ARTIKEL-29-DATENSCHUTZGRUPPE

14/DE
WP 228

Arbeitsdokument „Überwachung der elektronischen Kommunikation zu nachrichtendienstlichen und nationalen Sicherheitszwecken“

Angenommen am 5. Dezember 2014

Zusammenfassung

Das vorliegende Arbeitsdokument enthält die rechtliche Analyse, die der am 10. April 2014 von der Artikel-29-Datenschutzgruppe verabschiedeten *Stellungnahme 04/2014 zur Überwachung der elektronischen Kommunikation zu nachrichtendienstlichen und nationalen Sicherheitszwecken* zugrunde liegt. Die Stellungnahme betrifft vorrangig die angesichts der Enthüllungen von Edward Snowden für erforderlich erachteten Schritte. In diesem Sinne werden in der Stellungnahme eine Reihe von Empfehlungen dargelegt, wie die Achtung des Grundrechts auf Schutz der Privatsphäre und Datenschutz seitens der Nachrichten- und Geheimdienste erneut gewährleistet und die Überwachung der Aktivitäten dieser Behörden verbessert werden kann, ohne die nationale Sicherheit zu beeinträchtigten. Das vorliegende Arbeitsdokument enthält die Ergebnisse der Erörterungen und der rechtlichen Analysen, auf denen die Empfehlungen der Datenschutzgruppe beruhen.

Zuerst ist zu betonen, dass bei der Erörterung von Fragen der nationalen Sicherheit und der Überwachung unter dem Gesichtspunkt des Datenschutzes nicht nur das Unionsrecht zu berücksichtigen ist. Ebenso wichtig sind die Grundsätze, die in der Allgemeinen Erklärung der Menschenrechte und im Internationalen Pakt über bürgerliche und politische Rechte sowie in der Europäischen Menschenrechtskonvention und im Übereinkommen des Europarates über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten niedergelegt sind[1]. Ein Eingriff in diese Rechte kommt nur dann in Betracht, wenn eine derartige Maßnahme gemäß gesetzlich vorgesehen, notwendig und verhältnismäßig ist und einem zwingenden gesellschaftlichen Erfordernis entspricht. Das bedeutet zugleich, dass eine derartige Maßnahme nur unter der Voraussetzung erfolgen darf, dass keine anderen Optionen verfügbar sind, die weniger in die genannten Grundrechte eingreifen.

In Ermangelung einer klaren Definition des Begriffs „nationale Sicherheit“ hat die Datenschutzgruppe erörtert, wie dieser Begriff ausgelegt werden sollte, zumal die dünne Trennlinie zwischen Strafverfolgung und nationaler Sicherheit offenbar zuweilen verwischt. Auf jeden Fall ist die nationale Sicherheit abzugrenzen von der Sicherheit der Europäischen Union, aber auch von der staatlichen Sicherheit, von der öffentlichen Sicherheit und von der Verteidigung. Auf all diese Begriffe nehmen die EU-Verträge und die entsprechenden Rechtsvorschriften jeweils gesondert Bezug, wenngleich sie untrennbar miteinander verbunden sind. Die Definition der Umstände, die eine Ausnahme für den Bereich der nationalen Sicherheit begründen, kann daher nicht ausschließlich mit rechtlichen Argumenten erfolgen. Fest steht, dass bei Aktivitäten von Nachrichten- und Geheimdiensten in der Regel akzeptiert wird, dass sie als Ausnahme für den Bereich der nationalen Sicherheit zu

[1] Die Achtung dieser Grundrechte ist für sämtliche Vertragsstaaten – einschließlich der EU-Mitgliedstaaten – verbindlich.

betrachten sind, wohingegen eine solche Akzeptanz nicht immer gegeben ist, wenn allgemeine Strafverfolgungsbehörden vergleichbare Aufgaben erfüllen.

Im vorliegenden Arbeitsdokument wird ferner erörtert, ob eine Berufung auf nationale Sicherheitsinteressen eines Drittlands statthaft ist. Die Datenschutzgruppe betont, dass es gemäß der in den Verträgen vorgesehenen Ausnahme nicht möglich ist, sich lediglich auf nationale Sicherheitsinteressen eines Drittlands zu berufen, um die Anwendbarkeit des Unionsrechts zu umgehen. Sie räumt jedoch ein, dass es möglicherweise Bereiche gibt, in denen nationale Sicherheitsinteressen eines EU-Mitgliedstaats und eines Drittlands gleichgerichtet sind. Dies muss jedoch durch den betreffenden EU-Mitgliedstaat gegenüber den zuständigen Behörden von Fall zu Fall begründet werden.

Ein wesentlicher Teil des Arbeitsdokuments befasst sich mit der Anwendbarkeit der in der Richtlinie 95/46/EG niedergelegten Regelungen zur Datenübermittlung in Drittländer. Auch wenn viele Einzelheiten der Überwachungsprogramme noch immer unklar sind, ist davon auszugehen, dass die Überwachungsbehörden von Drittländern Zugang zu Daten erhalten, nachdem diese Daten durch einen für die Verarbeitung Verantwortlichen, welcher der Hoheitsgewalt der EU untersteht, an einen Ort außerhalb des EU-Hoheitsgebiets übermittelt worden sind. Derartige Datenübermittlungen in Drittländer erfolgen vermutlich grundsätzlich gemäß den Verfahren, die in der Richtlinie und den Rechtsvorschriften zu ihrer Umsetzung in mitgliedstaatliches Recht niedergelegt sind, wobei möglicherweise Standardvertragsklauseln, verbindliche unternehmensinterne Vorschriften oder das Safe-Harbor-Abkommen angewandt werden. Keines dieser Rechtsinstrumente enthält jedoch eine Bestimmung, die eine massenhafte, routinemäßige oder unbegrenzte Datenübermittlung in Drittländer erlauben würde. Sofern Behörden eines Drittlandes direkten Zugang zu personenbezogene Daten wünschen, die der Hoheitsgewalt der EU unterliegen, sollten sie die förmlichen Wege der Zusammenarbeit beschreiten, da im Unionsrecht keine ausdrücklichen Möglichkeiten vorgesehen sind, um personenbezogene Daten, die sich in der Obhut von privatwirtschaftlichen für die Verarbeitung Verantwortlichen in der Privatwirtschaft befinden, an Strafverfolgungsbehörden oder Geheimdienste eines Drittlandes zu übermitteln. Das vorliegende Arbeitsdokument enthält Beispielszenarien zur Veranschaulichung der dargelegten Analysen. Abschließend werden im vorliegenden Arbeitsdokument mögliche Optionen für die Zukunft erörtert.

Inhaltsverzeichnis

1. Einleitung

Am 10. April 2014 verabschiedete die Artikel-29-Datenschutzgruppe (im Folgenden „Datenschutzgruppe“) ihre Stellungnahme 04/2014 zur Überwachung der elektronischen Kommunikation zu nachrichtendienstlichen und nationalen Sicherheitszwecken[2]. Es handelte sich bei dieser Stellungnahme um eine erste Antwort auf die Enthüllungen über die Massenüberwachung durch Geheimdienste aus aller Welt, wie insbesondere durch die von Edward Snowden vorgelegten Dokumente belegt. In dieser Stellungnahme sind auch eine Reihe von Empfehlungen an die internationale Gemeinschaft sowie an die Gesetzgeber in der Europäischen Union und ihren Mitgliedstaaten enthalten, wie angesichts einer solchen Überwachungspraxis der Schutz personenbezogener Daten für die einzelnen Bürger verbessert werden kann.

Während der Schwerpunkt der Stellungnahme auf den angesichts der Enthüllungen von Edward Snowden dringend gebotenen Schritte für den Datenschutz liegt, haben die Mitglieder der Datenschutzgruppe auch umfangreiche Erörterungen zum rechtlichen Rahmen der Massenüberwachung durchgeführt, insbesondere hinsichtlich der Anwendbarkeit von Unionsrecht im Zusammenhang mit den aufgedeckten Überwachungsaktivitäten. Das vorliegende Arbeitsdokument enthält die Ergebnisse dieser Erörterungen. Zugleich ist die Datenschutzgruppe überzeugt, dass eine breitere Diskussion unter Einbeziehung verschiedener Interessenträger stattfinden sollte. Das vorliegende Arbeitsdokument ist daher vor allem als Beitrag zu einer solchen Diskussion gedacht. Zudem enthält es eine Reihe von Szenarien zur Datenübermittlung im Hinblick auf die Nachrichten- und Geheimdienste von Drittländern. Die Datenschutzgruppe betont, dass die Analyse im vorliegenden Arbeitsdokument keine zufriedenstellende Lösung für sämtliche denkbaren grenzüberschreitenden Datenverarbeitungsaktivitäten liefern kann, denn die endgültige rechtliche Analyse der Rechtmäßigkeit einer Datenverarbeitung hängt stets von den spezifischen Umständen des jeweiligen Falls ab.

[2] WP 215 – http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_de.pdf.

2. Überwachungsprogramme

Seit Mitte 2013 haben die Medien – vorrangig die britische Tageszeitung The Guardian[3] sowie die US-amerikanische Tageszeitung The Washington Post[4] – zahlreiche zuvor geheime Überwachungsprogramme aufgedeckt. Viele dieser Programme zielen offenbar auf das massenweise Abgreifen von personenbezogenen Daten aus verschiedenen Online-Quellen ab, wobei sowohl Inhalts- als auch Verkehrsdaten betroffen sind. Den Berichten zufolge wird bei den meisten Programmen nicht zwischen verdächtigen und nicht verdächtigen Personen unterschieden. Außerdem wurde aufgedeckt, dass die Nachrichtendienste, die Überwachungsprogramme in anderen Ländern durchführen, offenbar eng zusammenarbeiten.

Die elektronische Überwachung mittels Signals-Intelligence (Fernmeldeaufklärung und elektronische Aufklärung)[5] hat sich über die letzten Jahrzehnte zu einer üblichen Methode der Nachrichtendienste entwickelt, wobei eine rechtmäßige Verwendung nur gegeben ist, wenn die gesetzlich niedergelegten Verfahren zum rechtmäßigen Abfangen von Nachrichten eingehalten werden. Mit den Enthüllungen von Edward Snowden ist klar geworden, dass die Grenzen der Rechtmäßigkeit erreicht und zuweilen überschritten worden sind.[6] Wahrscheinlich gibt es überall auf der Welt Überwachungsprogramme.

In den nachfolgenden Abschnitten 2.1 und 2.2 findet sich ein Überblick, der als Sachinformation gedacht ist und vorrangig auf Medienberichten, auf dem

---

[3] http://www.theguardian.com/world/the-nsa-files.

[4] http://www.washingtonpost.com/nsa-secrets/.

[5] Signals-Intelligence (SIGINT – Fernmeldeaufklärung und elektronische Aufklärung) bezieht sich auf die Erfassung von Informationen über die Kommunikation zwischen Menschen sowie auf die Erfassung von elektronischen Signalen, beispielsweise von Radaranlagen und Waffensystemen. Die Informationen über Kommunikation können sowohl Inhaltsdaten als auch Daten zum „Betreff" umfassen, was in den Vereinigten Staaten als Metadaten bezeichnet wird.

[6] Vgl. insbesondere die in den Berichten der US-Agentur für den Schutz der Privatsphäre und der bürgerlichen Freiheiten (PCLOB – Privacy and Civil Liberties Oversight Board) dargelegten Entwicklungen. Verfügbar unter http://www.pclob.gov/

Bericht der EU/US-Sachverständigen-Arbeitsgruppe[7] sowie auf Informationen beruht, die von den US-Behörden nach der Aufdeckung mehrerer Überwachungsprogramme freigegeben worden sind. Bei diesem kurzen Überblick handelt es sich nicht um eine Stellungnahme der Datenschutzgruppe, wohingegen in späteren Abschnitten Einschätzungen der Datenschutzgruppe niedergelegt sind. Bis heute haben die europäischen Regierungen der Öffentlichkeit kaum Informationen über die Existenz und die Funktionsweise der mutmaßlichen Überwachungsprogramme geliefert, insbesondere hinsichtlich der Zusammenarbeit zwischen ihren jeweiligen Nachrichtendiensten und den Behörden, die für diese Programme zuständig sind. Es ist jedoch deutlich geworden, dass die massenhafte elektronische Überwachung keine rein US-amerikanische Angelegenheit ist, sondern eine Praxis, die in vielen Ländern weltweit stattfindet. Nachfolgend sollen am Beispiel der USA einige Problemkreise veranschaulicht werden, die sich ergeben haben, da die USA das Drittland sind, über dessen Praxis wohl am umfangreichsten diskutiert worden ist. Es gibt jedoch auch Fälle in anderen Ländern, wie in Abschnitt 2.2 dargelegt.

2.1 Überwachung seitens der USA

In den USA ist für die meisten Überwachungsprogramme die NSA zuständig. Die erzeugten Datenbanken sind je nach Programm für Suchabfragen seitens der NSA, der CIA und/oder des FBI zugänglich. Die meisten Überwachungsprogramme werden auf der Grundlage des USA PATRIOT Act und des Foreign Intelligence Surveillance Act (FISA) durchgeführt, aber auch

[7] „Report on the Findings by the EU Co-chairs of the Ad Hoc EU-US Working Group on Data Protection“, Begleitdokument zur Mitteilung der Kommission an das Europäische Parlament und an den Rat „Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA“ (COM(2013) 846 final) – http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf – *Diese EU/US-Arbeitsgruppe befasst sich mit den verschiedenen Aspekten der EU/US-Beziehungen im Hinblick auf Überwachung, einschließlich des Patriot Act, der Executive Order 12333 sowie der Kontrollfunktionen der Exekutive, der Legislative und der Judikative der USA. In der Mitteilung der Kommission liegt der Schwerpunkt mehr auf den möglichen und erforderlichen Änderungen an den Datenübermittlungsvereinbarungen zwischen EU und USA, etwa am Abkommen über Fluggastdatensätze („PNR-Abkommen“), am TFTP-Abkommen (Terrorist Finance Tracking Program – Programm zum Aufspüren von Finanzierungen des Terrorismus), am Rahmenabkommen zu Strafverfolgungsangelegenheiten sowie am Safe-Harbour-Abkommen.*

auf der Grundlage des Executive Order 12333 (eines Präsidialerlasses von 1981).

Als Reaktion auf die öffentliche Diskussion nach den Enthüllungen von Edward Snowden hat der US-Präsident die „Review Group on Intelligence and Communications Technologies" eingerichtet. Diese Gruppe hat am 12. Dezember 2013 ihren Bericht vorgelegt, einschließlich Empfehlungen zu möglichen Änderungen an der nationalen Sicherheitspolitik der USA.[8] Der Präsident hat diese Empfehlungen bei der Ausarbeitung eines neuen Erlasses mit Richtlinien für Signals-Intelligence-Aktivitäten (Fernmeldeaufklärung und elektronische Aufklärung) berücksichtigt, der bei einer Pressekonferenz am 17. Januar 2014 vorgestellt wurde.

Die wichtigsten bekanntgegebenen Änderungen beziehen sich auf die Überwachungsprogramme gemäß Abschnitt 215 des USA PATRIOT Act, insbesondere auf das so genannte Geschäftsunterlagenprogramm (Business Records Programme), das die Erfassung von Verkehrsdaten (Telefon-Metadaten) seitens der Telekommunikationsanbieter erlaubt. Ungeachtet der Schlussfolgerung des Privacy and Civil Liberties Oversight Board (PCLOB) zu Programmen gemäß Abschnitt 215 des USA PATRIOT Act, insbesondere zum so genannten Geschäftsunterlagenprogramm (Business Records Programme) zur Erfassung von Telefon-Metadaten, nämlich dass für die Erfassung von Metadaten eine tragfähige Rechtsgrundlage fehle („lacks a viable legal foundation"[9]), werden die Programme zur Massenüberwachung nicht beendet. Der US-Präsident kündigte jedoch eine strengere Kontrolle über die Aktivitäten der US-Geheimdienste an, einschließlich einer Änderung bei den Verfahren vor dem FISA-Gericht, um ein Gremium von Anwälten von außerhalb der Regierung einzuführen, als unabhängige Stimme in wichtigen Fällen („the introduction of a panel of advocates from outside government to

[8] Liberty and Security in a Changing World – Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, S. 11, http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (zuletzt aufgerufen am 20. November 2014).

[9] Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court, S. 1616, http://www.pclob.gov/All%20Documents/Report%20on%20the%20Telephone%20Records%20Program/PCLOB-Report-on-the-Telephone-Records-Program.pdf (zuletzt aufgerufen am 20. November 2014).

provide an independent voice in significant cases“).[10] Im Übrigen hat der US-Präsident zwar betont, dass es wichtig sei, bei den ausländischen Partnern wieder Vertrauen aufzubauen, aber die hinsichtlich der geheimdienstlichen Erfassung von Informationen im Ausland vorgeschlagenen Änderungen sind eher begrenzter Natur. Die genannten massenhaften Signals-Intelligence-Aktivitäten werden fortgesetzt, lediglich mit dem Unterschied, dass die Speicherung der erfassten Daten nicht mehr bei der Regierung erfolgt, sondern bei den Telekommunikationsanbietern. Ergänzend merkte der US-Präsident allerdings an, dass diese Datenerfassung und -speicherung gemäß den Zwecken der nationalen Sicherheit erfolgen müsse.

Die US-Datenschutzagentur PCLOB veröffentlichte im Juli 2014 einen zusätzlichen Bericht zu Programmen gemäß Abschnitt 702 des USA PATRIOT Act. Die in diesem Bericht enthaltene Kritik an der bestehenden Praxis geht nicht so weit wie im vorhergehenden Bericht zu Programmen gemäß Abschnitt 215 (der im Januar 2014 veröffentlicht wurde). Es wird anerkannt, dass bestimmte Aspekte des gemäß Abschnitt 702 durchgeführten Programms an der Grenze der verfassungsmäßigen Angemessenheit liegen würden (*„certain aspects of the Section 702 program push the program close to the line of constitutional reasonableness“*). Genannt werden dabei insbesondere der unbekannte und potenziell große Umfang der unbeabsichtigten Erfassung der Kommunikation von US-Personen, die Verwendung von Daten zum Betreff, um per Internet übermittelte Nachrichten zu erfassen, die weder von der Zielperson der Überwachung stammen noch an diese Zielperson gerichtet sind, sowie die Verwendung von Suchabfragen, um innerhalb der erfassten Daten nach Nachrichten spezifischer US-Personen zu suchen. In dem Bericht sind Empfehlungen niedergelegt, um das PRISM-Programm und das Upstream-Programm (die beide gemäß Abschnitt 702 des Patriot Act durchgeführt werden) hinsichtlich der durch die US-Verfassung gezogenen Grenzen „angemessener“ zu gestalten.

[10] Rede des Präsidenten der Vereinigte Staaten, verfügbar unter http://www.whitehouse.gov/blog/2014/01/17/president-obama-discusses-us-intelligence-programs-department-justice (zuletzt aufgerufen am 20. November 2014).

2.2. Überwachung seitens EU-Mitgliedstaaten und seitens Drittländern

Die Enthüllungen von Edward Snowden und die parallel dazu aufgedeckten Praktiken sind nicht auf US-amerikanische Überwachungsaktivitäten begrenzt, sondern betreffen auch Überwachung seitens der Nachrichtendienste von EU-Mitgliedstaaten, sowohl innerhalb als auch außerhalb des Gebiets der Europäischen Union. Dies ist von besonderer Relevanz, weil sich mittlerweile bestätigt hat, dass mehrere europäische Nachrichtendienste eine enge Zusammenarbeit mit den entsprechenden US-Nachrichtendiensten pflegen[11]. Je enger diese Zusammenarbeit mit den Vereinigten Staaten, desto umfangreicher der wechselseitige Datenaustausch. Das bedeutet, dass die nationale Sicherheit längst nicht so „national" ist, wie der Begriff vermuten lässt. Vielmehr erfolgt eine umfangreiche Weitergabe und ein umfangreicher Austausch von Daten – einschließlich personenbezogener Daten – zwischen den Geheimdiensten.

Die seitens europäischer Nachrichtendienste durchgeführten Überwachungsprogramme reichen mutmaßlich von der Erfassung von Metadaten der Kommunikation aus verschiedenen Quellen über die Überwachung von Internetforen bis hin zum Anzapfen von kabelgestützter Kommunikation. Bis heute ist kaum eines dieser Programme seitens der betreffenden Regierungen bestätigt worden[12].

Auch außerhalb der Europäischen Union sind die Regierungen kaum bereit, die Existenz von Überwachungsprogrammen ihrer Nachrichtendienste einzugestehen. Es gibt jedoch klare Anzeichen, dass derartige Programme zumindest seitens Australiens[13], Russlands[14], Indiens[15] und Chinas[16]

---

[11] Aussage von Charles Farr vor dem britischen Investigatory Powers Tribunal (Gericht zur Überprüfung der Überwachungstätigkeit) am 16. Mai 2014.

[12] Siehe insbesondere den Bericht des UN-Hochkommissariats für Menschenrechte über das Recht auf Privatsphäre im digitalen Zeitalter („The right to privacy in the digital age"), Ziffern 3, 4 und 5, veröffentlicht am 30. Juni 2014 und zugänglich unter folgendem Link: https://www.ccdcoe.org/sites/default/files/documents/UN-140730-RightToPrivacyReport.pdf

[13] http://www.theguardian.com/world/2014/oct/13/australias-defence-intelligence-agency-conducted-secret-programs-to-help-nsa

[14] http://www.theguardian.com/world/2014/sep/24/strasbourg-court-human-rights-russia-eavesdropping-texts-emails-fsb-

durchgeführt werden. Die Funktionsweise der aufgedeckten Überwachungsaktivitäten entspricht mit ziemlicher Sicherheit dem bekannten Muster: Die Nachrichtendienste erfassen personenbezogene Daten in sehr großem Ausmaß und arbeiten in unterschiedlichen Allianzen weltweit zusammen, indem sie Informationen austauschen. Zuweilen hat man den Eindruck, dass sich zahlreiche Länder die nationalen Sicherheitsinteressen eines einzigen Landes zueigen gemacht haben.

