ARTIKEL-29-DATENSCHUTZGRUPPE

819/14/DE
WP 215

Stellungnahme 04/2014 zur Überwachung der elektronischen Kommunikation zu nachrichtendienstlichen und nationalen Sicherheitszwecken

Angenommen am 10. April 2014

Zusammenfassung

Seit dem Sommer 2013 wird in verschiedenen internationalen Medien in großem Maßstab vor allem basierend auf von Edward Snowden bereitgestellten Dokumenten über die Überwachungstätigkeiten von Nachrichtendiensten in den USA und in der Europäischen Union berichtet. Die Enthüllungen haben eine weltweite Debatte über die Auswirkungen einer solch flächendeckenden Überwachung auf die Privatsphäre der Bürger entfacht. Die Art und Weise, in der sich Nachrichtendienste unserer täglichen Kommunikationsdaten sowie der Inhalte dieser Kommunikation bedienen, führt eindringlich vor Augen, dass der Überwachung Grenzen gesetzt werden müssen.

Das Recht auf Privatsphäre und auf Schutz der personenbezogenen Daten ist ein Grundrecht, das im Internationalen Pakt über bürgerliche und politische Rechte, in der Europäischen Menschenrechtskonvention und in der Charta der Grundrechte der Europäischen Union verankert ist. Die Einhaltung des Rechtsstaatsprinzips setzt deshalb zwingend voraus, dass dieses Recht in höchstmöglichem Maße geschützt wird.

Anhand ihrer Analyse kommt die Datenschutzgruppe zu dem Schluss, dass geheime, massive und willkürliche Überwachungsprogramme mit unseren grundlegenden Gesetzen unvereinbar sind und nicht mit der Bekämpfung des Terrorismus oder anderen größeren Bedrohungen der nationalen Sicherheit gerechtfertigt werden können. Die Beschränkung der Grundrechte aller Bürger ist nur hinnehmbar, wenn diese Maßnahme in einer demokratischen Gesellschaft unbedingt notwendig und verhältnismäßig ist.

Die Datenschutzgruppe empfiehlt daher verschiedene Maßnahmen zur Gewährleistung und Einhaltung der Rechtsstaatlichkeit.

Erstens fordert die Datenschutzgruppe mehr Transparenz in Bezug auf die Funktionsweise der Überwachungsprogramme. Transparenz trägt zur Wiederherstellung und Verbesserung des Vertrauensverhältnisses zwischen den Bürgern, Regierungen und privaten Einrichtungen bei. Dazu gehört, dass Einzelpersonen darüber in Kenntnis gesetzt werden, wenn Nachrichtendiensten Zugang zu Daten gewährt wurde. Um die Bürger besser über die Auswirkungen der Nutzung elektronischer Online- und Offline-Kommunikationsdienste und die Möglichkeiten, sich selbst besser zu schützen, zu informieren, möchte die Datenschutzgruppe im zweiten Halbjahr 2014 eine Konferenz zum Thema Überwachung mit allen relevanten Akteuren abhalten.

Darüber hinaus spricht sich die Datenschutzgruppe nachdrücklich für eine wirksamere Beaufsichtigung der Überwachungstätigkeiten aus. Da die wirksame und unabhängige Aufsicht über die Nachrichtendienste, einschließlich der Verarbeitung personenbezogener Daten, eine Voraussetzung ist, um den Missbrauch dieser Programme zu verhindern, vertritt die Datenschutzgruppe die Ansicht, dass die Datenschutzbehörden unbedingt darin einbezogen werden müssen.

Des Weiteren empfiehlt die Datenschutzgruppe die Durchsetzung der bestehenden Verpflichtungen der EU-Mitgliedstaaten und der Vertragsparteien der Europäischen Menschenrechtskonvention (EMRK) zum Schutz des Rechts auf Achtung der Privatsphäre

und der personenbezogenen Daten. Ferner erinnert die Datenschutzgruppe daran, dass den EU-Rechtsvorschriften unterliegende Datenverarbeiter die anwendbaren EU-Datenschutzvorschriften einhalten müssen. Sie verweist zudem darauf, dass Datenschutzbehörden die Datenübermittlung aussetzen können und gegebenenfalls entsprechend ihrer einzelstaatlichen Zuständigkeit Sanktionen verhängen sollten.

Weder die Grundsätze des „sicheren Hafens“ noch Standardvertragsklauseln oder unternehmensinterne Datenschutzregelungen können als Rechtsgrundlage herangezogen werden, um die Übermittlung personenbezogener Daten an eine Drittstaatsbehörde zum Zwecke massiver und willkürlicher Überwachung zu rechtfertigen. Die in diesen Instrumenten enthaltenen Ausnahmeregelungen haben nämlich einen beschränkten Anwendungsbereich und sollten eng ausgelegt werden. Unter keinen Umständen sollten sie so umgesetzt werden, dass das durch die EU-Vorschriften und -Instrumente für die Datenübermittlung garantierte Schutzniveau beeinträchtigt wird.

