenen und im wesentlichen nicht unter Druck geratenen Grundrechtskultur. Mit dem Hinweis auf kulturelle Unterschiede, sozusagen Verfassungsfolklore, kann es aber nicht sein Bewenden haben, wenn bei Grundrechtsbeeinträchtigungen Ländergrenzen keine Rolle mehr spielen. Wenn es Deutschland als größtem und einflussreichsten Mitgliedstaat der EU gelungen ist, den meisten anderen Mitgliedstaaten die deutsche Schuldenbremse als deutsche verfassungsrechtliche Errungenschaft vorzugeben, dann sollte dies doch erst recht möglich sein für einen grundrechtlich konzipierten hohen Datenschutzstandard und ein entsprechendes Übermaßverbot, was staatliche Eingriffe eingeht. Natürlich kann es nicht darum gehen, sicherheits- und nachrichtendienstliche Tätigkeiten zu verbieten oder unmöglich zu machen, sondern darum, ihre Tätigkeit rechtlich, vor allem grundrechtlich, einzuhegen. Und damit hat Deutschland, ohne dass fortbestehende Defizite hier übersehen werden dürfen, aus den bekannten traurigen historischen Gründen einen großen Bestand an weitergebenswerter Erfahrung.

Zusammenfassend ist festzuhalten, dass es unabhängig von der rechtlichen Verortung im Europarecht im einzelnen, auch unabhängig von europarechtsdogmatischen Einordnungen als Bereichsausnahmen, Rechtfertigungen, zwingende Erfordernisse usf., um eine grundsätzliche Abwägung zwischen dem Argument der nationalen und der inneren Sicherheit einerseits und den Freiheitsgewährleistungen des Unionsrechts andererseits geht. Diese Frage wird man klären müssen.

AUTOR*IN

Franz C. Mayer

Prof. Dr. Franz C. Mayer ist Professor für Öffentliches Recht, Europa- und Völkerrecht an der Universität Bielefeld.

EMPFOHLENE ZITATION

Mayer, Franz C.: Mit Europarecht gegen die amerikanischen und britischen Abhöraktionen? Teil 2: GCHQ, Verfassungsblog, 18.11.2013, doi: 10.17176/20171006-143709.

Lizensiert unter CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20171006-143709.