Aus der Perspektive des Datenschutzes ergibt sich daraus eine Reihe von Fragen. Ist die Verwendung (Verarbeitung) personenbezogener Daten durch Nachrichtendienste rechtmäßig? Wie sind die Daten erfasst worden, und auf welcher Rechtsgrundlage? Können personenbezogene Daten, die sich in der Obhut von privatwirtschaftlichen Unternehmen in der EU befinden, einfach vom Ausland her abgegriffen werden, ohne dass die betroffene Person merkt, dass dies geschieht, bzw. sich darüber im Klaren ist, dass dies geschehen könnte? Inwieweit ist das europaweit anerkannte Grundrecht auf Datenschutz heutzutage noch wirksam, wenn staatliche Einrichtungen offenbar dermaßen leicht auf personenbezogene Daten zugreifen können?

Über diese Fragen wurde in der Datenschutzgruppe rege diskutiert. Derzeit sind erst einige wenige Schlussfolgerungen gezogen worden, da eine umfassende Beurteilung sehr stark von den besonderen Umständen des jeweiligen Einzelfalls abhängt: Liegt ein Verdacht vor, welcher Rechtsrahmen ist anzuwenden, handelt es sich um eine spezifische und gezielte Datenerfassung usw.? Zugleich muss eine Diskussion darüber geführt werden, inwieweit der internationale und der europäische Datenschutzrechtsrahmen anwendbar ist bzw. sein sollte.

3. Allgemeiner Rechtsrahmen

Bei der Analyse des für Überwachungsaktivitäten geltenden Rechtsrahmens ist unbedingt die im Vertrag über die Europäische Union (EUV) Artikel 4

---

[15] Beispielsweise in Indien: https://www.opendemocracy.net/opensecurity/maria-xynou/big-democracy-big-surveillance-indias-surveillance-state

[16] Beispielsweise in China: http://www.theguardian.com/world/2011/jul/26/china-boosts-internet-surveillance (zuletzt aufgerufen am 20. November 2014).

Absatz 2 niedergelegte Ausnahmeregelung zu berücksichtigen, der zufolge „insbesondere die nationale Sicherheit […] weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten“ fällt. Derartige Aktivitäten unterliegen darüber hinaus einem wesentlich breiteren Spektrum von Rechtsvorschriften. Ausgehend von den ursprünglichen internationalen Normen, die weithin anerkannt sind und das Unionsrecht beeinflusst haben, sehen die einschlägigen Rechtsinstrumente der Vereinten Nationen ein allgemeines Menschenrecht auf Schutz vor willkürlichen oder ungesetzlichen Eingriffen in die Privatsphäre vor. Ferner ist durch die einschlägigen Rechtsinstrumente des Europarats und die einschlägige Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte (EGMR) ein europaweit gemeinsames Verständnis des Umfangs dieses Grundrechts auf Schutz der Privatsphäre sowie der zulässigen Eingriffe in dieses Recht gewährleistet.

3.1 Rechtsinstrumente der Vereinten Nationen

Die Datenschutzgruppe ruft in Erinnerung, dass die internationalen Menschenrechtsvorschriften den universellen Rahmen bilden, innerhalb dessen sämtliche Eingriffe in individuelle Rechte auf Schutz der Privatsphäre zu beurteilen sind.

Das internationale Menschenrecht auf Schutz der Privatsphäre ist in der Allgemeinen Erklärung der Menschenrechte der Vereinten Nationen (1948) sowie im Internationalen Pakt über bürgerliche und politische Rechte[17] niedergelegt.

Gemäß Artikel 12 der Allgemeinen Erklärung der Menschenrechte und gemäß Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte darf niemand willkürlichen oder ungesetzlichen Eingriffen in seine Privatsphäre ausgesetzt werden.

Jeder Staat, der sich der Charta der Vereinten Nationen unterworfen hat, ist verpflichtet, sich für die universelle Achtung und Verwirklichung der Menschenrechte und Grundfreiheiten einzusetzen[18]. Zudem ist jeder

[17] Internationaler Pakt über bürgerliche und politische Rechte, Resolution 2200A der Generalversammlung der Vereinten vom 16. Dezember 1966.

[18] Charta der Vereinten Nationen, Artikel 55 Buchstabe c)

Unterzeichnerstaat des Internationalen Pakts über bürgerliche und politische Rechte verpflichtet, die erforderlichen Schritte – im Einklang mit seinen eigenen verfassungsmäßigen Verfahren und mit dem Pakt – zu ergreifen, um alle Gesetze zu verabschieden und alle sonstigen Schritte zu ergreifen, die erforderlich sind, um die im Pakt niedergelegten Rechte zu verwirklichen. Dies umfasst die Bereitstellung wirkungsvoller Abhilfemaßnahmen – einschließlich der Ausarbeitung geeigneter Rechtsmittel – gegen Verletzungen der im Pakt niedergelegten Rechte sowie die wirksame Durchsetzung dieser Abhilfemaßnahmen und Rechtsmittel.

3.1.1 Resolution 68/167 der Generalversammlung der Vereinten vom 18. Dezember 2013

Mit der Resolution 68/167 der Generalversammlung der Vereinten Nationen[19] wurden die im Pakt niedergelegten Rechte bekräftigt und:

- anerkannt, dass eine Güterabwägung zwischen Privatsphäre und Sicherheit erforderlich ist, wobei festgestellt wurde, dass es im Interesse der öffentlichen Sicherheit gerechtfertigt sein kann, bestimmte sensible Daten zu sammeln und zu schützen, jedoch mit der Einschränkung, dass die Staaten dafür Sorge tragen müssen, ihre Pflichten nach den internationalen Menschenrechtsvorschriften umfassend einzuhalten;

- betont, dass dieselben Rechte, die Menschen offline haben, auch online geschützt werden müssen, insbesondere das Recht auf Schutz der Privatsphäre, wobei die Staaten aufgefordert wurden, diese Rechte auf sämtlichen digitalen Plattformen zu schützen;

- die Unterzeichnerstaaten aufgefordert, alle erdenklichen Schritte zu ergreifen, um bestehende Verletzungen dieser Rechte abzustellen und zudem Bedingungen zu schaffen, die eine Verletzung dieser Rechte verhindern; ferner wurden die Unterzeichnerstaaten aufgefordert, ihre nationalen Abläufe, Verfahren und Rechtsvorschriften (insbesondere hinsichtlich der Überwachung von Kommunikation, hinsichtlich des Abfangens und der

[19] Resolution 68/167 der Generalversammlung der Vereinten vom 21. Januar 2014 – http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167 (zuletzt aufgerufen am 20. November 2014).

Speicherung von personenbezogenen Daten einschließlich Massenüberwachung, -abfangen und -speicherung) zu überprüfen, um zu gewährleisten, dass die geltenden Rechtsvorschriften keine Verletzung der im Pakt niedergelegten Rechte gestatten; zudem wurden die Unterzeichnerstaaten aufgefordert, für die umfassende und wirksame Umsetzung ihrer Pflichten gemäß den internationalen Menschenrechtsvorschriften Sorge zu tragen.

Mit der Resolution wurden die Unterzeichnerstaaten des Pakts außerdem aufgefordert, unabhängige nationale Aufsichtsmechanismen einzurichten, um im Falle der Überwachung und des Abfangens von Kommunikation sowie des Sammelns von personenbezogenen Daten durch den Staat Transparenz und Rechenschaftspflicht zu gewährleisten. Insofern deckt sich diese UN-Resolution mit der in der am 10. April 2014 verabschiedeten Stellungnahme WP 215 der Datenschutzgruppe, in der eine Überprüfung der in den EU-Mitgliedstaaten bestehenden Mechanismen für die Aufsicht über die mitgliedstaatlichen Nachrichtendienste gefordert wird. Im Gefolge der im Jahr 2013 erfolgten Enthüllungen zur Überwachungspraxis stellte die Datenschutzgruppe die Notwendigkeit fest, auf mitgliedstaatlicher Ebene innerhalb der EU eine Überprüfung der bestehenden Mechanismen für die Aufsicht über die Aktivitäten der mitgliedstaatlichen Nachrichten- und Geheimdienste durchzuführen. Laut Einschätzung der Datenschutzgruppe sind diese Mechanismen oftmals maßgeblich für die Wirksamkeit des Datenschutzes und des Schutzes der Privatsphäre in der EU.

Die Datenschutzgruppe führte diese Erhebung in der Absicht durch, ein deutlicheres Bild über die unterschiedlichen Regelungen innerhalb Europas zu gewinnen. Zu diesem Zweck wurde ermittelt, in welchen Ländern bzw. Bereichen die jeweilige Datenschutzbehörde befugt ist, die Nachrichtendienste zu überwachen, und wo Einschränkungen bestehen. Laut Einschätzung der Datenschutzgruppe ist das wichtigste Ergebnis der Erhebung, dass die Datenschutzbehörden sich für eine engere Aufsicht aussprechen, um zu gewährleisten, dass die EU-Mitgliedstaaten einen kohärenten Rechtsrahmen für ihre Nachrichtendienste wahren. Zudem sollte der jeweilige mitgliedstaatliche Rechtsrahmen ggf. auf bestimmte Weise präzisiert werden, um letztlich für alle Bürgerinnen und Bürger sämtliche Datenschutzrechte zu

garantieren[20]. Die Einzelheiten zu den Ergebnissen dieser Erhebung sind in der genannten Stellungnahme nachzulesen[21].

Ferner wurde mit dieser UN-Resolution der Hohe Kommissar der Vereinten Nationen für Menschenrechte aufgefordert, einen Bericht über den Schutz und die Verwirklichung des Rechts auf Schutz der Privatsphäre im Kontext der inländischen und der extraterritorialen Überwachung und/oder Abfangung von digitaler Kommunikation sowie des Sammelns von personenbezogenen Daten – einschließlich Massenüberwachung – zu erstellen und dem Menschenrechtsrat sowie der Vollversammlung vorzulegen.

Eine derartige Resolution ist zwar nicht rechtsverbindlich, es wird damit aber trotzdem ein starkes Signal an die Unterzeichnerstaaten gesendet, dass ernsthaftes weiteres Nachdenken sowie kollektives und individuelles Handeln gemäß den in Kapitel 1 der UN-Charta niedergelegten Zielen der Vereinten Nationen erforderlich sind[22]. Ferner zielt die Resolution darauf ab, den durch den Internationalen Pakt über bürgerliche und politische Rechte garantierten

---

[20] In ihrer Stellungnahme (WP 215, S. 14 der deutschen Fassung) fordert die Datenschutzgruppe unter anderem eine *„effektive, solide und unabhängige externe Aufsicht, die entweder von einem zuständigen Gremium unter Mitwirkung der Datenschutzbehörden oder von der Datenschutzbehörde selbst wahrgenommen wird“*.

[21] Da der vorrangige Gegenstand des vorliegenden Arbeitsdokuments andere wichtige rechtliche Überlegungen sind, wird hier nicht näher auf diese Erhebung eingegangen.

[22] In der UN-Charta, Artikel 1 Absätze 3 und 4 heißt es zu den Zielen der Vereinten Nationen: „3. eine internationale Zusammenarbeit herbeizuführen, um internationale Probleme wirtschaftlicher, sozialer, kultureller und humanitärer Art zu lösen und die Achtung vor den Menschenrechten und Grundfreiheiten für alle ohne Unterschied der Rasse, des Geschlechts, der Sprache oder der Religion zu fördern und zu festigen;

4. ein Mittelpunkt zu sein, in dem die Bemühungen der Nationen zur Verwirklichung dieser gemeinsamen Ziele aufeinander abgestimmt werden.“

Im Rahmen der Diskussion über den UN-Bericht im November 2013 brachte der deutsche UN-Botschafter eine wichtige Frage ein: „Wir müssen uns fragen, ob alles, was technisch möglich ist, auch erlaubt sein darf.“ In dieser Frage spiegelt sich wider, dass ein weiteres Nachdenken erforderlich ist. Website: http://www.dw.de/germany-brazil-introduce-anti-spying-resolution-at-un-general-assembly/a-17213179 „http://www.dw.de/germany-brazil-introduce-anti-spying-resolution-at-un-general-assembly/a-17213179 "Germany, Brazil introduce anti-spying resolution“. Deutsche Welle (zuletzt aufgerufen am 20. November 2014)

Schutz auf elektronische Kommunikation und auf den Schutz der Privatsphäre auszuweiten.

3.1.2 UN-Bericht zum Recht auf Schutz der Privatsphäre im digitalen Zeitalter

Dieser Bericht[23] wurde im Juli 2014[24] verabschiedet, im Gefolge der oben skizzierten Ereignisse. Laut den im Bericht dargelegten Empfehlungen und Schlussfolgerungen ist eindeutig und dringend Wachsamkeit geboten, um sicherzustellen, dass bei sämtlichen Überwachungsregelungen oder -praktiken die internationalen Menschenrechtsvorschriften eingehalten werden, einschließlich des Rechts auf Schutz der Privatsphäre, indem wirksame Sicherheitsvorkehrungen gegen Missbrauch ausgearbeitet werden[25]. In dem Bericht werden die unzureichenden Rahmenbedingungen in vielen Ländern beklagt, die zu einem Mangel an Rechenschaftspflicht bei willkürlichen oder ungesetzlichen Eingriffen in das Recht auf Schutz der Privatsphäre beigetragen haben. Insbesondere werden mangelnde Transparenz im Umfeld der Überwachungspraktiken und mangelnde Rechtsrahmen genannt. Die Datenschutzgruppe verweist hiermit nachdrücklich auf die in dem UN-Bericht erhobene Forderung, dass die Staaten als Sofortmaßnahme ihre nationalen Abläufe, Verfahren und Rechtsvorschriften einer Überprüfung unterziehen sollten, um die umfassende Einhaltung der internationalen Menschenrechtsvorschriften zu gewährleisten.

In dem UN-Bericht wird zudem betont, dass es unbedingt erforderlich ist, diesen Prozess zur rechtlichen Überprüfung derart zu gestalten, dass er einen Dialog beinhaltet, in den sämtliche betroffenen Interessenträger eingebunden sind, einschließlich der UN-Mitgliedstaaten, der Zivilgesellschaft, der

---

[23] Bericht des UN-Hochkommissariats für Menschenrechte über das Recht auf Privatsphäre im digitalen Zeitalter, veröffentlicht am 30. Juni 2014. Website: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (zuletzt aufgerufen am 20. November 2014).

[24] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (zuletzt aufgerufen am 20. November 2014).

[25] Bericht des UN-Hochkommissariats für Menschenrechte über das Recht auf Privatsphäre im digitalen Zeitalter, veröffentlicht am 30. Juni 2014, S. 16, Ziffer 50.

wissenschaftlichen, akademischen und technischen Fachwelt, der Wirtschaft und Menschenrechtsexperten. Die Datenschutzgruppe nimmt dies mit besonderem Interesse zur Kenntnis und wird sich bemühen, durch Ausrichtung einer Fachkonferenz Ende 2014 zu einer umfassenderen Diskussion in Europa beizutragen, wie in ihrer Stellungnahme 4/2014 skizziert.

Ferner nimmt die Datenschutzgruppe zur Kenntnis, dass die Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre im Jahr 2013 eine Resolution[26] verabschiedet hat, mit der sie an ihre bereits zuvor erhobenen Forderungen nach einer detaillierteren Ausgestaltung des internationalen Rechts im Hinblick auf den Schutz der Privatsphäre und insbesondere im Hinblick auf den Datenschutz anknüpft. Mit ihrer Resolution fordern die Beauftragten für den Datenschutz und den Schutz der Privatsphäre die Regierungen auf, sich für die Verabschiedung eines Zusatzprotokolls zu Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte (IPbpR) einzusetzen. Dieses Zusatzprotokoll sollte auf den von der Internationalen Konferenz ausgearbeiteten und verabschiedeten Normen sowie auf den in der Allgemeinen Anmerkung (General Comment) Nr. 16 zum Pakt niedergelegten Bestimmungen beruhen.

Zusammenfassend ist festzustellen, dass – trotz einiger Initiativen in jüngster Zeit[27] – noch keine detailliertere Ausgestaltung der rechtlichen Bestimmungen zum Schutz der Privatsphäre auf UN-Ebene erfolgt ist. In Europa ist das Recht auf Schutz der Privatsphäre – ebenso wie das Recht auf Datenschutz – bereits wesentlich detaillierter ausgestaltet worden, womit die ersten Schritte getan sind, um bestimmte Rechte, die in der Allgemeinen Erklärung der Menschenrechte niedergelegt sind, gemeinsam zu verwirklichen.

---

[26] Entschließung „Verankerung des Datenschutzes und des Schutzes der Privatsphäre im internationalen Recht“, angenommen von der 35. Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre in Warschau, September 2014. Website: https://privacyconference2013.org/web/pageFiles/kcfinder/files/5.%20International%20law%20resolution%20EN%281%29.pdf (zuletzt aufgerufen am 20. November 2014).

[27] In der Allgemeinen Anmerkung (General Comment) Nr. 16 des Menschenrechtsausschusses der Vereinten Nationen zu Artikel 17 IPbpR, die am 8. April 1988 verabschiedet wurde, ist eine detaillierte Auslegung dieses Rechts enthalten, einschließlich bestimmter Datenschutzgrundsätze, in Absatz 10.

3.2 Rechtsinstrumente des Europarats

Die beiden wichtigsten verbindlichen Rechtsinstrumente hinsichtlich der Grundrechte und des Datenschutzes auf der Ebene des Europarats sind die Europäische Menschenrechtskonvention[28] (EMRK) und das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten[29] (in Folgenden „Übereinkommen Nr. 108“).

3.2.1 Die EMRK

Gemäß Artikel 1 EMRK sind die Vertragsparteien dazu verpflichtet, allen ihrer Hoheitsgewalt[30] unterstehenden Personen die in der Konvention bestimmten Rechte und Freiheiten zuzusichern. Daraus ergibt sich, dass den Vertragsparteien nicht nur negative, sondern auch positive Verpflichtungen auferlegt sind, nämlich dass die Behörden des betreffenden Staates verpflichtet

---

[28] Konvention zum Schutz der Menschenrechte und Grundfreiheiten, Rom, 4. November 1950.

[29] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, Straßburg, 28. Januar 1981, SEV Nr. 108

[30] Der Begriff der Hoheitsgewalt, auf den in EMRK Artikel 1 Bezug genommen wird, ist weder im Übereinkommen noch in den Vorarbeiten definiert worden. In seiner Rechtsprechung setzt der EGMR den Begriff der „wirksamen Kontrolle“ seitens eines Staates als maßgeblich für dessen Hoheitsgewalt im Sinne von Artikel 1 an. So rief der EGMR in seinem Urteil in der Rechtssache Loizidou / Türkei vom 23. März 1995 in Erinnerung, dass – obwohl durch Artikel 1 (Verpflichtung zur Achtung der Menschenrechte) Grenzen für den Geltungsbereich der Hoheitsgewalt gezogen sind – der in diesem Artikel 1 enthaltene Begriff der „Hoheitsgewalt“ nicht auf das Hoheitsgebiet der Unterzeichnerstaaten der EMRK begrenzt ist. Insbesondere könne sich die Zuständigkeit eines Staates auch dadurch ergeben, dass dieser Staat infolge militärischer Aktionen – ungeachtet ihrer Rechtsmäßigkeit oder Unrechtmäßigkeit – die wirksame Kontrolle über ein Gebiet außerhalb seines Hoheitsgebiets erlangt. Die Verpflichtung eines Staates, in einem derartigen Gebiet für die Wahrung der in der EMRK niedergelegten Rechte und Freiheiten Sorge zu tragen, ergebe sich aus dem Umstand, dass dieser Staat in diesem Gebiet die wirksame Kontrolle ausübe, gleichgültig ob dies durch die Streitkräfte des betreffenden Staates oder durch eine untergeordnete lokale Verwaltung erfolge. Siehe in dieser Hinsicht auch EGMR, Al-Skeini u. a. / Vereinigtes Königreich, 7. Juli 2011.

Nach dem Völkerrecht bezieht sich der Begriff „Hoheitsgewalt“ auf die Befugnis eines Staates, die Normen zu gestalten, gerichtlich auszulegen und durchzusetzen, denen seine Rechtssubjekte unterworfen sind.

sind, die erforderlichen Maßnahmen zur Wahrung eines Rechts zu ergreifen[31] *bzw. angemessene und geeignete Maßnahmen zu ergreifen, um die Rechte des Einzelnen zu schützen,*[32,33]. Unter außergewöhnlichen Umständen sind laut Rechtsprechung des EGMR die Hoheitsgewalt und die Pflichten eines Vertragsstaats nicht auf das Hoheitsgebiet dieses Vertragsstaats begrenzt. In seiner Rechtsprechung zu dieser Frage setzt der EGMR den Begriff der „wirksamen Kontrolle" seitens des Vertragsstaats als maßgeblich für die Ausübung der Hoheitsgewalt an.

In dieser Hinsicht heißt es im Echelon-Bericht des Europäischen Parlaments unter Verweis auf die Rechtsinstrumente des Europarats: *„[Die Vertragsstaaten] bleiben für ihr Staatsgebiet verantwortlich und damit den europäischen Rechtsunterworfenen auch dann verpflichtet, wenn die Ausübung der Hoheitsgewalt durch nachrichtendienstliche Tätigkeit von einem anderen Staat vorgenommen wird."*[34]

3.2.1.1 Anwendungsbereich der EMRK

Zusätzlich zu dem in Artikel 1 definierten räumlichen Geltungsbereich gilt die EMRK auch für diejenigen Gebiete, für deren internationale Beziehungen die betreffende Vertragspartei verantwortlich ist, sofern diese Vertragspartei eine entsprechende Notifizierung gemäß EMRK Artikel 56 Absatz 1 vorgenommen hat.

Allgemeine Einschränkungen zum sachlichen Anwendungsbereich der EMRK sind nicht zulässig. Allerdings hatten die Vertragsparteien zum Zeitpunkt der Unterzeichnung und Ratifikation die Gelegenheit, Vorbehalte hinsichtlich etwaiger Bestimmungen der Konvention anzumelden, sofern ein auf ihrem Hoheitsgebiet geltendes Gesetz nicht mit der betreffenden Bestimmung

---

[31] EGMR, Hokkanen / Finnland, 24. August 1994.

[32] EGMR, Lopez-Ostra / Spanien, 9. Dezember 1994.

[33] Jean-François Akandji-Kombe, *Positive obligations under the European Convention on Human Rights*, Human rights handbook No. 7, Europarat, 2007.