Die Datenschutzgruppe fordert die EU-Organe auf, die Verhandlungen über das Datenschutz-Reformpaket zum Abschluss zu bringen. Sie begrüßt insbesondere den Vorschlag des Europäischen Parlaments für einen neuen Artikel 43a, der die Verpflichtung auferlegt, Personen zu informieren, wenn einer Behörde innerhalb der letzten zwölf Monate Zugriff auf Daten gewährt wurde. Durch Transparenz bei diesen Vorgehensweisen wird das Vertrauen enorm gestärkt.

Darüber hinaus ist die Datenschutzgruppe der Ansicht, dass der Anwendungsbereich der Ausnahmen aus Gründen der nationalen Sicherheit präzisiert werden sollte, um Rechtssicherheit hinsichtlich des Geltungsbereichs des EU-Rechts zu schaffen. Bislang hat der europäische Gesetzgeber weder eine klare Definition des Begriffs „nationale Sicherheit“ vorgenommen, noch gibt es diesbezüglich eine schlüssige Rechtsprechung der europäischen Gerichte.

Abschließend empfiehlt die Datenschutzgruppe die unverzügliche Einleitung von Verhandlungen über ein internationales Abkommen, um Personen bei der Durchführung nachrichtendienstlicher Tätigkeiten angemessene Datenschutzgarantien zu gewähren. Die Datenschutzgruppe unterstützt zudem die Entwicklung eines weltweiten Instruments, das durchsetzbare hohe Grundsätze für den Schutz der Privatsphäre und den Datenschutz vorschreibt.

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGNER DATEN,

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,

gestützt auf Artikel 29 und auf Artikel 30 Absatz 1 Buchstabe c und Absatz 3 dieser Richtlinie,

gestützt auf ihre Geschäftsordnung und insbesondere Artikel 12 und 14,

HAT DIESE STELLUNGNAHME ANGENOMMEN:

1. Einleitung

Seit dem Sommer 2013 wird in verschiedenen internationalen Medien viel über die elektronischen Überwachungstätigkeiten von Nachrichtendiensten in den USA, in der Europäischen Union (EU) und in der übrigen Welt berichtet, wobei diese Berichte in erster Linie auf den von Edward Snowden zur Verfügung gestellten Dokumenten basieren. Die Enthüllungen haben eine weltweite Debatte über die Auswirkungen einer solch flächendeckenden elektronischen Überwachung auf die Privatsphäre der Bürger entfacht. So wurde auch die Frage aufgeworfen, inwieweit es Nachrichtendiensten gesetzlich erlaubt sein sollte, unseren Alltag betreffende Informationen zu sammeln und zu verwenden. Diese Stellungnahme enthält die Ergebnisse der Rechtsanalyse durch die Datenschutzbehörden in der EU, die in der Artikel-29-Datenschutzgruppe (die Datenschutzgruppe) vereint sind, in Bezug auf die Auswirkungen elektronischer Überwachungsprogramme auf den Schutz des Grundrechts auf Datenschutz und Schutz der Privatsphäre.

Die Hauptaufgabe von Datenschutzbehörden besteht darin, das Grundrecht jedes Einzelnen auf Datenschutz zu schützen und sicherzustellen, dass die entsprechenden gesetzlichen Vorgaben von den Datenverarbeitern eingehalten werden. Allerdings haben viele Datenschutzbehörden nur begrenzte oder sogar gar keine Aufsichtsbefugnisse über Nachrichtendienste. Für deren Beaufsichtigung, einschließlich der Verarbeitung personenbezogener Daten, haben die Mitgliedstaaten andere Regelungen getroffen. Die Datenschutzgruppe hat daher eine Bestandsaufnahme der in der EU für die Überwachung der Nachrichtendienste vorhandenen verschiedenen Regelungen vorgenommen, die Bestandteil dieser Stellungnahme ist.

Nicht berücksichtigt ist in dieser Stellungnahme das kabelgebundene Abfangen personenbezogener Daten. Der Datenschutzgruppe liegen zum gegenwärtigen Zeitpunkt nicht genügend Informationen zu diesen Behauptungen vor, um die anwendbare Rechtsgrundlage - und sei es auch nur hypothetisch - bewerten zu können.