[34] Siehe Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) – A5-0264/2001, S. 93 der deutschen Fassung.

übereinstimmt[35]. Was die EU-Mitgliedstaaten anbelangt, so betrifft keiner der angemeldeten Vorbehalte EMRK Artikel 8 „Recht auf Achtung des Privat- und Familienlebens“[36].

3.2.1.2 Das Recht auf Achtung der Privatsphäre

In der EMRK Artikel 8 Absatz 1 ist niedergelegt: „*Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.*“

Die Begriffe „Privatleben“ und „Korrespondenz“ umfassen Telefon- und Telekommunikationsdaten.[37] Aus der Rechtsprechung zur EMRK ergibt sich, dass der Geltungsbereich des Schutzes dieses Grundrechts sich nicht nur auf den Inhalt der Kommunikation erstreckt, sondern beispielsweise auch auf das Datum und die Länge von Telefongesprächen, sowie die gewählten Nummern umfasst, da derartige Daten als integraler Bestandteil von Telefongesprächen zu betrachten seien.[38] Mit anderen Worten: Der Geltungsbereich dieses Schutzes erstreckt sich sowohl auf den Inhalt der Kommunikation als auch auf die so genannten „Verkehrsdaten“ oder „Metadaten“.

3.2.1.3 Mögliche Eingriffe in das Recht auf Achtung der Privatsphäre

Gemäß EMRK Artikel 8 Absatz 2 darf eine Behörde in die Ausübung des Rechts auf Achtung des Privatlebens nur eingreifen, soweit der Eingriff:

• gesetzlich vorgesehen (wobei die betreffenden Rechtsvorschriften öffentlich zugänglich sein und absehbare Folgen haben müssen) [39]und

---

[35] Siehe EMRK Artikel 57.

[36] Die Notifizierungen und Erklärung sind verfügbar unter http://www.conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=005&CM=8&DF=29/07/2014&CL=ENG&VL=1. (zuletzt aufgerufen am 20. November 2014).

[37] Siehe EGMR, Klass u. a. / Deutschland, 6. September 1978, Randnr. 41.

[38] Siehe EGMR, Malone / Vereinigtes Königreich, 2. August 1984, Randnr. 84.

[39] Siehe EGMR, Malone / Vereinigtes Königreich, 2. August 1984, Randnr. 83 ff.

• in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.

Aus der ersten Bedingung folgt, dass die zweite Bedingung sich auf die Interessen der Vertragsparteien der Konvention bezieht und nicht auf die Interessen von Drittländern, ungeachtet der Frage, ob diese Interessen übereinstimmen.

In der Rechtsprechung des EMRK heißt es: „*Diese Bestimmung muss, da sie eine Ausnahme zu einem von der Konvention geschützten Recht enthält, eng ausgelegt werden.*“ [40] In der Rechtssache Klass führte das Gericht näher aus: „*Befugnisse zur geheimen Überwachung von Bürgern, wie sie für den Polizeistaat typisch sind, können nach der Konvention nur insoweit hingenommen werden, als sie zur Erhaltung der demokratischen Einrichtungen unbedingt notwendig sind.“*[41]

Daher muss in einer demokratischen Gesellschaft jeglicher Eingriff in das Recht auf Achtung des Privatlebens (d. h. im vorliegenden Fall jeder einzelne Zugriff seitens einer Behörde auf personenbezogene Daten im Zusammenhang mit Kommunikation) dahingehend begründet werden, dass dieser Eingriff unbedingt für einen der in Artikel 8 Absatz 2 genannten Zwecke erforderlich ist.

Nach Auffassung des EGMR ist ein solcher Eingriff als notwendig zu betrachten, wenn er einem zwingenden gesellschaftlichen Bedürfnis entspricht, in einem angemessenen Verhältnis zu dem verfolgten Zweck steht und wenn die von der Behörde als Begründung angeführten Gründe stichhaltig und ausreichend sind.[42]

---

[40] Siehe EGMR, Klass u. a. / Deutschland, 6. September 1978, Randnr. 42. Siehe auch das Urteil in der Rechtssache Youth Initiative for Human Rights / Serbien, 25. Juni 2013 , Randnr. 24-26, mit dem bestätigt wurde, dass auch die Geheimdienste die Grundrechte sowie die jeweiligen einzelstaatlichen Rechtsvorschriften zur Umsetzung dieser Grundrechte achten bzw. einhalten müssen.

[41] Siehe Klass, oben zitiert, auch Randnr. 42.

[42] Siehe u. a. EGMR, S. und Marper / Vereinigtes Königreich, 4. Dezember 2008, Randnr. 101.

In dieser Hinsicht stellte das Gericht in der Rechtssache S. und Marper / Vereinigtes Königreich[43] fest, dass die pauschale und unterschiedslose Speicherung der Fingerabdrücke der Antragsteller – bei denen es sich um Personen handelte, die verdächtigt aber nicht verurteilt wurden, – gemäß EMRK Artikel 8 Absatz 2 nicht gerechtfertigt war.

Im EU-Kontext befand auch der Gerichtshof der Europäischen Union (EuGH), dass zum Nachweis der Verhältnismäßigkeit des Eingriffs aufgezeigt werden muss, dass keine anderen Verfahren verfügbar waren, mit denen weniger stark in die genannten Grundrechte eingegriffen worden wäre[44].

Im spezifischen Bereich der nationalen Sicherheit stellte der EGMR fest, dass die Rechtsvorschriften hinsichtlich der Vorhersehbarkeitsanforderung sich zwar von den entsprechenden Rechtsvorschriften in anderen Bereichen unterscheiden dürfen, dass es aber stets ein Gesetz geben müsse, in dem eindeutig niedergelegt ist, unter welchen Umständen und zu welchen Bedingungen der Staat geheime – und somit potenziell gefährliche – Eingriffe in die Ausübung des Rechts auf Achtung des Privatlebens durchführen darf.[45]

Dies ist nach Einschätzung der Datenschutzgruppe in besonderem Maße relevant und anwendbar auf Überwachungsaktivitäten, an denen ein

---

[43] Siehe EGMR, S. und Marper / Vereinigtes Königreich, 4. Dezember 2008, insbesondere Randnr. 125: Nach Auffassung des Gerichts ist durch die – im Fall der Antragsteller angewandte – pauschale und unterschiedslose Befugnis zur Speicherung von Fingerabdrücken, Zellproben und DNA-Profilen von Personen, die einer Straftat zwar verdächtigt aber nicht verurteilt wurden, das gebotene Gleichgewicht zwischen den widerstreitenden öffentlichen und privaten Interessen verletzt und der Antragsgegner - nämlich der Staat – hat in dieser Hinsicht den hinnehmbaren Ermessensspielraum überschritten. Deshalb handle es sich bei der betreffenden Speicherung um einen unverhältnismäßigen Eingriff in das Recht der Antragsteller auf Achtung des Privatlebens, der nicht als in einer demokratischen Gesellschaft notwendig zu betrachten sei. Angesichts dieser Schlussfolgerung braucht das Gericht sich nicht mit den Kritikpunkten der Antragsteller hinsichtlich der Angemessenheit von bestimmten Schutzmaßnahmen zu befassen, beispielsweise dass ein zu breiter Zugriff auf die betreffenden personenbezogenen Daten erfolge oder dass ein unzureichender Schutz gegen eine unsachgemäße oder missbräuchliche Verwendung dieser personenbezogenen Daten bestehe.

[44] Siehe EuGH, Verbundene Rechtssachen C-92/09 P und C-93/09 P, Volker und Markus Schecke GbR und Hartmut Eifert / Land Hessen, 9. November 2010, Randnr. 81.

[45] Siehe EGMR, Rotaru / Rumänien, 4. Mai 2000, Randnr. 50, 52 und 55; und Amann / Schweiz, 16. Februar 2000, Randnr. 50 ff.

Vertragsstaat des EMRK mitwirkt – gleichgültig ob allein oder in Zusammenarbeit mit einem Drittland[46]. Zudem ist das Recht auf Achtung des Privatlebens für sämtliche Personen garantiert, die der Hoheitsgewalt eines Vertragsstaats unterstehen, ungeachtet der Staatsangehörigkeit oder des Wohnorts dieser Personen.

Diese Argumentation wird gestützt durch das Urteil in der Rechtssache Loizidou / Türkei[47], in dem das Gericht feststellte, dass der Begriff der Hoheitsgewalt im Sinne der vorliegenden Bestimmung nicht begrenzt sei auf das Staatsgebiet der Hohen Vertragsparteien, sondern dass die Vertragsstaaten verantwortlich seien für die Handlungen ihrer Behörden, gleichgültig ob diese Handlungen innerhalb oder außerhalb der Staatsgrenzen erfolgen, wenn sich durch diese Handlungen Folgen außerhalb des Staatsgebiets ergeben. In dieser Hinsicht verwies das Gericht auf das Urteil des EGMR in der Rechtssache Drozd und Janousek / Frankreich und Spanien[48].

3.2.2 Übereinkommen Nr. 108

„Zweck dieses Übereinkommens ist es, im Hoheitsgebiet[49] jeder Vertragspartei für jedermann ungeachtet seiner Staatsangehörigkeit oder seines Wohnorts sicherzustellen, dass seine Rechte und Grundfreiheiten, insbesondere sein Recht auf einen Persönlichkeitsbereich, bei der automatischen Verarbeitung personenbezogener Daten geschützt werden ('Datenschutz').“

Dem Übereinkommen können auch Staaten beitreten, die nicht Mitglied des Europarats sind[50]. Mit der Ratifizierung des Übereinkommens bekundet ein

---

[46] In einem solchen Fall ist nicht das Drittland verantwortlich, sondern der EMRK-Vertragsstaat.

[47] Siehe EGMR, Loizidou / Türkei, 23. März 1995, Randnr. 62, mit Verweis auf die Rechtssache Drozd und Janousek, siehe Drozd und Janousek / Frankreich und Spanien, 26. Juni 1992, Randnr. 91.

[48] Siehe EGMR, Drozd und Janousek / Frankreich und Spanien, 26. Juni 1992, Randnr. 91.

[49] Der räumliche Geltungsbereich kann durch die Vertragsstaaten gemäß Artikel 24 des Übereinkommens näher festgelegt werden.

[50] Artikel 23 des Übereinkommens.

Land, dass es sich entschlossen für den Schutz personenbezogener Daten einsetzt und sich ausdrücklich an gemeinsame internationale Normen halten möchte. Die Datenschutzgruppe würde es daher begrüßen, wenn außereuropäische Staaten tatsächlich dem Übereinkommen beitreten würden.

3.2.2.1 Geltungsbereich des Übereinkommens Nr. 108

Grundsätzlich sind das Übereinkommen Nr. 108 und sein Zusatzprotokoll für *„automatisierte Dateien/Datensammlungen und automatische Verarbeitungen von personenbezogenen Daten im öffentlichen und privaten Bereich anzuwenden“*[51], außer soweit ein Vertragsstaat gemäß Artikel 3 Absatz 2 Buchstabe a bekanntgegeben hat, dass er das Übereinkommen auf bestimmte Arten von Dateien/Datensammlungen nicht anwendet. Es ist ein Verzeichnis dieser Arten von Dateien/Datensammlungen zu erstellen und zu hinterlegen. In das Verzeichnis darf der Vertragsstaat jedoch Arten automatisierter Dateien/Datensammlungen nicht aufnehmen, die nach seinem innerstaatlichen Recht Datenschutzvorschriften unterliegen.[52]

Daher gelten die innerstaatlichen Rechtsvorschriften zur Umsetzung des Übereinkommens auch für Dateien, die im Zusammenhang mit der „nationalen Sicherheit“ eines Vertragsstaats des Übereinkommens stehen, außer sofern der betreffende Vertragsstaat sich ausdrücklich für eine Ausnahme entschieden hat, diese Ausnahme wie vorgeschrieben in einem Verzeichnis niedergelegt und dieses Verzeichnis hinterlegt hat. Bis heute hat nur eine Minderheit der Vertragsstaaten Erklärungen hinterlegt, um für die „staatliche Sicherheit“ oder „Staatsgeheimnisse“ die Ausnahmeregelung in Anspruch zu nehmen[53].

Manche Vertragsstaaten haben sich zudem entschieden, das Übereinkommen auch auf Dateien/Datensammlungen mit personenbezogenen Daten anzuwenden, die nicht automatisch verarbeitet werden, wie in Artikel 3 Absatz 2 Buchstabe c vorgesehen, sowie auf Informationen über Personengruppen, Vereinigungen, Stiftungen, Gesellschaften, Körperschaften

[51] Siehe Artikel 3 Absatz 1 des Übereinkommens.

[52] Siehe Artikel 3 Absatz 2 Buchstabe a des Übereinkommens.

[53] Zehn Parteien haben eine solche Erklärung hinterlegt, darunter die EU-Mitgliedstaaten Irland, Lettland, Malta und Rumänien.

oder andere Stellen, die unmittelbar oder mittelbar aus natürlichen Personen bestehen, unabhängig davon, ob diese Stellen Rechtspersönlichkeit besitzen oder nicht, wie in Artikel 3 Absatz 2 Buchstabe b vorgesehen.

3.2.2.2 Datenschutzgrundsätze innerhalb des Übereinkommens Nr. 108

Kapitel II des Übereinkommens enthält die „Grundsätze für den Datenschutz". Der Grundsatz der Qualität der Daten (Artikel 5) umfasst die Verpflichtung, dass die Daten nach Treu und Glauben und auf rechtmäßige Weise beschafft sein und verarbeitet werden müssen; dass sie für festgelegte und rechtmäßige Zwecke gespeichert sein müssen und nicht so verwendet werden dürfen, dass es mit diesen Zwecken unvereinbar ist; dass sie den Zwecken, für die sie gespeichert sind, entsprechen müssen, dafür erheblich sein müssen und nicht darüber hinausgehen dürfen; dass sie sachlich richtig und wenn nötig auf den neuesten Stand gebracht sein müssen; dass sie so aufbewahrt werden müssen, dass der Betroffene nicht länger identifiziert werden kann, als es die Zwecke, für die sie gespeichert sind, erfordern.

In Artikel 6 ist unter der Überschrift „Besondere Arten von Daten" niedergelegt, dass personenbezogene Daten, welche die rassische Herkunft, politische Anschauungen oder religiöse oder andere Überzeugungen erkennen lassen, sowie personenbezogene Daten, welche die Gesundheit oder das Sexualleben betreffen, sowie ferner personenbezogene Daten über Strafurteile nur unter der Bedingung automatisch verarbeitet werden dürfen, dass das innerstaatliche Recht einen geeigneten Schutz gewährleistet.

Artikel 7 enthält die Verpflichtung, dass geeignete Sicherungsmaßnahmen getroffen werden müssen, und in Artikel 8 sind die Rechte der von der Datenverarbeitung betroffenen Person auf Auskunft, Zugang, Berichtigung und Löschung sowie ggf. auf ein Rechtsmittel niedergelegt, falls ihrer diesbezüglichen Forderung nicht entsprochen wird.

Gemäß Artikel 10 verpflichte sich jede Vertragspartei, geeignete Sanktionen und Rechtsmittel für Verletzungen der Vorschriften des innerstaatlichen Rechts, welche diese Grundsätze für den Datenschutz verwirklichen, festzulegen. Gemäß Artikel 11 steht es jeder Vertragspartei frei, dass sie den Betroffenen ein größeres Maß an Schutz als das in diesem Übereinkommen vorgeschriebene gewährt.

3.2.2.3 Ausnahmen

Gemäß Artikel 9 ist eine Abweichung von den genannten Grundsätzen – Qualität (Artikel 5), geeigneter Schutz bei sensiblen Daten (Artikel 6) und Rechte der Betroffenen (Artikel 8)[54] – zulässig, wenn eine derartige Abweichung:

- durch das Recht der Vertragspartei vorgesehen und

- in einer demokratischen Gesellschaft eine notwendige Maßnahme ist: zum Schutz des Betroffenen oder der Rechte und Freiheiten Dritter; oder zum Schutz der Sicherheit des Staates, der öffentlichen Sicherheit sowie der Währungsinteressen des Staates oder zur Bekämpfung von Straftaten.

Es sei einmal mehr in Erinnerung gerufen, dass der EGMR in seiner Rechtsprechung großen Wert auf die Auslegung der in Artikel 8 der EMRK niedergelegten Ausnahmen legt. Diese Argumentation gilt umso mehr für die Auslegung der im Übereinkommen Nr. 108 niedergelegten Ausnahmen[55]. Der EGMR legt Grundrechte auf ziemlich weite Weise aus, gemäß dem Grundsatz der Effektivität, demzufolge diese Rechte in der Weise ausgelegt werden können, die für den besten Schutz des Menschen sorgt[56]. Das ergibt sich auch aus dem Zusatzprotokoll zum Übereinkommen, dem zufolge es im Ermessen der Vertragsstaaten steht, Abweichungen vom Grundsatz des angemessenen Schutzniveaus festzulegen. Die einschlägigen innerstaatlichen Rechtsvorschriften müssen allerdings dem inhärenten Grundsatz des europäischen Rechts entsprechen, dass Bestimmungen zur Festlegung von Ausnahmen restriktiv auszulegen sind, damit die Ausnahme nicht zur Regel wird.[57]

---

[54] Siehe Artikel 9 des Übereinkommens.

[55] Man kann argumentieren, dass das Gericht seine Zuständigkeit für die Auslegung des Übereinkommens Nr. 108 auf die Bestimmungen von Artikel 8 der EMRK stützt.

[56] Jean-François Akandji-Kombe, *Positive obligations under the European Convention on Human Rights*, Human rights handbook No. 7, Europarat, 2007.

[57] Vgl. „Report on the Additional Protocol to Convention 108 on the control authorities and cross border flows of data“ (Bericht zum Zusatzprotokoll zum Übereinkommen zum Schutz

3.2.2.4 Das Zusatzprotokoll Nr. 181[58] und die Regelungen für Datenübermittlungen

In einem nicht von allen EU-Mitgliedstaaten ratifizierten Zusatzprotokoll zum Übereinkommen Nr. 108 sind Regelungen zum grenzüberschreitenden Datenverkehr sowie die Verpflichtung zur Einrichtung von unabhängigen Kontrollstellen für den Datenschutz niedergelegt.

Gemäß Artikel 2 Absatz 1 des Zusatzprotokolls ist die grenzübergreifende Weitergabe von personenbezogenen Daten an einen Staat oder eine Organisation, der nicht der Hoheitsgewalt eine Vertragspartei des Übereinkommens untersteht, nur unter der Bedingung zulässig, dass der Empfänger ein angemessenes Schutzniveau für die beabsichtigte Datenweitergabe gewährleistet.

Gemäß Artikel 2 Absatz 2 kann jedoch abweichend von dieser Bestimmung jede Vertragspartei die Weitergabe personenbezogener Daten erlauben, a) wenn dies im internen Recht vorgesehen ist – wegen spezifischer Interessen des Betroffenen, oder – wegen berechtigter überwiegender Interessen, insbesondere wichtiger öffentlicher Interessen; oder b) wenn Garantien, die sich insbesondere aus Vertragsklauseln ergeben können, von der für die Weitergabe verantwortlichen Stelle geboten werden und diese von den zuständigen Behörden in Übereinstimmung mit dem internen Recht für ausreichend befunden werden.

---

des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr), Artikel 2 Absatz 2 Buchstabe a.

[58] Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr; SEV-Nr. 181), Straßburg, 8. November 2001.

3.2.2.5 Empfehlung Nr. (87)15[59] über die Verarbeitung personenbezogener Daten im Polizeibereich

Zusätzlich zu den oben genannten verbindlichen Rechtsinstrumenten hat das Ministerkomitee des Europarats mehrere an die Mitglieder des Europarats gerichtete Empfehlungen hinsichtlich der Verarbeitung personenbezogener Daten verabschiedet. Auf der Grundlage dieser Empfehlungen wurden in mehreren Mitgliedstaaten inländische Rechtsvorschriften erlassen, und einige der Empfehlungen werden in rechtsverbindlichen EU-Rechtsinstrumenten genannt und umgesetzt.

Mit der Empfehlung Nr. (87)15 wird die Nutzung von personenbezogenen Daten im Polizeibereich geregelt. Es handelt sich um Leitlinien für die Mitgliedstaaten auf der Grundlage der EMRK Artikel 8, des Übereinkommens Nr. 108 und der Abweichungen, die gemäß Artikel 9 des Übereinkommens zulässig sind. Die Empfehlung erstreckt sich auf sämtliche Aufgaben, welche die Polizeibehörden zur Verhinderung und Bekämpfung von Straftaten und zur Aufrechterhaltung der öffentlichen Ordnung durchführen müssen.[60] Daher ist die Empfehlung nur relevant, soweit Aufgaben der nationalen Sicherheit durch reguläre Polizeibehörden durchgeführt werden, und nicht durch Nachrichten- oder Geheimdienste.

3.2.3 Schlussfolgerung

Als Schlussfolgerung ergibt sich: Da sämtliche EU-Mitgliedstaaten zugleich auch Vertragsstaaten der EMRK und des Übereinkommens sind, unterliegen sie einer positiven Verpflichtung – wie durch die Rechtsprechung der europäischen Gerichte ausgearbeitet –, für sämtliche Personen, die ihrer Hoheitsgewalt unterstehen, den wirksamen Schutz der Grundrechte zu gewährleisten.

Etwaige Einschränkungen dieser Grundrechte sind nur hinnehmbar, wenn die durch den EGMR festgelegten Bedingungen erfüllt sind, d. h. wenn diese

[59] Empfehlung Nr. (87)15 über die Nutzung personenbezogener Daten im Polizeibereich, 17. September 1987.

[60] Siehe Empfehlung Nr. R(87)15 „Scope and definitions" (Geltungsbereich und Begriffsbestimmungen).

Einschränkungen auf spezifische, genau beschriebene und vorhersehbare Situationen begrenzt sind. Die Datenschutzgruppe betont daher: Sofern eine wirksame Einhaltung der Rechtsinstrumente des Europarats angestrebt wird, kann seitens der Vertragsstaaten der EMRK kein massenhaftes, unterschiedsloses und heimliches Sammeln von Daten über Personen toleriert werden, die der Hoheitsgewalt von EU-Mitgliedstaaten unterstehen.

4. Unionsrecht

Hinsichtlich der anwendbaren Rechtsvorschriften auf Unionsebene werden in diesem Abschnitt der Geltungsbereich der Ausnahme für den Bereich der nationalen Sicherheit sowie relevante Texte, wie Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) sowie die Artikel 7 und 8 sowie 52 Absatz 1 der Grundrechtecharta der Europäischen Union, erörtert. Hinsichtlich des Sekundärrechts erfolgt eine Beurteilung der Bedingungen, unter denen die Bestimmungen der Richtlinie 95/46/EG[61,62] und der Datenschutzrichtlinie anwendbar sind, wobei besonders auf die Regelungen für Datenübermittlungen gemäß der Richtlinie 95/46/EG eingegangen wird.

4.1 Ausnahme für den Bereich der nationalen Sicherheit

Bevor auf die Einzelheiten der einschlägigen EU-Rechtsvorschriften eingegangen wird, ist eine Erörterung der Bedeutung der in Artikel 4 Absatz 2 des Vertrags über die Europäische Union (EUV) niedergelegten Ausnahme für den Bereich der nationalen Sicherheit erforderlich. In diesem Artikel heißt es: „*Die Union achtet die Gleichheit der Mitgliedstaaten […] und ihre jeweilige nationale Identität […] Sie achtet die grundlegenden Funktionen des Staates, insbesondere […] den Schutz der nationalen Sicherheit. Insbesondere die nationale Sicherheit fällt weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten.*“ Daher gilt das Unionsrecht – einschließlich der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“)[63] –

[61] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

[62] Wenn in diesem Kapitel von der Richtlinie die Rede ist, sind stets die mitgliedstaatlichen Rechtsvorschriften zur Umsetzung dieser Richtlinie mit gemeint, auch wenn diese nicht ausdrücklich genannt werden.

[63] Amtsblatt C 364 vom 18. Dezember 2000.

nicht für Angelegenheiten, welche die nationale Sicherheit der Mitgliedstaaten betreffen. Das ist eine wichtige Ausnahme der Anwendbarkeit des Unionsrechts, mit besonderer Relevanz für viele Fragen, die im vorliegenden Arbeitsdokument erörtert werden, da nach allgemeiner Einschätzung die Nachrichten- und Geheimdienste ihre Aufgaben zu Zwecken der nationalen Sicherheit der Mitgliedstaaten erfüllen.

4.1.1 Fehlen einer klaren Definition des Begriffs „nationale Sicherheit“

Kurz gesagt: Es ist der EU nicht gestattet, Gesetze im Zusammenhang mit der nationalen Sicherheit der Mitgliedstaaten zu erlassen. Es gibt im Unionsrecht jedoch keine klare Definition, was unter „nationaler Sicherheit“ zu verstehen ist. Ganz im Gegenteil: Die EU-Verträge enthalten und beziehen sich auf Begriffe, die kaum von der nationalen Sicherheit zu unterscheiden sind oder die zumindest eng mit ihr verwoben sind; für diese Bereiche ist es der EU jedoch sehr wohl gestattet, Gesetze zu erlassen.

Erstens ist im Vertrag über die Arbeitsweise der Europäischen Union (AEUV), Abschnitt „Der Raum der Freiheit, der Sicherheit und des Rechts“, Artikel 75, die Zuständigkeit der EU niedergelegt, einen Rahmen für Maßnahmen zur Verhütung und Bekämpfung von Terrorismus und damit verbundener Aktivitäten zu schaffen. Angesichts dieser Bestimmung ergibt sich die Frage, wie man denn zwischen der Bekämpfung des Terrorismus und dem Schutz der nationalen Sicherheit unterscheiden möchte. Spezifische Maßnahmen zur Bekämpfung des Terrorismus lassen diese Schwierigkeit noch deutlicher hervortreten.

Die EU und ihre Mitgliedstaaten arbeiten bei der Terrorismusbekämpfung eng mit den Vereinigten Staaten zusammen, beispielsweise durch Weitergabe von Daten über Finanztransaktionen zur weiteren Auswertung, im Rahmen des Programms zum Aufspüren der Finanzierung des Terrorismus (TFTP – Terrorist Finance Tracking Program). Der Geltungsbereich des zugrundeliegenden TFTP2-Abkommens[64] umfasst Verhinderung, Untersuchung, Aufspüren und Verfolgung von Handlungen, die zur

[64] Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung für die Zwecke des Programms der USA zum Aufspüren der Finanzierung des Terrorismus, 27. Juli 2010.

ernsthaften Destabilisierung der grundlegenden Strukturen eines Landes führen würden. Ferner müssen die Vereinigten Staaten etwaige Hinweise, die aus den seitens der EU-Mitgliedstaaten gemäß diesem Programm weitergegebenen Daten gewonnen werden und die für die Anstrengungen der EU-Mitgliedstaaten zur Terrorismusbekämpfung relevant sind, an die EU-Mitgliedstaaten weitergeben. Nach Einschätzung der Datenschutzgruppe weist die Verarbeitung personenbezogener Daten für derartige Zwecke zumindest eine ganz erhebliche Ähnlichkeit zu Aktivitäten zu Zwecken auf, die nach allgemeiner Auffassung in den Bereich der nationalen Sicherheit fallen, – ist aber offenbar sehr wohl Regelungen unterworfen, die seitens der EU vereinbart worden sind.

Ferner ist in EUV Artikel 24 Absatz 1 sowie AEUV Artikel 2 Absatz 4 niedergelegt, dass sich die Zuständigkeit der Union in Angelegenheiten der Gemeinsamen Außen- und Sicherheitspolitik (GASP) „*auf sämtliche Fragen im Zusammenhang mit der Sicherheit der Union*“ erstreckt. Daher liegt die „*Sicherheit der Union*“ innerhalb des Anwendungsbereichs des Unionsrechts und muss ebenfalls von der nationalen Sicherheit der Mitgliedstaaten unterschieden werden, die – gemäß EUV Artikel 4 Absatz 2 – außerhalb des Anwendungsbereichs des Unionsrechts liegt.

Auf der Ebene des Sekundärrechts ist in der Richtlinie 2000/31/EG[65] Artikel 3 niedergelegt: „*Die Mitgliedstaaten können Maßnahmen ergreifen, die im Hinblick auf einen bestimmten Dienst der Informationsgesellschaft […] abweichen, wenn die folgenden Bedingungen erfüllt sind: a) Die Maßnahmen […] sind aus einem der folgenden Gründe erforderlich: […] Schutz der öffentlichen Sicherheit, einschließlich der Wahrung nationaler Sicherheits- und Verteidigungsinteressen […]“*. Ein ähnlicher Wortlaut findet sich in der Datenschutzrichtlinie 95/46/EG Artikel 3 Absatz 2 erster Spiegelstrich: „*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, […] und auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines*

[65] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“).

wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich;" Diesen Bestimmungen zufolge muss man die Begriffe „nationale Sicherheit", „Sicherheit des Staates", „öffentliche Sicherheit" und „Verteidigung" allesamt voneinander unterscheiden.

Auch aus der Rechtsprechung des EuGH ergibt sich keine klare Definition des Begriffs „nationale Sicherheit". In der Rechtssache Promusicae[66] befand der EuGH: „*[Diese Ausnahmen] betreffen zum einen die nationale Sicherheit, die Verteidigung und die öffentliche Sicherheit, die spezifische Tätigkeiten der Staaten oder der staatlichen Stellen sind und mit den Tätigkeitsbereichen von Einzelpersonen nichts zu tun haben […]* "

Generalanwalt Francis Geoffrey Jacobs bezog sich in seinen Schlussanträgen in der Rechtssache C-120/94[67] auf die bestehende Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR). Der EGMR hatte festgestellt, dass es – angesichts der Zuständigkeit eines Staates für das „Leben der Nation" – in erster Linie einem jeden Vertragsstaat zukomme, zu ermitteln, ob dieses Leben durch einen öffentlichen Notstand gefährdet ist, und ggf. zu entscheiden, wie weit die Anstrengungen zur Überwindung dieses Notstands gehen müssen.

Zusammenfassend ist festzustellen, dass sich weder in den einschlägigen Bestimmungen des Unionsrechts noch in der Rechtsprechung des EuGH eine klare Definition des Begriffs „nationale Sicherheit" findet. Zudem verwenden die EU und die EU-Mitgliedstaaten eine ganze Reihe von sehr ähnlichen Begriffen, die einen Bezug zur Sicherheit aufweisen, ohne diese Begriffe zu definieren: „innere Sicherheit", „nationale Sicherheit", „Sicherheit des Staates", „öffentliche Sicherheit" und „Verteidigung". All diese Begriffe müsste man demnach voneinander unterscheiden. Nach Auffassung der Datenschutzgruppe sind sie jedoch unauflöslich miteinander verwoben. Die Definition der Umstände, die eine Ausnahme für den Bereich der nationalen Sicherheit begründen, kann daher nicht ausschließlich mit rechtlichen Argumenten erfolgen. In der Praxis muss man offenbar die politische Situation

[66] EuGH, Productores de Música de España (Promusicae) / Telefónica de España SAU (C-275/06, Urteil vom 29. Januar 2008), Randnr. 51.

[67] Kommission der Europäischen Gemeinschaften / Republik Griechenland; Schlussanträge vom 6. April 1995, Randnr. 55.

zum Zeitpunkt dieser „Entscheidung“ sowie die relevanten Akteure berücksichtigen. Fest steht, dass bei Aktivitäten von Nachrichten- und Geheimdiensten in der Regel akzeptiert wird, dass sie als Ausnahme für den Bereich der nationalen Sicherheit zu betrachten sind, wohingegen eine solche Akzeptanz nicht immer gegeben ist, wenn allgemeine Strafverfolgungsbehörden vergleichbare Aufgaben erfüllen.

Das einzige Organ, das mehr Rechtssicherheit hinsichtlich der Frage schaffen kann, was unter die Ausnahme für den Bereich der nationalen Sicherheit fällt und was nicht, ist der EuGH. Nur der Gerichtshof kann eine genauere Definition für den Geltungsbereich des Unionsrechts sowie – in der Folge – für die Anwendbarkeit der Charta liefern. Bis der Gerichtshof eine solche Klärung zum Geltungsbereich der Ausnahme für den Bereich der nationalen Sicherheit geliefert hat, fordert die Datenschutzgruppe von den Mitgliedstaaten, dass sie sich an die bestehende Rechtsprechung[68] halten, d. h. ihrer Verpflichtung nachkommen, die Inanspruchnahme dieser Ausnahme in jedem einzelnen Fall zu begründen. So befand der EuGH beispielsweise im Urteil in der Rechtssache Kadi I klar und deutlich, dass die Verpflichtungen, die sich aus einem internationalen Abkommen ergeben, keine Beeinträchtigung der in den EU-Verträgen niedergelegten Grundsätze nach sich ziehen dürfen, einschließlich des Grundsatzes, dass bei sämtlichen Handlungen der EU die Grundrechte geachtet werden müssen.

In der Rechtssache Rotaru / Rumänien[69] urteilte der EGMR ähnlich, dass die gesammelten Daten für den verfolgten Zweck der nationalen Sicherheit sein müssen und dass – auch im Kontext der nationalen Sicherheit – durch ein Gesetz festgelegt sein muss, welche Informationen gespeichert werden dürfen, gegen welche Personenkreise Überwachungsmaßnahmen wie das Sammeln und Speichern von Informationen ergriffen werden dürfen, unter welchen

---

[68] Einschließlich C-387/05, Europäische Kommission / Italienische Republik, Urteil vom 15. Dezember 2009, Randnr. 45: *„Aus ihnen lässt sich kein allgemeiner, dem Vertrag immanenter Vorbehalt ableiten, der jede Maßnahme, die im Interesse der öffentlichen Sicherheit getroffen wird, vom Anwendungsbereich des Gemeinschaftsrechts ausnähme. Würde ein solcher Vorbehalt unabhängig von den besonderen Tatbestandsmerkmalen der Bestimmungen des Vertrags anerkannt, so könnte das die Verbindlichkeit und die einheitliche Anwendung des Gemeinschaftsrechts beeinträchtigen.“*

[69] Siehe insbesondere EGMR, Rotaru / Rumänien, Randr. 53 bis 63, 4. Mai 2000, verfügbar (in englischer Sprache) unter http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58586#{%22itemid%22:[%22001-58586%22]} (zuletzt aufgerufen am 20. November 2014).

Umständen solche Maßnahmen getroffen werden dürfen und welches Verfahren einzuhalten ist, sowie für welchen Zeitraum solche Informationen maximal gespeichert werden dürfen. Zudem müsse das Gesetz ausdrückliche und detaillierte Bestimmungen enthalten, welcher Personenkreis auf die Dateien zugreifen darf, sowie ferner zur Art der Dateien, zum einzuhaltenden Verfahren und zur zulässigen Nutzung der auf diese Weise gewonnenen Informationen.

Bei der Beurteilung der Anwendbarkeit der Ausnahme für den Bereich der nationalen Sicherheit sollte ferner berücksichtigt werden, ob es sich um eine grundsätzliche Ausnahme handelt – wie die Ausnahme, die in den Verträgen sowie in der Richtlinie 95/46/EG Artikel 3 Absatz 2 niedergelegt ist – oder ob die Ausnahme Teil einer Bestimmung ist, durch welche aus Gründen der nationalen Sicherheit bestimmte Schutzmaßnahmen ausgeschlossen werden. Letzteres ist beispielsweise der Fall, wenn es Mitgliedstaaten gestattet wird, aus Gründen der nationalen Sicherheit Beschränkungen für das Zugangsrecht der von der Datenverarbeitung betroffenen Person festzulegen, wie in der Richtlinie 95/46/EG Artikel 13 Absatz 1 Buchstabe a niedergelegt.

4.1.2 Nationale Sicherheitsinteressen eines Drittlands

Die bis hierher dargelegten Erörterungen betreffen die Auslegung der Ausnahme für den Bereich der nationalen Sicherheit im Verhältnis zwischen der Europäischen Union und ihren Mitgliedstaaten. In diesem Zusammenhang ist die nationale Sicherheit maßgeblich für die Unterscheidung zwischen den Zuständigkeiten der Union und den Zuständigkeiten der Mitgliedstaaten. Die Tatsache, dass die Aktivitäten der Mitgliedstaaten im Bereich der nationalen Sicherheit vom Geltungsbereich des Unionsrechts ausgenommen sind, bedeutet jedoch nicht, dass das Unionsrecht nicht gelten würde, wenn auf Daten, die EU-Datenschutzrecht unterliegen, durch Drittländer im Namen der nationalen Sicherheit dieser Drittländer zugegriffen wird.

Die Datenschutzgruppe begreift EUV Artikel 4 als einen Versuch zur Abgrenzung der Zuständigkeiten zwischen der Union und den Mitgliedstaaten. Die Mitgliedstaaten bestehen auf ihrer Souveränität, wenn es um die nationale Sicherheit geht. Etwas ganz anderes ist dagegen die Pflicht zur Einhaltung des EU-Datenschutzrechts, der die für die Verarbeitung Verantwortlichen unterliegen, selbst wenn sie zugleich den Rechtsvorschriften zur nationalen

Sicherheit eines Drittlands unterliegen. Deshalb weist die Datenschutzgruppe nachdrücklich darauf hin, dass die Ausnahme für den Bereich der nationalen Sicherheit als Bestimmung zur Abgrenzung der Zuständigkeiten zwischen der EU und ihren Mitgliedstaaten zu verstehen ist – nicht jedoch als allgemeine Ausnahme von den EU-Datenschutzanforderungen für sämtliche Aktivitäten, die seitens eines Drittlands im Namen der nationalen Sicherheit verlangt werden.

Zudem muss nach Ansicht der Datenschutzgruppe unbedingt kritisch geprüft werden, ob Überwachungsaktivitäten tatsächlich zu Zwecken der nationalen Sicherheit durchgeführt werden. Dabei ist anzumerken, dass die aufgedeckten US-amerikanischen Überwachungsaktivitäten zwar auf den ersten Blick auf den Schutz der nationalen Sicherheit abzielen, es in Wirklichkeit aber um wesentlich breiter gefächerte Interessen geht. So sind beispielsweise gemäß dem FISA Act Abhörmaßnahmen erlaubt, sofern die Informationen einen *„Bezug zur […] Führung der auswärtigen Angelegenheiten der Vereinigte Staaten aufweisen".*[70] Es ist sehr fraglich, ob irgendeine Definition der in EU-Rechtsinstrumenten enthaltenen Ausnahme für den Bereich der nationalen Sicherheit – selbst wenn man sie über ihren ursprünglichen Geltungsbereich hinaus dehnen würde – einen derart breiten Zweck abdecken könnte. Zudem nimmt die Datenschutzgruppe zur Kenntnis, dass nur ein sehr schmaler Grat den Zweck der nationalen Sicherheit von Strafverfolgungszwecken trennt, wie auch die Einbindung von verschiedenen Agenturen (wie FBI, CIA und NSA) in die US-amerikanischen Überwachungsprogramme zeigt. Die Achtung des Grundsatzes der Zweckbindung ist daher unerlässlich.

Die Datenschutzgruppe ist besorgt, dass Unionsrecht im Allgemeinen und EU-Datenschutzrecht im Besonderen in der Praxis möglicherweise mit dem bloßen Verweis umgangen werden kann, dass die Datenverarbeitung für Zwecke der nationalen Sicherheit erforderlich sei.[71] Das ist eine gefährliche Entwicklung, insbesondere wenn nicht die nationale Sicherheit eines Mitgliedstaats auf dem

---

[70] Titel 50, United States Code, Paragraf 1801 Absatz e Ziffer 2 Buchstabe B

[71] Es sei in Erinnerung gerufen, dass gemäß der Rechtsprechung des EuGH – darunter ZZ / Secretary of State (C-300/11) – bei jeder Einschränkung eines Grundrechts insbesondere der Wesensgehalt des betreffenden Grundrechts zu wahren ist, und dass zudem – unter Wahrung des Grundsatzes der Verhältnismäßigkeit – diese Einschränkung erforderlich sein muss, tatsächlich seitens der Europäischen Union anerkannten Zielsetzungen entsprechen muss (Randnr. 52) sowie einer gerichtlichen Kontrolle unterliegen muss (Randnr. 58).

Spiel steht, sondern angeblich die nationale Sicherheit eines Drittlands. Die Datenschutzgruppe betont, dass es gemäß der in den Verträgen vorgesehenen Ausnahme nicht möglich ist, sich lediglich auf nationale Sicherheitsinteressen eines Drittlands zu berufen, um die Anwendbarkeit des Unionsrechts zu umgehen.

Es kann allerdings vorkommen, dass ein Mitgliedstaat behauptet, dass es sich bei einer Bedrohung für die nationale Sicherheit eines Drittlandes, das Partner oder Verbündeter dieses Mitgliedstaats ist, zugleich auch um eine Bedrohung für die eigene nationale Sicherheit dieses Mitgliedstaats handle – so dass das Unionsrecht nicht anwendbar sei. Die Datenschutzgruppe räumt ein, dass es Bereiche geben kann, in denen ein nationales Sicherheitsinteresse eines EU-Mitgliedstaats und eines Drittlandes dicht beieinander liegen und dass in solchen Fällen die Grenzen der nationalen Sicherheit eines EU-Mitgliedstaats zuweilen unscharf sein können. Die Behauptung, dass die nationalen Sicherheitsinteressen eines Drittlandes gleichgerichtet mit den eigenen nationalen Sicherheitsinteressen eines EU-Mitgliedstaats seien, sollte allerdings nur statthaft sein, wenn von Fall zu Fall eine ordnungsgemäße Begründung gegenüber den zuständigen Behörden erfolgt. Andernfalls muss sich der Mitgliedstaat an Unionsrecht halten. Diese Argumentation wird gestützt durch das Urteil des EuGH in der Rechtssache Europäischen Kommission / Italienische Republik, in dem klargestellt wird, dass die bloße Nennung der Ausnahme für den Bereich der nationalen Sicherheit nicht ausreichend ist, um die Nichtanwendbarkeit des Unionsrechts zu begründen.[72] Dies muss umso mehr gelten, wenn ein Mitgliedstaat behauptet, dass ein nationales Sicherheitsinteresse eines Drittlandes Teil seiner eigenen nationalen Sicherheitsinteressen sei. Daher muss die Rechtsgrundlage, um sich auf das nationale Sicherheitsinteresse eines Drittlandes zu berufen, klar in einer innerstaatlichen Rechtsvorschrift niedergelegt werden; dies gilt auch für rechtverbindliche internationale politische Abkommen, die von Regierungen von Mitgliedstaaten geschlossen werden[73].

[72] C-387/05, Randnr. 45 (andere Angaben oben)

[73] Die Artikel-29-Datenschutzgruppe ist sich bewusst, dass es auch in einigen bestehenden verbindlichen internationalen Rechtsinstrumenten – beispielsweise in Rechtshilfeabkommen – Bestimmungen gibt, die EU-Mitgliedstaaten erlauben, von den betreffenden Rechtsinstrumenten abzuweichen. Eine solche Abweichung ist aber nur zulässig, um eine Beeinträchtigung der wesentlichen Interessen dieses Mitgliedstaats zu verhindern – nicht

4.2 Gesetzgebung zum Datenschutz

Im AEUV Artikel 16 Absatz 1 ist niedergelegt: „Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.“ – ein Recht, also, das für „jede Person“ gilt.

Zur Umsetzung dieses Rechts ist in Artikel 16 Absatz 2 eine neue Rechtsgrundlage für das Erlassen von EU-Datenschutz-Rechtsvorschriften hinsichtlich der Verarbeitung von personenbezogenen Daten durch Organe und Einrichtungen der EU sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, sowie ferner hinsichtlich des freien Datenverkehrs. Zudem wird mit dem genannten Artikel vorgeschrieben, dass die Einhaltung dieser Vorschriften von unabhängigen Behörden überwacht wird.

In der Erklärung Nr. 21 zum Vertrag von Lissabon ist festgehalten, dass in den Bereichen Justizielle Zusammenarbeit in Strafsachen und Polizeiliche Zusammenarbeit möglicherweise spezifische Regelungen erforderlich sind. Aber auch diese Regelungen sind auf der Grundlage des AEUV Artikel 16 zu erlassen.