2. Metadaten

Um das Ausmaß der mutmaßlichen Verletzung von Datenschutzvorschriften beurteilen zu können, muss zunächst abgeklärt werden, worum es eigentlich geht. Regierungsvertreter sprechen oftmals von der Sammlung von Metadaten und implizieren damit, dass diese weniger bedenklich ist als die Sammlung von Inhalten. Diese Annahme ist jedoch falsch. Unter Metadaten fallen sämtliche Daten einer stattfindenden Kommunikation, ausgenommen der Inhalt der Konversation. Dazu zählen beispielsweise die Telefonnummer bzw. die IP-Adresse der anrufenden oder eine E-Mail versendenden Person, Informationen zum Zeitpunkt, Ort, Thema, Empfänger usw. Die Analyse kann sensible Daten von Personen zu Tage bringen, weil z. B. Auskunftsnummern medizinischer oder religiöser Zentren angewählt wurden. Wie der Europäische Gerichtshof für Menschenrechte bereits im Fall Malone[1] festgestellt hat, ist die Verarbeitung von Metadaten, wobei es in diesem Fall um die Registrierung von Kommunikationsverbindungsdaten („metering“) ging, ein integraler Bestandteil der Telefonkommunikation. Daher komme die Weitergabe dieser Informationen an die Polizei ohne die Einwilligung des Telefonteilnehmers einer Verletzung eines durch Artikel 8 gewährleisteten Rechts gleich. Der Gerichtshof hat seitdem an dieser Auffassung festgehalten.

Festzustellen ist auch, dass Metadaten oftmals leichter Informationen preisgeben als der eigentliche Inhalt der Kommunikation.[2] Aufgrund ihrer Strukturiertheit lassen sie sich mühelos sammeln und analysieren. Moderne Computerprogramme gestatten die Analyse großer Datensätze und die Identifizierung darin enthaltener Muster und Beziehungen, einschließlich privater Details, Gewohnheiten und Verhaltensweisen. Die eigentlichen Gespräche sind nicht gleichermaßen analysierbar, da sie in beliebiger Form und Sprache geführt werden.

Gemäß Artikel 2 Buchstabe a der Richtlinie 95/46/EG sind personenbezogene Daten „alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person“); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann“. Eine ähnliche Begriffsbestimmung erfolgt in Artikel 2 Buchstabe a der Konvention Nr. 108 des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten. Daher werden Metadaten in Europa im Gegensatz zu anderen Ländern als personenbezogene Daten betrachtet und sind zu schützen.[3]

In einem kürzlich ergangenen Urteil zur Vorratsdatenspeicherung bestätigte der Gerichtshof der Europäischen Union, dass „aus der Gesamtheit dieser [Telekommunikations-]Daten […] sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert

[1] Urteil des EGMR vom 2. August 1984, Malone/Vereinigtes Königreich.

[2] ACLU/Clapper, Fall Nr. 13-3994 (WHP) – Schriftliche Erklärung von Prof. Edward W. Felten vor dem US-Bezirksgericht des Southern District New York.

[3] Es handelt sich dabei um eine seit langem bestehende Auslegung des Datenschutzrechts. In ihrer Stellungnahme 4/2007 zum Begriff „personenbezogener Daten“ hat die Datenschutzgruppe bereits festgestellt, dass „auch wenn der Umfang der vorhandenen Kennzeichen auf Anhieb keinen Rückschluss auf eine bestimmte Person erlaubt, […] diese Person dennoch „bestimmbar“ sein [könnte], weil diese Information in Verbindung mit anderen Informationen (unabhängig davon, ob diese vom für die Verarbeitung Verantwortlichen gespeichert werden oder nicht) eine Unterscheidung dieser Person von anderen Personen ermöglicht“.

wurden, gezogen werden [können]“.[4] Und schließlich befand der Gerichtshof im selben Urteil, dass „die Pflicht, […] Daten über das 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. […] Außerdem ist der Umstand, dass die Vorratsspeicherung der Daten und ihre spätere Nutzung vorgenommen werden, ohne dass der Teilnehmer oder der registrierte Benutzer darüber informiert wird, geeignet, bei den Betroffenen […] das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist.“[5]

3. Hauptpunkte

Die Enthüllungen von Edward Snowden stellten für viele einen heftigen Weckruf dar. Erstmals wurde offenbar, wie viele verschiedene Überwachungsprogramme die Nachrichtendienste zu laufen haben, mit denen Daten über praktisch jeden gesammelt werden können. Einzelfälle sind bereits früher bekannt geworden, doch nun liegen erstmals umfassende Belege für die allgemeine Durchdringung auf dem Tisch. Die Art und Weise, in der Nachrichtendienste die Daten unserer täglichen Kommunikation wie auch deren Inhalt nutzen, verdeutlicht, dass der Überwachung Grenzen gesetzt werden müssen.

Selbst jene, die ihr Online-Leben mit Bedacht führen, können sich gegenwärtig nicht vor massiven Überwachungsprogrammen schützen. Und angesichts der vielen rechtlichen, technischen und praktischen Herausforderungen können Datenschutzbehörden in aller Welt auch keinen zufriedenstellenden Schutz bieten. Es muss daher ein Wandel vollzogen werden.