Hinsichtlich der nationalen Sicherheit ist in der Erklärung Nr. 20 zum Vertrag von Lissabon festgehalten: Immer wenn auf der Grundlage von Artikel 16 erlassene Regelungen zum Datenschutz direkte Auswirkungen auf die nationale Sicherheit haben könnten, sollten die spezifischen Besonderheiten der Angelegenheit berücksichtigt werden. In der Erklärung wird auch in Erinnerung gerufen, dass die geltenden Rechtsvorschriften – insbesondere die Richtlinie 95/46/EG – spezifische Abweichungen in dieser Hinsicht enthalten.

---

jedoch um eine Beeinträchtigung der wesentlichen Interessen eines Drittlandes zu verhindern, das keine Vertragspartei des betreffenden Rechtsinstruments ist. Dreh- und Angelpunkt ist also, dass der betreffende EU-Mitgliedstaat klar begründet, dass es sich um seine eigenen wesentlichen Interessen handelt.

4.3 Die Charta der Grundrechte der Europäischen Union

4.3.1 Der Geltungsbereich der Charta

Infolge der oben erörterten Ausnahme für den Bereich der nationalen Sicherheit und im Gegensatz zu den einschlägigen Rechtsinstrumenten des Europarats ist der Geltungsbereich der Charta begrenzt. Trotzdem gelten – soweit die nationale Sicherheit von EU-Mitgliedstaaten nicht betroffen ist – die in der Charta niedergelegten Grundsätze – insbesondere die Artikel 7 und 8 – für die Organe und Einrichtungen der EU sowie für sämtliche Aktivitäten von Mitgliedstaaten bei der Umsetzung von Unionsrecht.

4.3.2 Das Recht auf Achtung des Privatlebens und das Recht auf Datenschutz in der Charta

In Artikel 7 der Charta, der Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) entspricht, ist ein allgemeines Recht auf Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation niedergelegt, um den Einzelnen vor Eingriffen seitens der Behörden zu schützen. In Artikel 8 Absatz 1 ist niedergelegt, dass jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten hat und dass solche Daten nur verarbeitet werden dürfen, wenn bestimmte wesentliche Anforderungen erfüllt sind. Diese wesentlichen Anforderungen sind in Artikel 8 Absätze 2 und 3 der Charta niedergelegt *„Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden."* Ferner ist hier festgelegt, dass jede Person das Recht hat, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken; sowie ferner dass die Einhaltung dieser Vorschriften von einer unabhängigen Stelle überwacht wird.

In dem Urteil, mit dem die Richtlinie zur Vorratsdatenspeicherung[74] kassiert wurde, stellte der EuGH fest, dass *„die […] Pflicht, […] Daten über das*

[74] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG.

Privatleben einer Person und ihre Kommunikationsvorgänge während eines bestimmten Zeitraums auf Vorrat zu speichern, als solche einen Eingriff in die durch Art. 7 der Charta garantierten Rechte darstellt. Zudem stellt der Zugang der zuständigen nationalen Behörden zu den Daten einen zusätzlichen Eingriff in dieses Grundrecht dar […]. Desgleichen greift die [Vorratsdatenspeicherung] in das durch Art. 8 der Charta garantierte Grundrecht auf den Schutz personenbezogener Daten ein, da sie eine Verarbeitung personenbezogener Daten vorsieht.“[75] Ferner argumentiert der Gerichtshof, dass die Richtlinie zur Vorratsdatenspeicherung *„keine klaren und präzisen Regeln zur Tragweite des Eingriffs in die in Art. 7 und Art. 8 der Charta verankerten Grundrechte vorsieht. Somit ist festzustellen, dass die Richtlinie einen Eingriff in diese Grundrechte beinhaltet, der in der Rechtsordnung der Union von großem Ausmaß und von besonderer Schwere ist, ohne dass sie Bestimmungen enthielte, die zu gewährleisten vermögen, dass sich der Eingriff tatsächlich auf das absolut Notwendige beschränkt.“*[76]

Auch wenn sich die Rechtssache zur Vorratsdatenspeicherung auf eine Angelegenheit der Strafverfolgung bezieht, ist die Argumentation des Gerichtshofs von großer Bedeutung, insbesondere für jene Programme, bei denen der Zweck der Datenverarbeitung die Bekämpfung von Terrorismus und/oder schweren Straftaten umfasst (da diese beiden Zwecke nach bestehender Auffassung unter die Zuständigkeit der Europäischen Union fallen[77]). Anders formuliert: Um die Einhaltung des EU-Datenschutzrechtsrahmens zu gewährleisten, müssen diese Programme durch genaue Bestimmungen eingegrenzt werden, so dass eine Beschränkung auf das absolut Notwendige sichergestellt ist. Diese Schutzmaßnahmen sind in der Charta Artikel 52 Absatz 1 niedergelegt.

[75] Siehe EuGH, Digital Rights Ireland sowie Seitlinger u. a. (Verbundene Rechtssachen C-293/12 und C-594/12), 8. April 2014, Randnr. 34-36.

[76] Ebenda, Randnr. 64

[77] Siehe Abschnitt 4.1.1.

4.3.3 Der Umfang von Einschränkungen des Rechts auf Achtung des Privatlebens und des Rechts auf Datenschutz

Gemäß der Charta Artikel 52 Absatz 1 sind Einschränkungen der Ausübung der in der Charta anerkannten Rechte und Freiheiten zulässig, aber nur soweit diese Einschränkungen:

- erforderlich und verhältnismäßig sind,
- den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen,
- gesetzlich vorgesehen sind,
- und den Wesensgehalt der betreffenden Rechte und Freiheiten achten.

In der Rechtssache ZZ / Secretary of State for the Home rief der EuGH in Erinnerung, dass *„dass Art. 52 Abs. 1 der Charta zwar Einschränkungen der Ausübung der in ihr anerkannten Rechte zulässt, dabei aber verlangt, dass jede Einschränkung insbesondere den Wesensgehalt des fraglichen Grundrechts achtet, und außerdem voraussetzt, dass jede Einschränkung unter Wahrung des Grundsatzes der Verhältnismäßigkeit erforderlich ist und tatsächlich den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen entspricht.“*[78]

Zudem bekräftigte der Gerichtshof, dass der Nachweis erbracht werden muss, dass die betreffende spezifische Einschränkung tatsächlich erforderlich ist, um die Sicherheit des Staates zu schützen – und dass die bloße Nennung einer solchen Ausnahme seitens des Mitgliedstaats nicht ausreicht: *„Es obliegt daher der zuständigen nationalen Behörde, entsprechend den nationalen*

[78] Siehe EuGH, ZZ / Secretary of State for the Home department, Rechtssache C-300/11, 4. Juni 2013, Randnr. 51.

Zudem hat der EuGH in der Rechtssache Unitrading verfügt, dass mitgliedstaatliche Rechtsvorschriften „die Ausübung der durch die Gemeinschaftsrechtsordnung verliehenen Rechte nicht praktisch unmöglich machen oder übermäßig erschweren (Effektivitätsgrundsatz)“ dürfen. CJEU, Unitrading Ltd / Staatssecretaris van Financiën, Rechtssache CRS437/13, 23. Oktober 2014.

Verfahrensregeln den Nachweis dafür zu erbringen, dass die Sicherheit des Staates tatsächlich beeinträchtigt würde, wenn dem Betroffenen die genauen und umfassenden Gründe, die einer […] getroffenen Entscheidung zugrunde liegen, […] mitgeteilt würden. […] Daraus folgt, dass es keine Vermutung zugunsten des Vorliegens und der Stichhaltigkeit der von einer nationalen Behörde angeführten Gründe gibt.“[79]

Und selbst wenn der Nachweis für die Notwendigkeit einer solchen Einschränkung erbracht wird, ist deshalb keine pauschale Abweichung von der Verpflichtung zur Wahrung der Grundrechte zulässig: *„Wenn sich dagegen zeigt, dass die Sicherheit des Staates der Mitteilung der entsprechenden Gründe an den Betroffenen tatsächlich entgegensteht, hat die gerichtliche Kontrolle […] im Rahmen eines Verfahrens zu erfolgen, das die Erfordernisse, die sich aus der Sicherheit des Staates ergeben, und diejenigen aus dem Recht auf einen effektiven gerichtlichen Rechtsschutz in angemessener Weise zum Ausgleich bringt und dabei die eventuellen Eingriffe in die Ausübung dieses Rechts auf das unbedingt Erforderliche begrenzt.“*[80]

4.3.4 Zusammenspiel zwischen der Charta und der EMRK

Die Geltungsbereiche der Charta und der EMRK sind nicht identisch. Wie oben erörtert ist der Bereich der nationalen Sicherheit vom Geltungsbereich des Unionsrechts – einschließlich der Charta – ausgenommen. Dagegen sind die Vertragsstaaten der EMRK durch den Wortlaut der Konvention verpflichtet, allen ihrer Hoheitsgewalt unterstehenden Personen bestimmte Rechte und Freiheiten zuzusichern, darunter das Recht auf Achtung des Privatlebens, und die EMRK enthält keine allgemeine Ausnahme für den Bereich der nationalen Sicherheit. Allerdings ist es auch gemäß der EMRK den EMRK-Vertragsstaaten gestattet, in die Ausübung des Rechts auf Achtung des Privatlebens im Einklang mit ihren innerstaatlichen Rechtsvorschriften einzugreifen, soweit die betreffende Maßnahme im Interesse der nationalen Sicherheit in einer demokratischen Gesellschaft notwendig ist.

[79] Ebenda, Randnr. 61.

[80] *Ebenda,* Randnr. 64.

In der Charta Artikel 52 Absatz 3 ist niedergelegt: „Soweit [die] Charta Rechte enthält, die den durch die [EMRK] garantierten Rechten entsprechen, haben sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der [EMRK] verliehen wird.“ Die in den beiden Texten niedergelegten Grundsätze sind daher umfassend miteinander vereinbar. Zudem ist in dem genannten Artikel niedergelegt, dass diese Bestimmung dem nicht entgegensteht, dass das Recht der Union einen weiter gehenden Schutz gewährt.

4.4 Richtlinie 95/46/EG[81,82]

4.4.1 Anwendungsbereich der Richtlinie

Die Richtlinie 95/46/EG findet keine Anwendung 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“*. Diese Einschränkung des Anwendungsbereichs ist in Artikel 3 Absatz 2 Richtlinie niedergelegt. Darin spiegelt sich die Aufteilung der Zuständigkeiten zwischen der EU und den Mitgliedstaaten wider, insbesondere vor dem Inkrafttreten des Vertrags von Lissabon. Trotzdem ist die Richtlinie nicht als irrelevant im Kontext der Strafverfolgung und von Angelegenheiten der nationalen Sicherheit zu betrachten. Im Gegenteil: Durch die Richtlinie wird zwar die Datenverarbeitung seitens der Strafverfolgungsbehörden und seitens der Nachrichtendienste nicht geregelt, aber durch die mitgliedstaatlichen Rechtsvorschriften zur Umsetzung der Richtlinie wird die Übermittlung von personenbezogene Daten von den für die Verarbeitung Verantwortlichen bzw. von den Auftragsverarbeitern an die Nachrichtendienste und an die Strafverfolgungsbehörden geregelt, wenn den für die Verarbeitung

[81] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

[82] Wenn in diesem Kapitel von der Richtlinie die Rede ist, sind stets die mitgliedstaatlichen Rechtsvorschriften zur Umsetzung dieser Richtlinie mit gemeint, auch wenn diese nicht ausdrücklich genannt werden.

Verantwortlichen bzw. den Auftragsverarbeitern eine solche Datenübermittlung angeordnet wird. Gemäß Artikel 13 der Richtlinie darf der nationale Gesetzgeber – unter bestimmten Bedingungen – Rechtsvorschriften zur Einschränkung bestimmter Rechte und Pflichten erlassen, so dass beispielsweise der Zweck der Datenverarbeitung geändert werden kann.

Wie in Abschnitt 4.1 erörtert, bezieht sich die Ausnahme für den Bereich der nationalen Sicherheit auf die nationale Sicherheit der EU-Mitgliedstaaten; diese *„fällt weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten."*[83] Daher erfolgt kein Ausschluss der Anwendbarkeit der Richtlinie, wenn die Datenverarbeitung nicht die nationale Sicherheit der EU oder der EU-Mitgliedstaaten betrifft, sondern die nationale Sicherheit eines Drittlandes. In solchen Fällen gilt die Richtlinie, sofern eines der nachfolgend zitierten Anwendbarkeitskriterien erfüllt ist. Folglich müssen die für die Verarbeitung Verantwortlichen die Richtlinie einhalten und können Durchsetzungsmaßnahmen unterworfen werden.

Hinsichtlich des persönlichen/räumlichen Geltungsbereich ist in Artikel 4 Absatz 1 niedergelegt, dass die mitgliedstaatlichen Rechtsvorschriften zur Umsetzung der Richtlinie auf die Verarbeitung personenbezogener Daten anzuwenden sind, wenn:

a) die Verarbeitung im Rahmen der Tätigkeiten einer Niederlassung ausgeführt wird, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet eines EU-Mitgliedstaats besitzt;

In der Stellungnahme der Datenschutzgruppe zum anwendbaren Recht finden sich eine Reihe von Kriterien als Hilfestellung zur Klärung der Frage, was als Niederlassung im Sinne dieser Bestimmung zu betrachten ist. Dabei wird auf einen funktionalen Ansatz Wert gelegt, d. h. es kommt nicht so sehr auf den Standort der Daten oder des für die Verantwortung Verantwortlichen an, sondern es ist der Kontext der Aktivitäten der Niederlassung zu berücksichtigen und der Grad der Mitwirkung an der Verarbeitung personenbezogener Daten.[84] Der EuGH hat ferner klargestellt, dass Artikel 4 Absatz 1 Buchstabe a Richtlinie nicht verlangt, dass die *Verarbeitung personenbezogener Daten 'von' der betreffenden Niederlassung selbst*

[83] EUV Artikel 4 Absatz 2

[84] Artikel-29-Datenschutzgruppe, Stellungnahme 8/2010 zum anwendbaren Recht, 16. Dezember 2010.

ausgeführt wird"[85]. Ferner befindet der Gerichtshof: *„Außerdem kann diese Wendung im Hinblick auf das Ziel der Richtlinie […], nämlich […] einen wirksamen und umfassenden Schutz der Grundfreiheiten und Grundrechte natürlicher Personen, […] nicht eng ausgelegt werden"*[86].

b) der für die Verarbeitung Verantwortliche nicht im Hoheitsgebiet des Mitgliedstaats, aber an einem Ort niedergelassen ist, an dem das einzelstaatliche Recht dieses Mitgliedstaats gemäß dem internationalen öffentlichen Recht Anwendung findet;

c) der für die Verarbeitung Verantwortliche nicht im Gebiet der Gemeinschaft niedergelassen ist und zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel[87] zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind, es sei denn, dass diese Mittel nur zum Zweck der Durchfuhr durch das Gebiet der Europäischen Gemeinschaft verwendet werden.

In diesem Fall hat der für die Verarbeitung Verantwortliche gemäß Artikel 4 Absatz 2 einen im Hoheitsgebiet des genannten Mitgliedstaats ansässigen Vertreter zu benennen, unbeschadet der Möglichkeit eines Vorgehens gegen den für die Verarbeitung Verantwortlichen selbst.

Die Datenschutzgruppe begrüßt, dass der räumliche Anwendungsbereich der EU-Datenschutzrechtsvorschriften in der vorgeschlagenen Allgemeinen Datenschutzverordnung ausdrücklicher definiert werden soll. In Artikel 3 Absatz 2 des Vorschlags der Kommission[88] heißt es nämlich: „Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen, wenn die

---

[85] EuGH, *Google / Spanien,* 13. Mai 2014, Randnr. 52.

[86] *Ebenda,* Randnr. 54.

[87] In der oben genannten Stellungnahme der Artikel-29-Datenschutzgruppe finden sich weitere Leitlinien zur Auslegung des Begriffs „Mittel".

[88] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Allgemeine Datenschutzverordnung).

Datenverarbeitung a) dazu dient, diesen Personen in der Union Waren oder Dienstleistungen anzubieten, oder b) der Beobachtung ihres Verhaltens dient."

Der Vorschlag befindet sich zwar derzeit noch in der Diskussion im Parlament und im Rat, doch die beiden Gesetzgeber der EU sind sich hinsichtlich des von der Kommission vorgeschlagen Geltungsbereich im Wesentlichen einig. Der Rat hat seine ausdrückliche Unterstützung für den vorgeschlagenen räumlichen Geltungsbereich der Verordnung geäußert und hat betont, dass umfassend sichergestellt werden muss, dass die EU-Datenschutzrechtsvorschriften auch auf für die Verarbeitung Verantwortliche angewandt werden, wenn eine Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen erfolgt[89]. Das Parlament hat ebenfalls seine Unterstützung für den vorgeschlagenen Anwendungsbereich bekundet und ihn sogar noch ausgeweitet[90].

In seinem Urteil von 2009 zur Vorratsdatenspeicherung befand der EuGH, dass Artikel 95 des früheren EG-Vertrags (Annäherung der Rechtsvorschriften im Binnenmarkt) die gültige Rechtsgrundlage darstellte, um eine Pflicht zur Vorratsdatenspeicherung zu verhängen. In seiner Argumentation legte der Gerichtshof dar, dass die Richtlinie 2006/24/EG sich auf die Aktivitäten von Diensteanbietern im Binnenmarkt bezieht, eine Änderung ihrer Datenschutzpflichten enthält[91], erhebliche wirtschaftliche Auswirkungen auf diese Diensteanbieter hat und keine Regelungen hinsichtlich der Aktivitäten von Behörden zu Strafverfolgungszwecken enthält. Das von Irland vorgebrachte Argument, dass die Pflicht zur Vorratsdatenspeicherung nur auf der Grundlage von Titel VI des früheren EU-Vertrags (Justiz und Inneres) verhängt werden könne, wurde zurückgewiesen.

In der Rechtssache „Vorratsdatenspeicherung" wurde die obligatorische Speicherung von personenbezogenen Daten durch Diensteanbieter – obwohl

[89] Rat der Europäischen Union, Pressemitteilung, 3319. Tagung des Rates der Europäischen Union (Justiz und Inneres), 5. und 6. Juni 2014; sowie Dokument 2012/0011 (COD).

[90] Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Allgemeine Datenschutzverordnung).

[91] Festgelegt durch die Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation).

sie zu Strafverfolgungszwecken erfolgen sollte – als Verarbeitung betrachtet, die mitgliedstaatlichen Rechtsvorschriften zur Umsetzung von EU-Datenschutzregelungen (insbesondere der Datenschutzrichtlinie für die elektronische Kommunikation[92]) unterliegt. Bei der Richtlinie zur Vorratsdatenspeicherung handelte es sich daher um eine spezifische Abweichung von bestimmten Bestimmungen der Datenschutzrichtlinie für die elektronische Kommunikation[93].

Ebenso gelten mitgliedstaatliche Rechtsvorschriften zur Umsetzung der Richtlinie 95/46/EG für die Verarbeitung von Daten durch private Stellen für gewerbliche Zwecke, einschließlich der von derartigen privaten Stellen ausgehenden Übermittlung von Daten. Sie gelten auch für die Verarbeitung durch die Behörden von EU-Mitgliedstaaten, soweit diese Verarbeitung unter die Richtlinie fällt, d. h. nicht durch Artikel 3 Absatz 2 ausgenommen ist.

Das Gericht stellte auch klar, dass diese Situation nicht mit dem Kontext des Urteils in der Rechtssache „Fluggastdatensätze“ (PNR – Passenger Name Records)[94] vergleichbar ist. Das Gericht argumentierte: *„Im Unterschied zu dem [durch das PNR-Urteil kassierten] Beschluss 2004/496, der eine Übermittlung personenbezogener Daten innerhalb eines von staatlichen Stellen geschaffenen Rahmens zum Schutz der öffentlichen Sicherheit betraf, bezieht sich nämlich die Richtlinie 2006/24 auf die Tätigkeiten der Diensteanbieter im Binnenmarkt und enthält keine Regelung der Handlungen staatlicher Stellen zu Strafverfolgungszwecken.“*

Zudem enthalten die von der EU geschlossenen Fluggastdatensatzabkommen („PNR-Abkommen“) Datenschutzbestimmungen[95], denen die Behörden unterworfen sind, die diese Daten verarbeiten. Diese Schutzmaßnahmen

---

[92] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, geändert durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009.

[93] Insbesondere von den Artikeln 5, 6 und 9 der Richtlinie 2002/58/EG.

[94] EuGH, Verbundene Rechtssachen C-317/04 und C-318/04, Europäisches Parlament / Rat der Europäischen Union und Kommission der Europäischen Gemeinschaften, 30. Mai 2006.

[95] Seitens des Rats der Europäischen Union für angemessen erachtet, aber kritisiert seitens

wurden seitens des Rats der Europäischen Union für „angemessen“ erachtet[96], wohingegen die Artikel-29-Datenschutzgruppe und der Europäische Datenschutzbeauftragte sie für unzureichend befanden[97].

Dies alles zeigt: Wenn privatwirtschaftliche Unternehmen verpflichtet werden, zu Strafverfolgungszwecken Daten zu übermitteln, gilt weiterhin der allgemein Datenschutzrechtsrahmen – und zwar bis zum Abschluss der Datenübermittlung. Für Nachrichtendienste ist die Situation in vielen EU-Mitgliedstaaten anders, da sie nicht den allgemeinen Datenschutzrechtsvorschriften unterliegen.[98] Es liegt jedoch auf der Hand, dass auch für die Übermittlung von personenbezogenen Daten an Nachrichtendienste sowie für das Sammeln von personenbezogenen Daten durch Nachrichtendienste eine angemessene Rechtsgrundlage vorhanden sein muss.

4.4.2 Die Datenschutzgrundsätze in der Richtlinie 95/46/EG

Wenn eine Verarbeitungstätigkeit unter den Geltungsbereich der Richtlinie fällt, müssen die in Richtlinie niedergelegten Datenschutzgrundsätze sowie Rechte und Pflichten geachtet und eingehalten werden:

- Grundsätze hinsichtlich der Datenqualität: Gemäß Artikel 6 der Richtlinie müssen die für die Verarbeitung Verantwortlichen[99] sicherstellen, dass personenbezogene Daten a) nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden; b) für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden; c) den Zwecken entsprechen,

[96] Siehe beispielsweise Artikel 19 des geltenden EU-US-PNR-Abkommens (Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über die Verwendung von Fluggastdatensätzen und deren Übermittlung an das United States Department of Homeland Security, 2011).

[97] Siehe die Stellungnahmen des EDSB und der Artikel-29-Datenschutzgruppe zu den PNR-Abkommen, verfügbar unter www.edps.europa.eu bzw. unter http://ec.europa.eu/justice/data-protection/article-29.

[98] WP215 (andere Angaben oben), S. 9

[99] Artikel 6 Absatz 2 der Richtlinie.

für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen; d) sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind; und e) nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht[100].

• Kriterien für die Zulässigkeit der Verarbeitung personenbezogener Daten: In Artikel 7 ist niedergelegt, dass die Verarbeitung personenbezogener Daten lediglich erfolgen darf, wenn eine der folgenden Voraussetzungen erfüllt ist: a) Die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben; b) die Verarbeitung ist erforderlich für die Erfüllung eines Vertrags; c) die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt; d) die Verarbeitung ist erforderlich für die Wahrung lebenswichtiger Interessen der betroffenen Person; e) die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde; f) die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden (sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen).

• Sensible Daten: Artikel 8 enthält ein grundsätzliches Verbot der Verarbeitung so genannter besonderer Kategorien personenbezogener Daten (d. h. die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben), außer in ganz bestimmten Ausnahmefällen[101]. Zudem sind durch diesen Artikel zusätzliche Garantien für die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen, vorgeschrieben.

---

[100] Artikel 6 Absatz 1 der Richtlinie.

[101] Niedergelegt in Artikel 8 Absätze 2 und 3.

• Transparenz: In den Artikeln 10 und 11 ist festgelegt, welche Informationen die betroffene Person bei der Erhebung personenbezogener Daten bei der betroffenen Person bzw. für den Fall, dass die Daten nicht bei der betroffenen Person erhoben wurden, erhalten muss. Gemäß Artikel 18 sind die für die Verarbeitung Verantwortlichen auch verpflichtet, etwaige Verarbeitungsaktivitäten den Datenschutzbehörden zu melden[102]. Artikel 21 sieht die Veröffentlichung des Registers der gemeldeten Verarbeitungen vor.

• Rechte der betroffenen Person: In den Artikeln 12 und 14 sind das Auskunftsrecht, das Recht auf Berichtigung, Löschung oder Sperrung von Daten sowie das Widerspruchsrecht der betroffenen Person gegen die Verarbeitung niedergelegt.

• Automatisierte Einzelentscheidungen: In Artikel 15, der auf den Schutz der betroffenen Person vor bestimmten Profiling-Aktivitäten abzielt, ist das Recht niedergelegt, keiner für sie rechtliche Folgen nach sich ziehenden und keiner sie erheblich beeinträchtigenden Entscheidung unterworfen zu werden, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens.

• Vertraulichkeit und Sicherheit der Verarbeitung: In den Artikeln 16 und 17 sind die Pflichten der für die Verarbeitung Verantwortlichen oder der Auftragsverarbeiter zur Wahrung der Vertraulichkeit der Verarbeitung sowie zur Durchführung der geeigneten technischen und organisatorischen Maßnahmen für die Sicherheit der Verarbeitung festgelegt.

Mit der Richtlinie werden zudem die Aufsicht über die Einhaltung dieser Rechte und Pflichten durch unabhängige Datenschutzbehörden sowie Rechtsbehelfe und Rechtsmittel vorgeschrieben.

4.4.3 Ausnahmen von den Datenschutzgrundsätzen

Gemäß Artikel 13 Absatz 1 können die EU-Mitgliedstaaten Rechtsvorschriften erlassen, die die Pflichten und Rechte – d. h. die Grundsätze der Datenqualität, der Transparenz, des Auskunftsrechts, des Rechts auf Berichtigung, Löschung

[102] Siehe auch Artikel 19.

oder Sperrung – beschränken, sofern eine solche Beschränkung notwendig ist für a) 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.

Im Gegensatz zu den in Artikel 3 Absatz 2 niedergelegten allgemeinen Ausnahmen zum Anwendungsbereich der Richtlinie, liegt bei den Abweichungen von bestimmten Grundsätzen, Rechten und Pflichten, wie sie in Artikel 13 Absatz 1 oder in anderen Bestimmungen Richtlinie[103] enthalten sind, die Prämisse zugrunde, dass die Richtlinie für die betreffende Verarbeitung grundsätzlich gilt. Wie in der Richtlinie[104] ausdrücklich vorgeschrieben müssen derartige Ausnahmen dann in Rechtsvorschriften der Mitgliedstaaten niedergelegt werden, die in vielen Fällen zusätzliche Garantien[105] beinhalten müssen.

4.5 Die Datenschutzrichtlinie für die elektronische Kommunikation

Was die Anwendung der allgemeinen Datenschutzgrundsätze anbelangt, ist die Datenschutzrichtlinie für die elektronische Kommunikation eng an die Richtlinie 95/46/EG angebunden. Mit dieser Richtlinie werden zusätzliche Vorkehrungen, Maßnahmen und Garantien vorgeschrieben, die auf den Schutz der elektronischen Kommunikation abzielen. Der Geltungsbereich der Richtlinie ist jedoch auf die Anbieter von öffentlich zugänglichen elektronischen Kommunikationsdiensten begrenzt.

---

[103] *Ebenda.*

[104] Siehe beispielsweise Artikel 13 Absatz 1 sowie Artikel 13 Absatz 2, in denen festgelegt ist, dass ein Mitgliedstaat entsprechende Rechtsvorschriften erlassen muss.

[105] Siebe beispielsweise Artikel 13 Absatz 2.

Durch Artikel 5 Absatz 1 der Richtlinie 2002/58/EG wird die Vertraulichkeit der Kommunikation folgendermaßen geschützt: *„Die Mitgliedstaaten stellen die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicher. Insbesondere untersagen sie das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, dass diese Personen gemäß Artikel 15 Absatz 1 gesetzlich dazu ermächtigt sind.“*

Ein Szenario, bei dem die Anwendung von Artikel 5 Absatz 1 ausgelöst werden könnte, wurde seitens der Presse im Zusammenhang mit den Enthüllungen von Edward Snowden dargelegt: Angenommen, Nachrichtendienste erhalten durch ein Schlupfloch in den Sicherheitssystemen eines Anbieters von Kommunikationsdiensten, welcher der Datenschutzrichtlinie für elektronische Kommunikation unterliegt, (höchstwahrscheinlich unter vertraulicher Mitwirkung des Anbieters) Zugriff auf die Server dieses Anbieters. Im Extremfall dieses Szenarios hätten die Nachrichtendienste dann Zugriff auf sämtliche ein- und ausgehenden Daten dieses Servers[106] .

Man kann nun argumentieren, dass *durch Unterlassung des gesetzlichen Verbots* eines solchen Zugriffs (bzw. durch Unterlassung der wirksamen Aufsicht, die zu seiner Unterbindung erforderlich wäre) – 1.) die Mitgliedstaaten der ihnen durch die Datenschutzrichtlinie für elektronische Kommunikation auferlegten Pflicht zur Sicherstellung der Vertraulichkeit nicht nachkommen; und – 2.) die Anbieter von öffentlich zugänglichen elektronischen Kommunikationsdienste den mitgliedstaatlichen Rechtsvorschriften zur Umsetzung des in der Richtlinie festgelegten Vertraulichkeitsgrundsatzes nicht nachkommen.

Zudem sind durch die Artikel 6 und 9 der Datenschutzrichtlinie für elektronische Kommunikation die Verkehrsdaten und die Standortdaten (andere Standortdaten als Verkehrsdaten) geschützt und müssen sofort gelöscht oder anonymisiert werden, außer in spezifischen Fällen und unter

[106] Ähnliche Tatbestände im Belgacom-Fall führten zur Einleitung einer Untersuchung durch die belgische Datenschutzbehörde.

strikten Schutzmaßnahmen im besonderen Zusammenhang mit Rechnungsstellungs- oder Marketingzwecken.

Sonstige Formen der Verarbeitung oder Übermittlung von Kommunikationsdaten und zugehörigen Verkehrsdaten an Dritte sind daher nach der Datenschutzrichtlinie für elektronische Kommunikation gesetzwidrig, außer nach Artikel 15 Absatz 1. Gemäß dieser Bestimmung sind bei jeder Beschränkung des in den Artikeln 5 und 6 niedergelegten Vertraulichkeitsgrundsatzes strikte Bedingungen zu wahren, d. h. eine solche Beschränkung ist nur zulässig, sofern sie *„gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist.“*

Diese strikten Bedingungen sind unter Berücksichtigung des EuGH-Urteils von 2014 zur Vorratsdatenspeicherung auszulegen. In diesem Urteil heißt es nämlich, dass derartige Eingriffe einer genauen Eingrenzung durch Bestimmungen bedürfen, „die zu gewährleisten vermögen, dass sich der Eingriff tatsächlich auf das absolut Notwendige beschränkt.“[107] Der Zugang und Nutzung durch die zuständigen mitgliedstaatlichen Behörden sind hinsichtlich der Datenkategorien und der betroffenen Personen auf das absolut Notwendige zu beschränken sowie materiell- und verfahrensrechtlichen Bedingungen zu unterwerfen. Zudem müssen die mitgliedstaatlichen Rechtsvorschriften einen wirksamen Schutz angesichts der Gefahr eines rechtswidrigen Zugangs sowie sonstiger missbräuchlicher Nutzungen bieten, einschließlich der Anforderung, dass die Speicherung der Daten unter der Aufsicht einer unabhängigen Behörde erfolgen muss, welche die Einhaltung des EU-Datenschutzrechts sicherstellt.

Wie bereits dargelegt, sind Ausnahmen für Zwecke der nationalen Sicherheit innerhalb des EU-Rechtsrahmen zulässig, sofern es sich um die eigene nationale Sicherheit der betreffenden EU-Mitgliedstaaten handelt und sofern strikte Bedingungen eingehalten werden. Derartige Ausnahmen für Zwecke der nationalen Sicherheit sind jedoch keine zulässige Rechtfertigung für das

[107] Oben zitiert, Randnr. 65

Abfangen, für den Zugang oder für das Anfordern von personenbezogenen Daten seitens einer Behörde eines Drittlandes, auch wenn dies unter Berufung auf die nationale Sicherheit dieses Drittlandes erfolgt.

5. Regelung für die Datenübermittlung gemäß der Richtlinie 95/46/EG

Es ist noch immer nicht umfassend bekannt, wie die Überwachungsprogramme in aller Welt genau funktionieren. Möglicherweise werden noch weitere Fakten an die Öffentlichkeit gelangen, die uns zu einem deutlicheren Bild über diese Programme verhelfen. Man kann jedoch angemessener Sicherheit annehmen, dass die Überwachungsbehörden von Drittländern offenbar Zugang zu Daten erlangen, nachdem eine internationale Datenübermittlung von einem Unternehmen in der EU an ein anderes Unternehmen außerhalb der EU stattgefunden hat.

Derartige Datenübermittlungen müssen gemäß einem der in der Richtlinie 95/46/EG vorgesehenen Verfahren erfolgen, so dass die ausländische Stelle ihre entsprechenden Verpflichtungen einhalten muss, wenn sie aufgefordert wird, übermittelte Daten weiterzugeben oder Zugang zu übermittelten Daten zu gewähren. Deshalb ist es angebracht, die spezifischen Bestimmungen der für Datenübermittlungen vorgesehenen Verfahren zu analysieren, da diese Verfahren möglicherweise relevant sind, wenn eine Überwachungsbehörde eines Drittlandes sich Zugang zu Daten verschafft oder Daten anfordert, die ursprünglich aus der EU übermittelt worden sind.

Im vorliegenden Teil der Stellungnahme wird daher zunächst auf den bestehenden Rechtsrahmen für internationale Datenübermittlungen eingegangen, um dann die spezifischen Bestimmungen zu analysieren, die für verschiedene Szenarien gelten.

Die Richtlinie 95/46/EG enthält keinerlei Definition des Begriffs „Datenübermittlung“. Der Europäische Datenschutzbeauftragten meint zum Begriff der „Übermittlung personenbezogener Daten“: Es „kann zunächst einmal davon ausgegangen werden, dass der Begriff in seiner natürlichen Bedeutung verwendet wird und Daten bezeichnet, die sich zwischen

verschiedenen Verwendern ‘bewegen‘ oder ‘bewegen dürfen‘.“[108] Hinsichtlich der Verordnung (EG) Nr. 45/2001 führt der EDSB weiter aus: „Vor diesem Hintergrund […] sollten für die Verarbeitung Verantwortliche bedenken, dass dieser Begriff in der Regel die folgenden Elemente beinhaltet: Mitteilung, Weitergabe oder sonstige Bereitstellung personenbezogener Daten, vorgenommen mit dem Wissen oder in der Absicht eines der Verordnung unterworfenen Übermittlers, dass der/die Empfänger Zugriff darauf hat/haben. Der Begriff würde daher sowohl ‘beabsichtigte Übermittlungen‘ als auch den ‘zugelassenen Zugriff‘ auf die Daten durch den/die Empfänger abdecken“[109].

5.1 Angemessenes Schutzniveau

Wie jede Verarbeitung muss eine Datenübermittlung als erstes die oben genannten Grundsätze der Datenschutzrechtsvorschriften erfüllen. Ferner muss der Empfänger – gemäß Artikel 25 der Richtlinie – auch ein angemessenes Schutzniveau gewährleisten.

Artikel 25 Absatz 2: Angemessenheit des Schutzniveaus im Drittland, einschließlich Safe-Harbor-Abkommen: Gemäß Artikel 25 der Richtlinie 95/46/EG sind sämtliche Datenübermittlungen aus der Europäischen Union verboten, außer wenn ein Drittland ein angemessenes Schutzniveau gewährleistet. Wenn die Europäische Kommission einen Beschluss fast, mit dem anerkannt wird, dass das Drittland tatsächlich ein solches angemessenes Datenschutzniveau bietet, können Datenübermittlungen ohne weitere Einschränkungen erfolgen. In der Praxis bedeutet das, dass Datenübermittlungen in das betreffende Drittland genauso behandelt werden wie Datenübermittlungen in einen anderen EU-Mitgliedstaat.

So hat die Kommission beispielsweise bereits festgestellt, dass im Falle der Vereinigten Staaten das Safe-Harbor-Abkommen ein angemessenes Schutzniveau für gewerbliche Datenübermittlungen aus der Europäischen Union an US-Unternehmen gewährleistet, die diesem Programm beigetreten sind. Dieses Rechtsinstrument wurde jedoch nicht konzipiert, um ein

[108] Positionspapier des EDSB, Die Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen durch Organe und Einrichtungen der EU, 14. Juli 2014, S. 6.

[109] Ebenda, S. 7.

angemessenes Schutzniveau für Strafverfolgungszwecke zu gewährleisten, im Gegensatz zu anderen Abkommen, wie beispielsweise dem Abkommen zwischen der EU und den USA über die Verwendung und Übermittlung von Fluggastdatensätzen („PNR-Abkommen"), das den Rechtsrahmen für den Austausch von personenbezogenen Daten zwischen der EU und den USA für Strafverfolgungszwecke – darunter die Verhinderung und Bekämpfung von Terrorismus und anderen schweren Straftaten – bildet[110].

Artikel 26 Absatz 2: Standardvertragsklauseln (SCC – Standard Contractual Clauses) und Verbindliche unternehmensinterne Vorschriften (BCR – Binding Corporate Rules): Außer im Rahmen des Safe-Harbor-Abkommens können gemäß Artikel 26 Absatz 2 der Richtlinie Datenübermittlungen auch dann genehmigt werden, *„wenn der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet"*. Diese *„Garantien können sich insbesondere aus entsprechenden Vertragsklauseln ergeben"* (beispielsweise aus den Beschlüssen der Europäischen Kommission zu Standardvertragsklauseln zwischen einem für die Verarbeitung Verantwortlichen und einem weiteren für die Verarbeitung Verantwortlichen bzw. zwischen einem für die Verarbeitung Verantwortlichen und einem Auftragsverarbeiter). Zudem widmet sich die Datenschutzgruppe seit 2003 der Ausarbeitung von Verbindlichen unternehmensinternen Vorschriften (BCR – Binding Corporate Rules) für die Genehmigung von Datenübermittlungen innerhalb von Konzernen.

Artikel 26 Absatz 1: Abweichungen von den Regelungen zu Datenübermittlungen: Gemäß Artikel 26 Absatz 1 der Richtlinie ist eine Datenübermittlung in ein Drittland, das kein angemessenes Schutzniveau gewährleistet, nur möglich, wenn sie durch eine der in dem Artikel aufgelisteten Bedingungen begründet ist, beispielsweise wenn *„die Übermittlung entweder für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben ist"*.

[110] Diese Vereinbarungen wurden nach der Aufhebung des 2004 von der Kommission verabschiedeten Angemessenheitsbeschlusses ausgehandelt, um die Übermittlung dieser Daten zu ermöglichen.

Die Datenschutzgruppe hat bereits Leitlinien zur Anwendung der Artikel 25 und 26 der Richtlinie 95/46/EG ausgearbeitet und in einem Arbeitsdokument veröffentlicht: „Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU".[111] Im später veröffentlichten Arbeitsdokument der Datenschutzgruppe WP114 ist die Leitlinie enthalten, dass Ausnahmen vom allgemeinen Grundsatz restriktiv ausgelegt werden sollten, selbst wenn es um öffentliche Interessen geht[112]. Das gilt auch, wenn ausländische Behörden betroffen sind. Im Arbeitsdokument WP114 heißt es: *„Die Verfasser der Richtlinie hatten eindeutig ausschließlich wichtige öffentliche Interessen im Sinn, die in den innerstaatlichen Rechtsvorschriften für die in der EU niedergelassenen, für die Datenverarbeitung Verantwortlichen gelten."*[113]

Die Verwendung dieser Abweichungen hat zur Folge, dass die Daten nach erfolgter Übermittlung nicht mehr unter den Schutz gemäß der Richtlinie fallen. Deshalb sind sie laut Rechtsprechung des EGMR restriktiv auszulegen (siehe Abschnitt 3.2.1.3), und die Datenschutzgruppe empfiehlt, *„dass für die wiederholte, massenhafte oder routinemäßige Übermittlung personenbezogener Daten […] möglichst ein spezifischer Rechtsrahmen geschaffen wird (also Verträge oder verbindliche Unternehmensregelungen)"*.[114] Auf jeden Fall ist die Datenschutzgruppe der Auffassung, dass die Nutzung der Abweichung gemäß Artikel 26 Absatz 1 selbstverständlich niemals zu einer Situation führen darf, in der Grundrechte verletzt werden könnten.

---

[111] Artikel-29-Datenschutzgruppe, WP12, Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU, 24. Juli 1998.

[112] Artikel-29-Datenschutzgruppe, WP 114, Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995, 24. Oktober 1995, S. 7.

[113] Artikel-29-Datenschutzgruppe, WP 114, Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995, 24. Oktober 1995, S. 15.

[114] Artikel-29-Datenschutzgruppe, WP114, Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995, 24. Oktober 1995, S. 9.

5.2 Spezifische Rechtsinstrumente, die verwendet werden, um gemäß der Richtlinie 95/46/EG die Angemessenheit des Schutzniveaus zu belegen oder angemessene Schutzmaßnahmen zu erbringen

5.2.1 Das Safe-Harbor-Abkommen

Aufgrund des Kommissionsbeschlusses zum Safe-Harbor-Abkommen[115] gelten die Safe-Harbor-Grundsätze als angemessenes Schutzniveau im Sinne von Artikel 25 Absatz 2 der Richtlinie 95/46/EG. Daher kann die Beachtung und Einhaltung der Safe-Harbor-Grundsätze als Grundlage für Datenübermittlungen genutzt werden, und die Safe-Harbor-Grundsätze werden durch eine breite Palette von US-amerikanischen Unternehmen und Einrichtungen[116] genutzt, die sich einer entsprechenden Selbstzertifizierung unterzogen haben, um die Safe-Harbor-Grundsätze als Grundlage für Datenübermittlungen aus der EU nutzen zu können.

Was Weiterübermittlungen anbelangt, ist im Safe-Harbor-Abkommen niedergelegt, dass die Unternehmen und Einrichtungen bei der Weitergabe von Informationen an Dritte den Grundsatz der Benachrichtigung und der Wahlfreiheit einhalten müssen. Mit anderen Worten: Vor der Weitergabe von Daten an einen Dritten, der als für die Verarbeitung Verantwortlicher[117]

---

[115] Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (Bekannt gegeben unter Aktenzeichen K(2000) 2441).

[116] Der Geltungsbereich des Safe-Harbor-Abkommens ist begrenzt, so dass nicht alle Unternehmen und Einrichtungen beitreten können.

[117] Wenn das Unternehmen bzw. die Einrichtung eine Weiterübermittlung an eine Stelle durchführen möchte, die als Auftragsverarbeiter fungiert, ist keine Anwendung des Grundsatzes der Benachrichtigung und der Wahlfreiheit erforderlich. Das Unternehmen bzw. die Einrichtung muss sich jedoch vergewissern, dass der Dritte, der als Auftragsverarbeiter fungieren soll, entweder dem Safe-Harbor-Abkommen beigetreten ist, oder der Richtlinie unterliegt, oder dass ein entsprechender Beschluss der Kommission zur Angemessenheit des Schutzniveaus vorliegt, oder dass er eine schriftliche Vereinbarung eingeht, die mindestens das gleiche Schutzniveau gewährleistet wie nach dem Safe-Harbor-Abkommen vorgeschrieben. Es ist jedoch zu bedenken, dass im Falle der Überwachung der Nachrichtendienst eines Drittlandes ausschließlich als für die Verarbeitung Verantwortlicher eingestuft werden kann.

fungieren soll, muss das in den USA niedergelassene Unternehmen, das derzeit als für die Verarbeitung Verantwortlicher[118] fungiert, die betroffene Person über die beabsichtigte Weitergabe an den Dritten informieren und ihr die Möglichkeit einräumen, dieser Weitergabe zu widersprechen („opt out"), falls die Daten für einen Zweck verwendet werden sollen, der mit dem Zweck bzw. den Zwecken unvereinbar ist, für den/die die ursprüngliche Erfassung erfolgt ist.