In den folgenden Kapiteln analysiert die Artikel-29-Datenschutzgruppe die massive Datensammlung durch Nachrichtendienste im Lichte ihrer Überwachungsprogramme. Aus rechtlicher Sicht ist zwischen Überwachungsprogrammen von Nachrichtendiensten der Mitgliedstaaten und Überwachungsprogrammen der Nachrichtendienste von Drittländern, die Daten von EU-Bürgern verwenden, zu unterscheiden.

Von EU-Mitgliedstaaten durchgeführte Überwachungsprogramme unterliegen entsprechend den in die EU-Verträge aufgenommenen Ausnahmeregelungen aus Gründen der nationalen Sicherheit und den – nach diesem Beschluss der vertragschließenden Mitgliedstaaten – erlassenen EU-Verordnungen und -Richtlinien, einschließlich der EU-Datenschutzrichtlinie 95/46/EG, generell nicht den EU-Rechtsvorschriften. Das heißt allerdings nicht, dass solche Programme nur dem einzelstaatlichen Recht unterworfen sind. Die Analyse durch die Artikel-29-Datenschutzgruppe zeigt, dass auch wenn das EU-Recht im Allgemeinen und die Datenschutzrichtlinie im Besonderen nicht anwendbar sind, aus der Europäischen Menschenrechtskonvention und der Konvention Nr. 108 des Europarates zum Schutz personenbezogener Daten folgt, dass die Grundsätze des Datenschutzes[6] von den

[4] Siehe Urteil des EuGH vom 8. April 2014, verbundene Rechtssachen C-293/12 und C-594/12, Randnr. 27.

[5] Siehe Urteil des EuGH vom 8. April 2014, verbundene Rechtssachen C-293/12 und C-594/12, Randnrn. 34, 35 und 37.

[6] Zu den wichtigsten Datenschutzgrundsätzen gehören eine rechtmäßige Verarbeitung nach Treu und Glauben, Zweckbindung, Erforderlichkeit und Verhältnismäßigkeit, sachliche Richtigkeit, Transparenz, Wahrung der Rechte des Einzelnen und angemessene Datensicherheit.

Nachrichtendiensten bei der rechtmäßigen Wahrnehmung ihrer Aufgaben gleichwohl zum Großteil einzuhalten sind. Diese Grundsätze sind in vielen Mitgliedstaaten Bestandteil der jeweiligen nationalen Verfassung. Überwachungsprogramme, die auf der unterschiedslosen und flächendeckenden Sammlung personenbezogener Daten basieren, können keinesfalls den in diesen Datenschutzgrundsätzen niedergelegten Anforderungen an die Erforderlichkeit und die Verhältnismäßigkeit genügen. Beschränkungen der Grundrechte sind der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR)[7] und des Gerichtshofs der Europäischen Union (EuGH)[8] zufolge eng auszulegen. Dazu gehört, dass alle Eingriffe im Hinblick auf das verfolgte Ziel erforderlich und verhältnismäßig sein müssen. Außerdem ist zu beachten, dass nicht automatisch davon auszugehen ist, dass das von einer nationalen Behörde vorgebrachte Argument der nationalen Sicherheit tatsächlich zutrifft und berechtigt ist. Dies muss erst nachgewiesen werden.

Die Datenschutzgruppe bekräftigt, dass es Sache der Regierungen der Mitgliedstaaten ist, sämtlichen nationalen und internationalen Verpflichtungen einschließlich dem Internationalen Pakt über bürgerliche und politische Rechte nachzukommen, denn andernfalls würden nicht nur die Grundrechte ihrer Bürger verletzt, sondern auch das Vertrauen der Gesellschaft in die Rechtsstaatlichkeit beschädigt.

Bei Überwachungsprogrammen, die von Drittstaaten durchgeführt werden, ist die Sachlage komplizierter. Werden Daten entweder direkt aus einer Quelle in der EU oder nach der Übermittlung in den jeweiligen Drittstaat (oder auch einen weiteren Drittstaat) erfasst, können die im Zuge der Überwachungsprogramme offengelegten Informationen weiterhin unter das EU-Recht fallen. Die bereits genannte Ausnahme aus Gründen der nationalen Sicherheit gilt nämlich nur für die nationale Sicherheit eines EU-Mitgliedstaats und nicht für die eines Drittstaats. Natürlich kann es zu Situationen kommen, in denen sich die nationalen Sicherheitsinteressen eines Drittstaats mit denen eines Mitgliedstaats überschneiden und gemeinsame Überwachungsmaßnahmen berechtigt sind. Auch dann müssen die an der Überwachung beteiligten Behörden nachweisen können, warum und inwiefern sich die nationalen Sicherheitsinteressen überschneiden und damit die Anwendung des EU-Rechts ausschließen.