Die Geltung der Safe-Harbor-Grundsätze kann begrenzt werden *„a) insoweit, als [...] Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss, b) durch Gesetzesrecht, staatliche Regulierungsvorschriften oder Fallrecht, die unvereinbare Verpflichtungen oder ausdrückliche Ermächtigungen schaffen, vorausgesetzt, die Organisation kann in Wahrnehmung dieser Ermächtigungen nachweisen, dass die Nichteinhaltung der Grundsätze sich auf das Ausmaß beschränkte, das die Einhaltung übergeordneter berechtigter Interessen aufgrund eben dieser Ermächtigung erforderte, [...] oder c) wenn die Richtlinie oder das nationale Recht Ausnahmeregelungen vorsieht, sofern diese Ausnahmeregelungen unter vergleichbaren Voraussetzungen getroffen werden."*[119]

Das durch das Safe-Harbor-Abkommen gewährleistete Schutzniveau wird in Zweifel gezogen, und zwar seit Beginn der Ausarbeitung des Texts. Insbesondere die Umsetzung des Safe-Harbor-Abkommens wird scharf kritisiert. In ihrer kürzlich veröffentlichten Mitteilung zum Funktionieren des Safe-Harbor-Abkommens geht die Europäische Kommission auf das Problem der Massenüberwachung im Zusammenhang mit dem Safe-Harbor-Programm ein und stellt fest, dass das große Ausmaß der US-amerikanischen Überwachungsprogramme möglicherweise darauf zurückzuführen sei, dass auf Daten, die im Rahmen des Safe-Harbor-Abkommens übermittelt werden, möglicherweise durch US-Behörden zugegriffen werden, die diese Daten weiterverarbeiten, wobei dieser Zugriff und diese Verarbeitung über das Maß hinausgehe, das im Sinne der im Safe-Harbor-Beschluss enthaltenen

[119] Diese Bestimmung wird näher erläutert in Anhang IV Abschnitt B der Safe-Harbor-Entscheidung: „Ausdrückliche rechtliche Ermächtigungen".

Ausnahme absolut notwendig und für den Schutz der nationalen Sicherheit verhältnismäßig sei.[120]

Zudem merkte die Kommission an, dass Unternehmen in ihren Datenschutzrichtlinien nicht systematisch angeben, ob sie Ausnahmen von den Safe-Harbor-Grundsätzen nutzen. Die betroffenen Privatpersonen und Unternehmen seien sich deshalb nicht darüber im Klaren, was mit ihren Daten geschieht.

Die Europäische Kommission gelangte zur Schlussfolgerung, dass aufgrund von Mängeln bei der Transparenz und bei der Durchsetzung des Abkommens nach wie vor spezifische Probleme bestehen, auf die eingegangen werden sollte:

a) Transparenz der Datenschutzrichtlinien von Safe-Harbor-Mitgliedern,

b) wirksame Anwendung von Datenschutzgrundsätzen durch Unternehmen in den USA; und

c) Wirksamkeit der Durchsetzung.

Ferner gebe es angesichts des großen Ausmaßes des Zugriffs seitens der Nachrichtendienste auf Daten, die

von Safe-Harbor-zertifizierten Unternehmen in die USA übermittelt werden, ernsthafte Fragen hinsichtlich der Kontinuität der Datenschutzrechte von Europäern, wenn ihre Daten in die USA übermittelt werden.[121]

Die Europäische Kommission formulierte 13 Empfehlungen, darunter die beiden folgenden, in denen es um den Zugriff von US-Behörden auf übermittelte Daten geht:

- Die Datenschutzrichtlinien von selbstzertifizierten Unternehmen sollten Informationen darüber enthalten, in welchem Ausmaß es den US-Behörden gemäß US-Recht gestattet ist, im Rahmen des Safe-Harbor-Abkommens übermittelte Daten zu sammeln und zu verarbeiten. Insbesondere

[120] COM(2013) 847 Communication from the Commission to the European Parliament and the Council on the functioning of the safe Harbor from the perspective of EU citizens and companies established in the EU (nur in englischer Sprache verfügbar), 27. November 2013, S. 17.
[121] Ebenda, S. 17-18.

sollten die Unternehmen aufgefordert werden, in ihren Datenschutzrichtlinien anzugeben, ob sie Ausnahmen von den Safe-Harbor-Grundsätzen nutzen, um Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung zu tragen.

- Es ist wichtig, dass die in der Safe-Harbor-Entscheidung vorgesehene Ausnahme für den Bereich der nationalen Sicherheit nur in einem Ausmaß verwendet wird, das strikt erforderlich und verhältnismäßig ist.

In einem Schreiben vom 10. April 2014[122] stellte sich die Datenschutzgruppe öffentlich hinter die Empfehlungen der Europäischen Kommission, einschließlich der Empfehlungen zum Zugriff von US-Behörden auf übermittelte Daten, und wies auf einige weitere Elemente in der Safe-Harbor-Entscheidung hin, die verbessert werden sollten. Die Verbesserungen am Safe-Harbor-Abkommen, die seitens der USA in den kommenden Monaten getroffen werden, müssen ausreichend sein, um das Vertrauen wiederherzustellen. Die Datenschutzgruppe teilt die Auffassung, dass das Safe-Harbor-Abkommen ausgesetzt werden sollte, falls der Überarbeitungsprozess, den die Europäische Kommission derzeit vorantreibt, zu keinem positiven Ergebnis führt. Auf jeden Fall ruft die Datenschutzgruppe in Erinnerung, dass die Datenschutzbehörden gemäß ihrer mitgliedstaatlichen Zuständigkeit und gemäß Unionsrecht Datenströme aussetzen können. Die Datenschutzgruppe sieht zudem gespannt dem Ausgang der Rechtssache Max Schrems entgegen, die kürzlich durch den Obersten Gerichtshof der Irischen Republik dem EuGH vorgelegt worden ist und in der es um die Rolle der Datenschutzbehörden hinsichtlich der Aussetzungen von Datenübermittlungen im Rahmen des Safe-Harbor-Abkommens geht[123].

---

[122] Schreiben der Artikel-29-Datenschutzgruppe an die Vizepräsidentin der Europäischen Kommission, Viviane Reding, zu den von der Europäischen Kommission vorgeschlagenen Maßnahmen zur Wiederherstellung des Vertrauens bei Datenströmen zwischen der EU und den USA.

http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf (zuletzt aufgerufen am 20. November 2014).

[123] Schrems / Data Protection Commissioner, C-362/14 (irisches Aktenzeichen 2013 Nr. 765JR: [2014] IEHC 351)

5.2.2 Standardvertragsklauseln (SCC – Standard Contractual Clauses)

Die SCC von 2001 und die SCC von 2004 umfassen eine Liste der Datenschutzgrundsätze, die bei jeder Verarbeitung von Daten – einschließlich der Datenübermittlung – einzuhalten sind. Diese Grundsätze sind unter anderem: der Zweckbindungsgrundsatz, der Transparenzgrundsatz, der Sicherheits- und Vertraulichkeitsgrundsatz, die Regeln für die Weiterübermittlung, das Recht auf Zugriff, Löschung und Widerspruch.

Gemäß den SCC von 2010 darf der außerhalb der EU niedergelassene Datenimporteur die personenbezogenen Daten nur im Auftrag des Datenexporteurs und entsprechend dessen Anweisungen verarbeiten. Da der in der EU niedergelassene Datenexporteur den Pflichten gemäß der Richtlinie unterliegt, müssen seine Anweisungen notwendigerweise den in der Richtlinie niedergelegten Datenschutzgrundsätzen entsprechen. Zudem ist es dem außerhalb der EU niedergelassenen Datenimporteur nicht gestattet, Daten zu übermitteln, außer wenn der in der EU niedergelassene Datenexporteur ihn dazu auffordert.

Die SCC enthalten zudem Regelungen zum Kollisionsrecht. So heißt es beispielsweise in den SCC von 2001 und in den SCC von 2004: *„Der Datenimporteur erklärt sich bereit und garantiert, dass […] er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen, und eine Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die die Klauseln bieten sollen, dem Datenexporteur mitteilen wird, sobald er von einer solchen Änderung Kenntnis erhält; unter diesen Umständen ist der Datenexporteur berechtigt, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten“*.

In den SCC von 2010 ist niedergelegt, dass der Datenimporteur sich verpflichtet, dass *„er die personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dessen Anweisungen und den vorliegenden Klauseln verarbeitet; dass er sich, falls er dies aus irgendwelchen Gründen nicht einhalten kann, bereit erklärt, den Datenexporteur unverzüglich davon in Kenntnis zu setzen, der unter diesen Umständen berechtigt ist, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten“*. Zudem ist in den SCC festgelegt, dass der Datenimporteur den Datenexporteur unverzüglich informiert über *„alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur*

Weitergabe der personenbezogenen Daten". Diese Benachrichtigungspflicht gilt allerdings nicht, wenn eine solche Benachrichtigung untersagt ist, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen.

Wie bereits festgestellt ist der massenhafte, unterschiedslose und geheime Zugriff auf personenbezogene Daten als unverhältnismäßig für den angestrebten Zweck zu betrachten. Dabei handelt es sich um den maßgeblichen Faktor für die Beurteilung der Rechtmäßigkeit der Verarbeitung. In diesem Kontext und unter Berücksichtigung der unlängst erfolgten Enthüllungen zu den US-amerikanischen Überwachungsprogrammen besteht möglicherweise Grund zur Annahme, dass die US-amerikanischen Rechtsvorschriften den Datenimporteur daran hindern, seinen Verpflichtungen aus dem Vertrag nachzukommen, so dass der Datenexporteur die Datenübermittlung aussetzen und/oder den Vertrag beenden könnte. Es obliegt dem für die Verarbeitung Verantwortlichen, den zukünftigen Status der Datenübermittlung zu beurteilen. Die gleiche Argumentation würde für jede ähnliche Situation in jedem anderen Drittland gelten.

Ferner enthalten sämtliche SCC Abweichungen in folgendem Sinn: Sie gelten vorbehaltlich der nach den nationalen Rechtsvorschriften für den Datenimporteur geltenden zwingenden Anforderungen, die nicht weitergehen, als es in einer demokratischen Gesellschaft unter Zugrundelegung der in Artikel 13 Absatz 1 der Richtlinie 95/46/EG[124] aufgeführten Interessen erforderlich ist; d. h. die Anforderungen müssen notwendig sein für die Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit, die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen oder den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen.[125]

[124] d. h. die Anforderungen müssen notwendig sein für die Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit, die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen oder den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen.

[125] Beschluss der Kommission 2010/87/EU vom 5. Februar 2010, Artikel 4.

5.2.3 Verbindliche unternehmensinterne Vorschriften (BCR – Binding Corporate Rules)

Gleichermaßen wie die SCC müssen die BCR für die für die Verarbeitung Verantwortlichen sowie die BCR für die Auftragsverarbeiter sämtliche Datenschutzgrundsätze enthalten, die bei der Verarbeitung von Daten zu achten sind, auch im Falle von Datenübermittlungen innerhalb eines Konzerns.[126]

- **BCR für die für die Verarbeitung Verantwortlichen**: Gemäß WP74 und WP153 müssen die BCR für die für die Verarbeitung Verantwortlichen eine eindeutige Verpflichtung enthalten, dass ein Unternehmen, das einem Konzern angehört, wenn es Grund/Gründe zur Annahme hat, dass es Rechtsvorschriften unterliegt, welche den Konzern als Ganzes daran hindern, seine Pflichten gemäß den BCR zu erfüllen, und dass dies wesentliche Auswirkungen auf die durch die BCR erzielten Garantien hat, die in der EU niedergelassene Konzernzentrale oder das in der EU niedergelassene Konzernunternehmen, dem die Zuständigkeiten für den Datenschutz übertragen sind, oder eine sonstige für den Datenschutz zuständige Stelle im Konzern unverzüglich informieren wird (außer wenn dies durch eine Strafverfolgungsbehörde untersagt ist, beispielsweise durch ein Verbot gemäß

[126] Siehe das Arbeitsdokument: „Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 26 Absatz 2 der EU-Datenschutzrichtlinie auf verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer“ (WP74), angenommen von der Artikel-29-Datenschutzgruppe am 29. Juni 2003, im Folgenden „WP74“; das Arbeitsdokument: „Einführung eines Prüfungskatalogs für einen Antrag auf Genehmigung verbindlicher unternehmensinterner Vorschriften“ (WP108), angenommen von der Artikel-29-Datenschutzgruppe am 3. Juni 2003, im Folgenden „WP108“; die „Empfehlung 1/2007 über das Antragsformular für die Genehmigung von verbindlichen unternehmensinternen Datenschutzregelungen zur Übermittlung personenbezogener Daten“ (WP133), angenommen von der Artikel-29-Datenschutzgruppe am 10. Januar 2007, im Folgenden „WP133“; das „Arbeitsdokument mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR)“ (WP153), angenommen von der Artikel-29-Datenschutzgruppe am 24. Juni 2008, im Folgenden „WP153“; das Arbeitsdokument „Rahmen für verbindliche unternehmensinterne Datenschutzregelungen (BCR)“ (WP154), angenommen von der Artikel-29-Datenschutzgruppe am 24. Juni 2008, im Folgenden „WP154“; das „Arbeitsdokument zu ‘Häufig gestellten Fragen‘ über verbindliche unternehmensinterne Datenschutzregelungen (BCR)“ (WP155), angenommen von der Artikel-29-Datenschutzgruppe am 24. Juni 2008, zuletzt überarbeitet und angenommen am 8. April 2009, im Folgenden „WP155“; das „Arbeitsdokument 02/2012 mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR) für Auftragsverarbeiter“. Alle genannten Dokumente sind auf der Website der Datenschutzgruppe verfügbar.

dem Strafrecht, um die Vertraulichkeit einer strafrechtlichen Untersuchung zu wahren).

Zudem müssen die BCR auch eine spezifische Verpflichtung enthalten, dass – falls der Datenempfänger einer obligatorischen Anforderung gemäß seinen nationalen Rechtsvorschriften unterliegt, die sich auf die anderen Unternehmen im Konzern auswirkt, d. h. falls ein Unterschied zwischen den betreffenden nationalen Rechtsvorschriften und den in den BCR niedergelegten Verpflichtungen besteht, die in der EU niedergelassene Konzernzentrale, oder das in der EU niedergelassene Unternehmen, dem die Zuständigkeiten für den Datenschutz übertragen sind, oder eine sonstige für den Datenschutz zuständige Stelle im Konzern eine verantwortungsvolle Entscheidung über die zu ergreifenden Schritte treffen und die zuständigen Datenschutzbehörden konsultieren wird. Ferner müssen sämtliche Vorfälle im Zusammenhang mit solchen Anforderungen genau dokumentiert und in regelmäßigen Prüfungen untersucht werden, wie in den BCR festgelegt.

BCR für Auftragsverarbeiter: In der Stellungnahme WP195 ist niedergelegt, jede rechtsverbindliche Aufforderung seitens einer Strafverfolgungsbehörde zur Weitergabe von personenbezogenen Daten dem für die Verarbeitung Verantwortlichen zu melden ist, außer wenn dies untersagt ist, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen. Auf jeden Fall sollte die Aufforderung ausgesetzt werden und die Datenschutzbehörde, die für den für die Verarbeitung Verantwortlichen zuständig ist, sowie die für die BCR maßgebliche Datenschutzbehörde sollten eindeutig darüber informiert werden. Jede Datenschutzbehörde ergreift Schritte gemäß ihrem geltenden mitgliedstaatlichen Recht und gemäß ihrer üblichen Praxis.

Ferner ist in der Stellungnahme WP195 festgelegt, dass die verschiedenen Mitglieder des Konzerns, in dem die BCR eingeführt werden, eine eindeutige Verpflichtung einzugehen haben, dass ein Konzernunternehmen, das den BCR unterliegt, – falls es Grund zur Annahme hat, dass die bestehenden oder zukünftigen Rechtsvorschriften, denen es unterliegt, es daran hindern könnten, den Anweisungen des für die Verarbeitung Verantwortlichen nachzukommen, oder seine Pflichten gemäß den BCR oder gemäß der Dienstleistungsvereinbarung zu erfüllen, – dies unverzüglich folgenden Stellen melden wird:

• den für die Verarbeitung Verantwortlichen; dieser darf die Datenübermittlung aussetzen und/oder vom Vertrag zurücktreten;

• den Auftragsverarbeiter der in der EU niedergelassenen Konzernzentrale oder das in der EU niedergelassene Konzernunternehmen, dem die Zuständigkeiten für den Datenschutz übertragen sind;

• oder den sonstigen zuständigen Datenschutzbeauftragten im Konzern bzw. die betreffenden Datenschutzstellen im Konzern; und

• auch die Datenschutzbehörde, die für den für die Verarbeitung Verantwortlichen zuständig ist.

5.3 Schlussfolgerung zu Datenübermittlungen

Der massenhafte, unterschiedslose und geheime Zugriff auf personenbezogene Daten, die ursprünglich unter der Hoheitsgewalt der EU verarbeitet worden sind und die dann aus der EU in ein Drittland übertragen worden sind, wo auf diese Daten dann für die Zwecke der Überwachungsprogramme dieses Drittlandes zugegriffen werden kann, stellt eine Verletzung der Anforderungen dar, die in der Richtlinie 95/46/EG für Datenübermittlungen niedergelegt sind. Routinemäßige (massenhafte) Datenübermittlungen durch für die Verarbeitung Verantwortliche, die der Hoheitsgewalt der EU unterliegen, unterliegen den EU-Rechtsvorschriften. Dies schließt die Weiterübermittlung an Dritte im Empfängerland ein. Eine solche Weiterübermittlung darf nur erfolgen, wenn die Bestimmungen der Richtlinie sowie der verschiedenen verfügbaren Rechtsinstrumente für Datenübermittlungen erfüllt sind. Es ist jedoch in keiner dieser Bestimmungen eine Datenübermittlung von personenbezogenen Daten, die sich in der Obhut von für die Verarbeitung Verantwortlichen in der Privatwirtschaft befinden, an Behörden von Drittländern zu Überwachungszwecken vorgesehen. Zudem war nie beabsichtigt, die genannten Rechtsinstrumente für Datenübermittlungen an Behörden zu verwenden, insbesondere nicht für die Übermittlung von Informationen im Zusammenhang mit den Aktivitäten von Strafverfolgungsbehörden[127].

[127] Da für Beurteilungen der Angemessenheit des Schutzniveaus eine Analyse der Anwendung der Rechtsstaatlichkeit in einem Drittland erforderlich ist, werden die Eigenschaften des öffentlichen Sektors dabei zumindest in einem gewissen Maß berücksichtigt. (Auch wenn man nicht realistisch erwarten kann, dass eine Beurteilung der Angemessenheit des Schutzniveaus

Deshalb müssen die Behörden von Drittländern – einschließlich der Strafverfolgungsbehörden und der Nachrichtendienste – wenn sie Zugriff auf Daten wünschen, die in einem EU-Mitgliedstaat gespeichert sind oder in anderer Weise der Hoheitsgewalt der EU unterliegen, Amtshilfe bei den zuständigen mitgliedstaatlichen Behörden über die bestehenden offiziellen Kanäle beantragen, beispielsweise über Rechtshilfeabkommen. In diesen Rechtsinstrumenten müssen die Datenschutzgrundsätze berücksichtigt werden.

In Ausnahmefällen können einzelne Übermittlungen auf der Grundlage der Abweichungen erfolgen, die in der Datenschutzrichtlinie (Artikel 13 sowie Artikel 26 Absatz 1) oder in den nationalen Rechtsvorschriften des Drittlandes niedergelegt sind, allerdings nur im Falle von Ländern, die anerkanntermaßen ein ausreichendes Schutzniveau im privaten Sektor aufweisen. Die oben erörterten Rechtsinstrumente (BCR, Safe-Harbor-Abkommen, SCC) enthalten ebenfalls Ausnahmen. Bei derartigen Ausnahmen handelt es sich jedoch um Einschränkungen eines Grundrechts, so dass sie restriktiv auszulegen sind. Sie dürfen nicht als Grundlage für massenhafte, routinemäßige oder wiederholte Datenübermittlungen herangezogen werden.

Auf jeden Fall darf der Zugriff seitens der Behörden eines Drittlandes auf übermittelte personenbezogene Daten zu Strafverfolgungszwecken – und erst recht zu Überwachungszwecken – nur einen begrenzten Umfang aufweisen. Die genannten Ausnahmen dürfen daher nicht die Grundlage für den Zugriff in einer unbegrenzten Anzahl von Fällen und/oder auf die Daten einer unbegrenzten Anzahl von Personen bilden, da dies dem Grundsatz der Verhältnismäßigkeit widerspricht, der die Grundlage der EU-Rechtsvorschriften bildet und in Artikel 8 EMRK niedergelegt ist.

Es sei auch in Erinnerung gerufen, dass die EU/US-Ad-hoc-Sachverständigengruppe zum Datenschutz in ihrem Bericht bestätigt hat, dass es zwar in den US-amerikanischen Rechtsvorschriften zahlreiche Grundlagen für das massenhafte Sammeln von personenbezogenen Daten geben mag, die bei US-amerikanischen Unternehmen gespeichert und verarbeitet werden, dass ein solches massenhaftes Sammeln aber eine Verletzung der Kriterien der Erforderlichkeit und der Verhältnismäßigkeit darstellt, wie sie in der

---

sich auf den gesamten öffentlichen Sektor eines Landes erstrecken kann.) Das ist einer der Gründe dafür, dass bei der Ausarbeitung der Rechtsinstrumente für Datenübermittlungen der öffentliche Sektor weniger stark berücksichtigt wurde.

Europäischen Menschenrechtskonvention niedergelegt sind. Ferner wird in dem Bericht bestätigt, dass der massenhafte Charakter dieser Programme wahrscheinlich zu einem Zugriff und zu einer Verarbeitung führt, die jenseits des strikt Notwendigen und Verhältnismäßigen liegen.

5.4 Beispiele

Im folgenden Kapitel werden – ausgehend von verschiedenen Szenarien – einige der verschiedenen Datenübermittlungen veranschaulicht, die möglicherweise stattfinden, im Prinzip ungeachtet des Drittlandes, das Ziel der Übermittlung ist.