Alle in der Richtlinie 95/46/EG aufgeführten Anforderungen an die internationale Übermittlung personenbezogener Daten müssen beachtet werden: Dies bedeutet vor allem, dass der Empfänger ein angemessenes Schutzniveau gewährleistet und die Übermittlungen mit dem ursprünglichen Zweck, aus dem die Daten erfasst wurden, in Einklang stehen. Die Übermittlungen müssen auch das Erfordernis einer angemessenen Rechtsgrundlage für eine rechtmäßige Verarbeitung nach Treu und Glauben erfüllen.

---

[7] Siehe Urteile des EGMR vom 17. Januar 1970 (Delcourt) und vom 6. September 1978 (Klass).

[8] Siehe Urteil des EuGH vom 8. April 2014 in den verbundenen Rechtssachen C-293/12 und C-594/12, in dem der Gerichtshof feststellte, dass die Vorratsdatenspeicherung von Verkehrsdaten „ohne irgendeine Differenzierung, Einschränkung oder Ausnahme“ […] „einen Eingriff in diese Grundrechte beinhaltet, der in der Rechtsordnung der Union von großem Ausmaß und von besonderer Schwere ist, ohne dass sie (Richtlinie 2006/24, Anm. d. Ü.) Bestimmungen enthielte, die zu gewährleisten vermögen, dass sich der Eingriff tatsächlich auf das absolut Notwendige beschränkt” (Randnrn. 57 und 65).

Keines der verfügbaren Instrumente, das als alternative Grundlage für die Übermittlung personenbezogener Daten an unsichere Staaten genutzt werden kann (Grundsätze des „sicheren Hafens“, Standardvertragsklauseln und unternehmensinterne Datenschutzregelungen), erlauben Drittstaatsbehörden den Zugang zu den auf ihrer Grundlage übermittelten personenbezogenen Daten zum Zwecke der massiven und willkürlichen Überwachung. Die in diesen Instrumenten enthaltenen Ausnahmeregelungen haben nämlich einen beschränkten Anwendungsbereich und sollten eng ausgelegt werden (d. h. sie sind nur in Sonderfällen und bei einzelnen Ermittlungen anwendbar). Da die Instrumente zur Sicherstellung der Angemessenheit insbesondere dem Schutz der aus der EU stammenden personenbezogenen Daten dienen sollen, sollten sie unter keinen Umständen so umgesetzt werden, dass das durch die EU-Vorschriften und -Instrumente für die Datenübermittlung garantierte Schutzniveau beeinträchtigt wird. Die Datenschutzgruppe betont außerdem, dass sich gemäß der Datenschutzrichtlinie die Bewertung des Datenschutzniveaus in Drittstaaten derzeit im Allgemeinen nicht auf die Verarbeitung von Daten für Strafverfolgungs- oder Überwachungszwecke erstreckt.

Unternehmen sollte zudem bewusst sein, dass sie gegen EU-Recht verstoßen könnten, wenn Nachrichtendienste von Drittstaaten Zugang zu den auf ihren Servern gespeicherten Daten von EU-Bürgern erlangen, oder sie einer Anweisung folgen, in großem Maßstab personenbezogene Daten herauszugeben. Diesbezüglich könnten Unternehmen bei der Entscheidung, ob sie einer Anweisung zur Herausgabe personenbezogener Daten in großem Maßstab nachkommen oder nicht, in eine Zwickmühle geraten: Entweder sie verstoßen gegen EU-Recht oder das Recht des jeweiligen Drittstaats. Strafverfolgungsmaßnahmen gegen diese Unternehmen sollten insbesondere in Fällen nicht ausgeschlossen werden, in denen für die Datenverarbeitung Verantwortliche willentlich und wissentlich mit Nachrichtendiensten zusammengearbeitet und ihnen Zugang zu ihren Daten verschafft haben. Unternehmen müssen für ein möglichst hohes Maß an Transparenz sorgen und sicherstellen, dass sich Betroffene im Klaren darüber sind, dass, sobald ihre personenbezogenen Daten auf der Grundlage der für diese Übermittlungen verfügbaren Instrumente an unsichere Drittstaaten übermittelt wurden, sie von Drittstaatsbehörden überwacht werden können oder diese Zugangsrechte haben können, sofern derartige Ausnahmen in den genannten Instrumenten vorgesehen sind. Am wichtigsten ist es allerdings, eine wirksame Lösung auf politischer Ebene zu finden. Durch ein Schutzbestimmungen enthaltendes internationales Abkommen könnte sichergestellt werden, dass Nachrichtendienste die Grundrechte achten.

Damit die Nachrichtendienste die Beschränkungen für Überwachungsprogramme auch tatsächlich einhalten, sind wirksame Aufsichtsmechanismen in den Gesetzen aller Mitgliedstaaten vorzusehen. Dazu sollten gänzlich unabhängige Kontrollen der Datenverarbeitungsvorgänge durch eine unabhängige Stelle sowie wirksame Durchsetzungsbefugnisse gehören. Neben einer stärkeren und effektiven parlamentarischen Kontrolle könnten diese Aufgaben je nach den von dem jeweiligen Mitgliedstaat erlassenen Aufsichtsregeln von einer Datenschutzbehörde oder einem anderen geeigneten unabhängigen Gremium wahrgenommen werden. Sollte die Aufsicht durch ein anderes Gremium erfolgen, empfiehlt die Datenschutzgruppe regelmäßige Kontakte zwischen diesem Gremium und der nationalen Datenschutzbehörde, um eine kohärente und einheitliche Anwendung der Datenschutzgrundsätze sicherzustellen.

Es sei darauf hingewiesen, dass Aufsichtsmechanismen nicht nur auf dem Papier bestehen dürfen, sondern konsequent anzuwenden sind. Die Enthüllungen von Edward Snowden haben gezeigt, dass es auf dem Papier zwar viele Kontrollmechanismen gibt, darunter eine gerichtliche Kontrolle geplanter Datenerhebungsprogramme, die wirksame Umsetzung der Schutzmaßnahmen jedoch zu wünschen übrig lässt. Werden die Schutzmaßnahmen gegen den unberechtigten Zugriff weder auf alle Überwachungsprogramme noch auf alle Personen angewendet, gewährleisten sie nicht die von der Datenschutzgruppe angestrebte umfassende Aufsicht.

4. Aufsicht über Nachrichtendienste

Während die Aufsichtsmodalitäten für die Sicherheits- und Nachrichtendienste von Drittstaaten in den letzten Jahren eingehend von Sachverständigen verschiedener Einrichtungen untersucht wurden, standen die nationalen Nachrichtendienste der einzelnen EU-Mitgliedstaaten weniger im Fokus eingehenderer Analysen. Um ein klareres Bild von den verschiedenen Modalitäten für die Aufsicht über nationale Nachrichtendienste in Europa zu gewinnen, hat die Datenschutzgruppe allen Datenschutzbehörden (darunter zwei Nicht-EU-Beobachtern) einen Fragebogen zugesandt, um Auskünfte über ihre diesbezügliche nationale Vorgehensweise einzuholen.[9]

Zwei Aspekte sollen eingehender beleuchtet werden:

1. das Vorhandensein eines gesetzlichen Rahmens für eine umfassende Aufsicht über nationale Sicherheits- und Nachrichtendienste;

2. die Funktion (oder die fehlende Funktion) der nationalen Datenschutzaufsichtsbehörde innerhalb dieses gesetzlichen Rahmens.

Die Datenschutzgruppe kommt damit auch der Aufforderung der Vizepräsidentin der Europäischen Kommission, Viviane Reding, nach, die künftige Funktion der Datenschutzbehörden zu prüfen.[10]

4.1. Überblick über die einschlägigen nationalen Aufsichtsmechanismen

Die Überwachungstätigkeiten, um die es in dieser Stellungnahme und dem beigefügten Arbeitsdokument geht, werden überwiegend von Nachrichtendiensten im Rahmen der ihnen übertragenen Aufgaben zum Schutz der nationalen Sicherheit ausgeführt. Entsprechend den jeweiligen einzelstaatlichen Rechtstraditionen und -strukturen für nationale Sicherheitsmodalitäten gibt es ein breites Spektrum von Aufsichtssystemen. In 26 der 27 Mitgliedstaaten, die den Fragebogen beantworteten [11], bestehen und agieren die Nachrichtendienste auf der Grundlage von Gesetzen, in denen ihre Befugnisse, Struktur und

[9] Antworten auf den Fragebogen gingen von 27 nationalen Datenschutzbehörden der EU, der subnationalen Datenschutzbehörde Sachsens (Deutschland) und den Nicht-EU-Datenschutzbehörden der Schweiz und Serbiens ein.
[10] Schreiben von Vizepräsidentin Reding an den Vorsitzenden der Artikel-29-Datenschutzgruppe vom 30. August 2013.
[11] Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Österreich, Polen, Portugal, Rumänien, Schweden, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn, Vereinigtes Königreich, Zypern.

Zuständigkeiten niedergelegt sind. In einem Mitgliedstaat, in dem es keine Nachrichtendienste gibt, werden die Sicherheitsaufgaben des Staats von der nationalen Polizei wahrgenommen.[12]

In der Mehrheit der Länder, die den Fragebogen beantwortet haben, gibt es ein bis drei Sicherheits- und Nachrichtendienste auf nationaler Ebene. Im Allgemeinen erfolgt eine Trennung der Aufgaben nach interner und externer (ausländischer) Bedrohung der nationalen Sicherheit, was auch zu getrennten Zuständigkeiten, nämlich der zivilen (Innen- oder Justizministerium) und der militärischen (Verteidigungsministerium) führt. In drei Mitgliedstaaten sind die verschiedenen Strukturen zu einem Schutzsystem verbunden, das direkt dem Regierungschef (z. B. dem Premierminister) untersteht.