Es liegt auf der Hand, dass im vorliegenden Arbeitsdokument nicht auf sämtliche denkbaren Szenarien eingegangen werden kann. Zudem ist der Rechtsrahmen zu den vielen verschiedenen Szenarien äußerst komplex. Um die Rechtmäßigkeit von Ersuchen seitens der Behörden von Drittländern um Rechtshilfe zu beurteilen sowie um sicherstellen zu können, dass der Datenempfänger ein ausreichendes Schutzniveau aufweist, ist es besonders wichtig, ob der für die Verarbeitung Verantwortliche dem EU-Datenschutzrecht unterliegt.[128] Hinsichtlich der Anwendbarkeit des EU-Datenschutzrechts ist jedoch nicht der Standort der Daten maßgeblich, sondern ob der für die Verarbeitung Verantwortliche eine Niederlassung in der EU hat oder Anlagen („Mittel“) in der EU verwendet und ob die Verarbeitung der Daten im Kontext der Aktivitäten dieser Niederlassung erfolgt. Hinsichtlich der Anwendbarkeit der Rechtsvorschriften von Drittländern, die das Sammeln von Daten gestatten, ist eine Reihe von Szenarien denkbar, bei denen es jeweils um Kollisionsrecht geht (d. h. um EU-Rechtsvorschriften und Rechtsvorschriften des betreffenden Drittlandes, die sich widersprechen), je nachdem wie weit dieses Drittland seine Hoheitsgewalt ausdehnt.

Die Antworten auf diese Fragen sind oftmals komplex, und möglicherweise sind auch noch weitere Aufdeckungen von Fakten und Präzisierungen von Rechtsvorschriften erforderlich, beispielsweise zur Bedeutung des Begriffs „Datenübermittlung“. Somit hat sich die Datenschutzgruppe entschieden, für die Zwecke des vorliegenden Arbeitsdokuments gewisse Vereinfachungen zu treffen.

[128] Siehe Richtlinie 95/46/EG, Artikel 4.

Beispiel 1: Eine direkte Datenübermittlung / ein direkter Datenzugriff von einer in der EU niedergelassenen privaten Einrichtung an eine Behörde außerhalb der EU

Die Datenschutzgruppe ruft als erstes in Erinnerung, dass das internationale Recht und das nationale Recht auf diese Szenarien umfassend anwendbar ist[129]. Bei direkten Übermittlungen von personenbezogenen Daten durch eine private Einrichtung aus der EU an eine Behörde eines Drittlandes oder bei direkten Zugriffen seitens einer Behörde eines Drittlandes auf derartige personenbezogene Daten müssen die genannten Rechtsordnungen geachtet werden.

In ihrem Schreiben vom 5. Dezember 2013 an den Cyberkriminalitätsausschuss des Europarats[130] hat die Datenschutzgruppe nachdrücklich darauf hingewiesen, dass das Verfahren, das gemäß Artikel 32 Buchstabe b der Budapester Konvention über Cyberkriminalität[131] vorgesehen

---

[129] Siehe insbesondere die Artikel 2 Absatz 1 und 2 Absatz 4 der Charta der Vereinten Nationen.

[130] Ref. Ares(2013)3645289 – 5. Dezember 2013, Schreiben der Artikel-29-Datenschutzgruppe an die Abteilung „Cyberkriminalität" des Europarats.

Betreff: Anmerkungen der Artikel-29-Datenschutzgruppe zum Problem des direkten Zugriffs der Strafverfolgungsbehörden von Drittländern auf Daten, die im Hoheitsgebiet eines anderen Staates gespeichert sind, wie im Entwurf zu einem Zusatzprotokoll zur Budapest Konvention über Cyberkriminalität vorgeschlagen (nur in englischer Sprache verfügbar) http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf

[131] Artikel 32 – Grenzübergreifender Zugriff auf gespeicherte Computerdaten ohne Einwilligung oder falls öffentlich verfügbar

„Ein Vertragsstaat darf – ohne Genehmigung eines anderen Vertragsstaats:

a) auf öffentlich verfügbare gespeicherte Computerdaten („Open-Source-Daten") zugreifen, ungeachtet des Standorts der Daten; oder

b) über ein auf seinem Hoheitsgebiet befindliches Computersystem auf gespeicherte Computerdaten zugreifen oder gespeicherte Computerdaten empfangen, die ihren Standort in einem anderen Vertragsstaat haben, wenn der Vertragsstaat die rechtmäßige und freiwillige Zustimmung der Person einholt, welche die gesetzliche Befugnis zur Weitergabe der

ist, beinhaltet, dass der Zugriff auf oder die Spiegelung von Computerdaten, die in einem anderen Vertragsstaat gespeichert sind, nur mit der rechtmäßigen und freiwilligen Zustimmung der Person erfolgen darf, welche die gesetzliche Befugnis zur Weitergabe der betreffenden Daten an den betreffenden Vertragsstaat über das betreffende Computersystem hat, d. h. dass es sich um einen ordnungsgemäßen Datenaustausch zwischen Strafverfolgungs- oder Justizbehörden in einem bestimmten Fall handeln muss.

Die Datenschutzgruppe betont in ihrem Schreiben ferner, dass *„gemäß dem EU-Datenschutz-Besitzstand*[132] *Unternehmen, die als für die Verarbeitung Verantwortliche fungieren in der Regel nicht über die gesetzliche Befugnis zur Weitergabe der von ihnen verarbeiteten Daten – etwa zu gewerblichen Zwecken – verfügen. Normalerweise dürfen solche Unternehmen Daten nur weitergeben, wenn zuvor durch eine nationale Strafverfolgungsbehörde eine richterliche Genehmigung/Anordnung bzw. ein sonstiges Dokument zur Begründung der Notwendigkeit des Zugriffs auf die Daten unter Nennung der einschlägigen Rechtsgrundlage für den Zugriff, gemäß den innerstaatlichen Rechtsvorschriften und unter Angabe des Zwecks, für den die Daten benötigt werden, vorgelegt worden ist. Ein für die Verarbeitung Verantwortlicher kann keinen rechtmäßigen Zugriff für – bzw. keine Weitergabe an – ausländische Strafverfolgungsbehörden gewähren, die hinsichtlich des Datenschutzes und hinsichtlich der strafrechtlichen Verfahren unter einem anderen Rechts- und Verfahrensrahmen arbeiten.“*[133] [nur in englischer Sprache verfügbar; inoffizielle Übersetzung für die Zwecke des vorliegenden Arbeitsdokuments]

Die Artikel-29-Datenschutzgruppe betont ferner, dass bei diesen Szenarien – sofern sie stattfinden – möglicherweise weitere schwerwiegende Grundrechtsaspekte berührt sind, beispielsweise hinsichtlich der rechtsstaatlichen Garantien in Strafverfahren, und dass ein solches Vorgehen in manchen Mitgliedstaaten sogar als Straftat eingestuft wird. So stellt ein derartiges Vorgehen beispielsweise in Frankreich und Deutschland eine

---

betreffenden Daten an den betreffenden Vertragsstaat über das betreffende Computersystem hat.“ [inoffizielle Übersetzung für die Zwecke des vorliegenden Arbeitsdokuments]

[132] Siehe insbesondere die Artikel 25 und 26 der Richtlinie 95/46/EG, zu Datenübermittlungen in Drittländer.

[133] Siehe das oben genannte Schreiben, S. 3.

Verletzung des im jeweiligen mitgliedstaatlichen Recht niedergelegten Fernmeldegeheimnisses[134] dar.

[134] So heißt es beispielsweise im deutschen Strafgesetzbuch (StGB) § 206 „Verletzung des Post- oder Fernmeldegeheimnisses“:
(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt

1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,

2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder

3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) Die Absätze 1 und 2 gelten auch für Personen, die

1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen,

2. von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder

3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigem Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Post- oder Fernmeldegeheimnis bekanntgeworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(5) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

Beispiel 2: Eine Datenübermittlung von einer in der EU niedergelassenen privaten Einrichtung an eine private Einrichtung, die nicht der Hoheitsgewalt der EU untersteht

In diesem Szenario betreffen die Zugriffsersuchen seitens einer Behörde eines Drittlandes Daten, die ursprünglich aus der EU übermittelt worden sind und die nun in diesem Drittland gespeichert sind. Dabei hat zwangsläufig zuvor eine Datenübermittlung von einem in der EU niedergelassenen Datenexporteur an einen nicht in der EU niedergelassenen Datenimporteur zu gewerblichen Zwecken stattgefunden.

a) Datenübermittlungen in Länder, die anerkanntermaßen ein angemessenes Schutzniveau aufweisen, oder im Rahmen von angemessenen Schutzmaßnahmen

Die ursprüngliche Datenübermittlung zu einem gewerblichen Zweck muss im Einklang mit dem Artikel 25 oder mit dem Artikel 26 Absatz 2 Richtlinie 95/46/EG stattfinden, und die betroffenen Personen müssen über die Datenübermittlung sowie über die Eigenschaften dieser Datenübermittlung informiert werden, beispielsweise über das Ziel der Datenübermittlung (Datenempfänger), über den Zweck sowie über die Rechte der betroffenen

---

Auch im französischen Recht steht die Verletzung von Nachrichten, die per Telekommunikation gesendet, übermittelt oder empfangen werden gemäß **Artikel 226 Absatz 15 des Strafgesetzbuchs der Französischen Republik** unter Strafe, und die Weitergabe von gewerblichen, industriellen, technischen oder finanziellen Daten an ausländische juristische oder natürliche Personen wird geregelt durch das Gesetz Nr.°**68-678 vom 26. Juli 1968.**

Siehe insbesondere Artikel 226 Absatz 15 des Strafgesetzbuchs der Französischen Republik:

Wer böswillig an einen Dritten gerichtete Korrespondenz öffnet, zerstört, zurückhält oder fehlleitet – ungeachtet ob die Korrespondenz ihr Ziel schließlich erreicht – oder wer sich auf betrügerischem Wege Kenntnis von ihrem Inhalt verschafft, wird mit einem Jahr Gefängnis und einer Geldbuße von 45 000 EUR bestraft. Die gleiche Strafe gilt für das böswillige Abfangen, Fehlleiten, Nutzen oder Weitergeben von Korrespondenz, die per Telekommunikation gesendet, übermittelt oder empfangen wird, oder für das Einrichten eines Geräts, das derartige Abfangoperationen durchführen soll. [inoffizielle Übersetzung für die Zwecke des vorliegenden Arbeitsdokuments] – Siehe auch das Gesetz Nr. 68-678 vom 26. Juli 1968 zur Weitergabe von wirtschaftlichen, gewerblichen, industriellen, finanziellen oder technischen Dokumenten an ausländische natürliche und juristische Personen, geändert durch das französische Gesetz Nr. 80-538 vom 16. Juli 1980.

Person, wie in Artikel 10 Richtlinie niedergelegt. Sämtliche sonstigen Datenschutzgrundsätze, Rechte der betroffenen Personen und Pflichten sind ebenfalls zu achten. Die Einhaltung dieser Bestimmungen ist verpflichtend, ungeachtet ob der in der EU niedergelassene Datenexporteur eine gänzlich verschiedene Einrichtung von dem nicht in der EU niedergelassenen Datenimporteur ist oder ob es sich um ein Tochterunternehmen handelt.

Ferner muss jeder Zugriff auf diese personenbezogenen Daten durch Behörden eines Drittlandes sowie die Weitergabe von personenbezogenen Daten an derartige Behörden im Einklang mit den EU-Datenschutzgrundsätzen, mit den in der Richtlinie 95/46/EG niedergelegten Regeln für die Weiterübermittlung sowie mit den Rechtsinstrumenten erfolgen, die als Grundlage zum Erzielen angemessener Schutzmaßnahmen verwendet werden (beispielsweise Standardvertragsklauseln (SSC), Safe-Harbor-Abkommen oder Verbindliche unternehmensinterne Vorschriften (BCR)).

Die in den oben erörterten Rechtsinstrumenten für Datenübermittlungen niedergelegten Abweichungen sind nicht so weit gefasst, dass dadurch eine massenhafte, unterschiedslose und heimliche Überwachung gerechtfertigt werden könnte, die das in Artikel 13 und Artikel 26 Absatz 1 Richtlinie niedergelegte Ausmaß überschreitet. Vielmehr gilt:

a. der Zugang muss auf das absolut Notwendige beschränkt sein; und

b. der Zweck muss beschränkt sein auf die Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit, die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen oder den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen; und

c. gemäß dem EU-Rechtsrahmen sowie gemäß der Rechtsprechung des EGMR und des EuGH müssen Einschränkungen eng ausgelegt werden und müssen die Kriterien der Notwendigkeit und der Verhältnismäßigkeit erfüllen.

Ferner ist zu bedenken: Selbst wenn die Kriterien für eine Abweichung aus Gründen der nationalen Sicherheit erfüllt sein sollten, sind die genannten Rechtsinstrumente für die Datenübermittlung nicht so gestaltet, dass sie nachgewiesene angemessene Garantien dafür bieten würden, dass die Nachrichten- oder Geheimdienste eines Drittlandes ein angemessenes Schutzniveaus für die betroffenen Personen bieten würden.

b) Datenübermittlung auf der Grundlage der in Artikel 26 Absatz 1 der Richtlinie vorgesehenen Ausnahmen

In Ausnahmefällen kann eine Datenübermittlung von einer in der EU niedergelassenen privaten Einrichtung an eine außerhalb der EU niedergelassene private Einrichtung mit den in Artikel 26 Absatz 1 der Richtlinie vorgesehenen Ausnahmen gerechtfertigt werden. Diese Ausnahmen bilden jedoch keine statthafte Grundlage für massenhafte, routinemäßige oder wiederholte Datenübermittlungen, und dürfen nicht zur Verletzung von Grundrechten führen.

Bei der massenhaften, geheimen und unterschiedslosen Überwachung von personenbezogenen Daten wird gegen die Anforderung eines angemessenen Schutzniveaus hinsichtlich der in der Richtlinie 95/46/EG niedergelegten Grundsätze und hinsichtlich der Bedingungen des Rechtsinstruments verstoßen, das als Grundlage für die Datenübermittlung gewählt worden ist. Die Beurteilung, ob eine Weiterübermittlung im Einklang mit den in der Richtlinie niedergelegten Grundsätzen und mit dem als Grundlage für die Datenübermittlung verwendeten Rechtsinstrument steht, fällt auf jeden Fall negativ aus, sobald man es mit einer massenhafte, unterschiedslosen, geheimen und routinemäßigen Überwachung von personenbezogenen Daten zu tun hat. Faktisch können derartige Aktivitäten unter keinen Umständen als im Einklang mit bestimmten Datenschutzgrundsätzen betrachtet werden (unvereinbare Zwecke, unverhältnismäßiger Zugriff, mangelnde Transparenz, keine Auskunfts- bzw. Zugriffsmöglichkeit für die betroffene Person, keine Widerspruchsmöglichkeit für die betroffene Person gegen die Verarbeitung sowie keine angemessenen Rechtsmittel).

Beispiel 3: Datenübermittlung von einer Niederlassung in der EU an eine Niederlassung außerhalb der EU, die der Hoheitsgewalt der EU untersteht (Niederlassung oder Mittel der Datenverarbeitung befinden sich in der EU)

Bei diesem Szenario liegt im Wesentlichen die gleiche Struktur der Datenübermittlung wie im vorhergehenden Szenario vor, mit dem Unterschied, dass die außerhalb der EU niedergelassene private Einrichtung der Hoheitsgewalt der EU unterliegt, entweder weil es sich bei der in der EU

niedergelassenen Einrichtung um eine Niederlassung im Sinne von Artikel 4 Absatz 1 Buchstabe a Richtlinie handelt oder weil die außerhalb der EU niedergelassene private Einrichtung in der EU befindliche Anlagen („Mittel“) zur Datenverarbeitung im Sinne von Artikel 4 Absatz 1 Buchstabe c verwendet.

Folglich muss die außerhalb der EU niedergelassene private Einrichtung das Unionsrecht einhalten, so dass die Sachverhalte des Kollisionsrechts hier noch deutlicher hervortreten als im vorhergehenden Szenario.

In diesem Szenario gilt daher die gleiche rechtliche Argumentation:

- die gemäß Artikel 13 Richtlinie zulässigen Ausnahmen sind nicht so weit gefasst, dass dadurch eine systematische und unverhältnismäßige Überwachung in großem Ausmaß gerechtfertigt werden könnte,

- bisher sind die genannten Rechtsinstrumente für die Datenübermittlung nicht so gestaltet, dass sie nachgewiesene angemessene Garantien dafür bieten würden, dass die Nachrichten- oder Geheimdienste eines Drittlandes ein angemessenes Schutzniveaus für die betroffenen Personen bieten würden.

6. Anmerkungen zu möglichen Optionen für die Zukunft

Wie in der Einleitung dargelegt, soll mit diesem Arbeitsdokument ein Beitrag zur dringend erforderlichen Diskussion über den Geltungsbereich und die Grenzen des Grundrechts auf Datenschutz angesichts von Überwachung geleistet werden. Wie in den vorhergehenden Kapiteln aufgezeigt, sind nach Auffassung der Datenschutzgruppe bestimmte Bereiche der Datenschutzrechtsvorschriften auch dann auf die für die Verarbeitung Verantwortlichen und auf die Auftragsverarbeiter anwendbar, wenn diese Stellen mit Nachrichtendiensten zu tun haben. Dieses Fortgelten der Grundrechte auch im Umgang mit Nachrichtendiensten ist dringend geboten: Im Sinne der Rechtsstaatlichkeit und aufgrund der einschlägigen Rechtsprechung ist es nämlich unbedingt erforderlich, Einschränkungen von Grundrechten auf das unbedingt Notwendige und Verhältnismäßige zu begrenzen, spezifisch zu formulieren und in Form von Rechtsvorschriften niederzulegen.

6.1 Reform des Datenschutzes

Es gibt nur zwei Akteure, die im Kontext von Überwachung und nationaler Sicherheit für wirkliche Rechtssicherheit sorgen können: die Gerichte und der Gesetzgeber. Angesichts der laufenden Reform des Datenschutzes in der EU steht derzeit ein einzigartiges Zeitfenster offen, um die Situationen abzugrenzen, in denen die Datenschutzregelungen gelten sollen, auch bei der Datenübermittlung an Strafverfolgungsbehörden und Nachrichtendienste.

6.1.1 Der vorgeschlagene neue Artikel 43a

Der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlaments hat den Vorschlag der Kommission für eine Allgemeine Datenschutzverordnung um einen neuen Artikel 43a ergänzt. Dieser Artikel 43a beruht auf Artikel 42 des ursprünglichen Entwurfs des Kommissionsvorschlags[135], der aus dem vom Kommissionskollegium schließlich verabschiedeten endgültigen Vorschlag gestrichen wurde, so dass der endgültige Vorschlag lediglich einen entsprechenden Erwägungsgrund 90 enthielt.

Dieser Artikel bezieht sich auf Datenübermittlungen oder Weitergaben, die nicht im Einklang mit dem Unionsrecht stehen. Darin wird in Erinnerung gerufen, dass die Weitergabe von personenbezogenen Daten an irgendeine Behörde eine Drittlandes (Gericht, Verwaltungsgericht usw.) erst stattfinden darf, nachdem das Ersuchen der Aufsichtsbehörde gemeldet worden ist und nachdem die Aufsichtsbehörde ihre Genehmigung dazu erteilt hat, unbeschadet eine geltenden Rechtshilfeabkommen oder eines geltenden internationalen Abkommens zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat.

In dem Artikel ist ferner festgelegt, dass die seitens der Aufsichtsbehörde erteilte Genehmigung auf einer Beurteilung beruhen muss, ob das Ersuchen im Einklang mit der Allgemeinen Datenschutzverordnung steht, und dass die zuständige mitgliedstaatliche Strafverfolgungsbehörde über das Ersuchen zu informieren ist. Bis zu einem gewissen Grade wird auch eine Information der betroffenen Personen über die Weitergabe vorgeschrieben.

[135] Ans Licht der Öffentlichkeit gebracht durch statewatch.org.

In dieser Hinsicht verweist die Datenschutzgruppe auf ihre Stellungnahme zur Abstimmung vom 21. Oktober 2013 im LIBE-Ausschuss des Europäischen Parlaments. Insbesondere begrüßte die Datenschutzgruppe dort in ihren Anmerkungen zum Zugriff seitens der Behörden sowie zu Datenübermittlungen in Drittländer, dass die betroffenen Personen obligatorisch informiert werden sollen, wenn eine Behörde Zugang zu Daten erhalten hat. Zudem forderte die Datenschutzgruppe in der genannten Stellungnahme nachdrücklich einen robusten und soliden Datenschutzrechtsrahmen und begrüßte die Verwendung von Rechtshilfeabkommen oder internationalen Abkommen in Fällen von Weitergaben, die nach Unionsrecht bzw. nach dem Recht von Mitgliedstaaten nicht zulässig sind. Abschließend erklärte sie, dass bei Ersuchen seitens der Behörden von Drittländern auf Datenzugriff, die zuständige Aufsichtsbehörde nicht die Datenschutzbehörde sein sollte, sondern die Behörde des EU-Mitgliedstaats, die das Ersuchen bearbeitet.

6.2 Offene rechtliche Fragen

Manche Elemente des vorgeschlagenen Artikels 43a mögen ein Schritt in die richtige Richtung sein, doch er wird sich nicht als *deus ex machina* erweisen, der alle übrigen Fragen löst. Die Analysen im vorliegenden Arbeitsdokument haben aufgezeigt, dass grundlegende rechtliche Fragen nach wie vor offen sind, darunter die Definition der zentralen Begriffe „nationale Sicherheit“ und „Datenübermittlung“. Es steht daher eine schwierige Diskussion an, um praktikable Lösungen für diese grundlegenden Probleme zu finden: eine Diskussion auf europäischer und auf weltweiter Ebene, unter Einbindung aller Interessenträger. Nach Auffassung der Datenschutzgruppe müssen in unserer globalisierten Zeit – mit unbegrenzten Datenströmen zwischen den Ländern und in die „Cloud“ – neue Lösungen gefunden werden. Durch diese Lösungen muss gewährleistet sein, dass wir als Gesellschaft auch weiterhin die Grundrechte der Bürger schützen können, während wir zugleich für ein sicheres Lebensumfeld sorgen.