Der Verarbeitung personenbezogener Daten liegt jeweils ein einzelstaatliches Gesetz zugrunde, und die Aufsicht basiert entweder auf einem allgemeinen Datenschutzgesetz oder auf einem oder mehreren gesonderten Gesetzen für die Verarbeitung personenbezogener Daten durch einen oder mehrere Nachrichtendienste.

4.2. Die Funktion der nationalen Datenschutzaufsichtsbehörde

Die Analyse der einschlägigen nationalen Rechtsvorschriften zeigt, dass das allgemeine Datenschutzgesetz in vielen Ländern nicht für die nachrichtendienstlichen Tätigkeiten gilt und die Datenschutzbehörde eine begrenzte bzw. in einigen Fällen sogar gar keine Aufsichtsfunktion hat. Häufig sind spezifische Datenschutzregeln im Gesetz vorgesehen, doch diese sehen nicht zwangsläufig die Aufsicht durch die Datenschutzbehörde vor.

In den beiden Nicht-EU-Mitgliedstaaten, die den Fragebogen freundlicherweise ebenfalls beantworteten[13], ist die Verarbeitung personenbezogener Daten durch die Nachrichtendienste im allgemeinen Datenschutzgesetz geregelt. Die Aufsicht hierüber führt die nationale Datenschutzbehörde gestützt auf Vorschriften, die ebenfalls im allgemeinen Datenschutzgesetz niedergelegt sind.

Soweit anwendbar sieht das allgemeine Datenschutzgesetz in der Regel eine Reihe von Ausnahmeregelungen (Abweichungen von einem oder mehreren Grundsätzen) bei der Verarbeitung personenbezogener Daten durch Nachrichtendienste vor. Diese Ausnahmen betreffen zumeist die grundlegenden Verpflichtungen von Datenverarbeitern und die Rechte der betroffenen Personen.[14] Sie können in der Beschränkung des Rechts, unterrichtet zu werden, und des Rechts auf Zugang durch die betroffene Person bestehen, die im Allgemeinen durch die Datenschutzbehörde vorzunehmen ist.

Was die Aufsicht über die Datenverarbeitung anbelangt, so werden in nur vier Mitgliedstaaten mit den allgemeinen einzelstaatlichen Datenschutzgesetzen (oder dem Gesetz zur Errichtung eines allgemeinen Datenschutzaufsichtsgremiums) grundsätzlich die gleichen Aufsichtsbefugnisse über Nachrichtendienste verliehen wie über jeden anderen für die

[12] Irland.
[13] Serbien (ein ziviler und zwei militärische Dienste), Schweiz (ein ziviler und ein militärischer Dienst).
[14] Beispielsweise Belgien, Bulgarien, Deutschland, Griechenland, Ungarn und Zypern. Für einige Mitgliedstaaten liegen keine Informationen über Ausnahmeregelungen vor.

Datenverarbeitung Verantwortlichen.[15] In dreizehn Mitgliedstaaten fallen die nationalen Sicherheits- und Nachrichtendienste unter die Aufsichtsbefugnis der Datenschutzbehörde, doch in einigen Fällen sind spezielle Vorschriften oder Verfahren für die Beaufsichtigung von Sicherheits- und Nachrichtendiensten anwendbar, darunter die Möglichkeit, Sanktionen zu verhängen.[16] In neun Mitgliedstaaten hat die Datenschutzbehörde keine Aufsichtsbefugnis über den Nachrichtendienst als Datenverarbeiter.[17]

Nur in Schweden und Slowenien ist die volle Aufsicht der Datenschutzbehörde über die Einhaltung der geltenden Datenschutzverpflichtungen gewährleistet. Sofern andere nationale Datenschutzbehörden Befugnisse gegenüber Nachrichtendiensten haben, bestehen diese darin, die Einhaltung des geltenden allgemeinen Datenschutzgesetzes zu überprüfen, Beschwerden zu bearbeiten und das Recht der betreffenden Person auf Zugang auszuüben. Des Weiteren dürfen sie auf eigene Initiative oder auf Antrag eines Dritten Untersuchungen und Vor-Ort-Kontrollen durchführen. In einigen Mitgliedstaaten unterliegen diese Befugnisse gewissen Beschränkungen, indem beispielsweise die Einhaltung spezieller Sicherheitsbestimmungen bei der Untersuchung auferlegt wird, um staatlichen Geheimhaltungspflichten Rechnung zu tragen.

4.3. Die Funktion anderer unabhängiger Aufsichtsmechanismen

Zwanzig Mitgliedstaaten erklärten, dass das Gesetz neben der Zuständigkeit der Datenschutzbehörden für die Datenverarbeitung die parlamentarische Aufsicht und/oder Kontrolle über die Tätigkeiten der Nachrichtendienste[18] und spezielle interne Kontrollsysteme vorsieht.[19] Die Auffassungen über die parlamentarische Kontrolle gehen in den Mitgliedstaaten allerdings offenkundig auseinander, denn nur wenige von ihnen verfügen tatsächlich über eine Stelle, die für die Aufsicht über den Datenschutz (und die Bewertung der Rechte der Betroffenen sowie die Einhaltung der Bestimmungen des allgemeinen Datenschutzgesetzes und der spezifischen Vorschriften) zuständig ist.[20]

Die bestehenden Aufsichtsmechanismen sind äußerst vielfältig und bestehen aus folgenden Elementen:

- Ein Parlamentsausschuss mit der umfassenden Aufgabe, Geheimdienst- und Sicherheitsbehörden im Allgemeinen oder einen bestimmten Nachrichtendienst zu beaufsichtigen.

- Die parlamentarische Aufsicht und/oder Kontrolle erfolgt neben anderen unabhängigen Aufsichtsgremien (bei denen es sich nicht um Datenschutzbehörden handelt). Derzeit

[15] Bulgarien, Schweden, Slowenien, Ungarn.
[16] Belgien, Deutschland, Estland, Finnland, Frankreich, Irland, Italien, Lettland, Luxemburg, Österreich, Polen, Schweden, Zypern.
[17] Dänemark, Malta, Niederlande, Portugal, Rumänien, Slowakei, Spanien, Tschechische Republik, Vereinigtes Königreich.
[18] In Finnland beispielsweise besitzt neben der Datenschutzbehörde der Bürgerbeauftragte des Parlaments entsprechende Befugnisse; diese basieren allerdings auf dem speziellen Gesetz für Sicherheits- und Nachrichtendienste.
[19] Diese 20 Mitgliedstaaten sind: Bulgarien, Deutschland, Estland, Finnland, Frankreich, Griechenland, Italien, Lettland, Luxemburg, Österreich, Polen, Portugal, Rumänien, die Slowakei, Slowenien, Spanien, die Tschechische Republik, Ungarn, das Vereinigte Königreich und Zypern.
[20] In der Stellungnahme werden keine Informationen zur Kontrolle der Verwaltung (der Ministerien) und zur allgemeinen politischen Kontrolle berücksichtigt, die von mehreren beitragenden Ländern vorgelegt wurden.

erfolgt die parlamentarische Kontrolle entweder durch den Bürgerbeauftragten des Parlaments, eine parlamentarische Delegation oder einen parlamentarischen Ausschuss.

- Ein Parlamentsausschuss ist das einzige Aufsichtsgremium außerhalb der Exekutivstruktur. Die Aufgaben des Parlaments sind in diesem Fall entweder sehr allgemein oder so formuliert, dass kein Zugang zu offenen Fällen vorgesehen ist.

- Für die Aufsicht ist ausschließlich eine spezielle Behörde zuständig. Der Zuständigkeit können Datenschutzvorschriften zugrundeliegen, in einem Fall wurde allerdings gemeldet, dass für diese Behörde bis vor kurzem unverbindliche Regelungen („Soft Law“) galten.

- Neben der allgemeinen parlamentarischen Aufsicht erfolgt eine spezielle gerichtliche Kontrolle.

- Neben der Aufsicht durch die allgemeine Datenschutzbehörde erfolgt eine gemischte exekutive und parlamentarische Kontrolle; den Vorsitz der eingesetzten Kommission hat ein Richter inne, und die Mitglieder gehören verschiedenen ehemals oder derzeit im Parlament vertretenen politischen Partien an. Es sind Konsultationsverfahren mit der Datenschutzbehörde vorgesehen.

- Denkanstöße für die Verbesserung der Aufsicht geben auch Länder, in denen ein spezielles Gremium für die Beaufsichtigung der Einhaltung des Datenschutzes durch Nachrichtendienste eingesetzt wurde, so z. B. eine aus drei vom Generalstaatsanwalt ernannten Staatsanwälten bestehende Datenaufsichtskommission, die die Nachrichtendienste neben dem parlamentarischen Aufsichtsrat beaufsichtigt.

- Die Datenschutzbehörde kann mit der Prüfung befasst werden, ob die nationale Sicherheit im Einzelfall berührt ist, und muss – sofern dies festgestellt wird – den Fall zwei unabhängigen Beauftragten mit unabhängiger gerichtlicher Aufsichtsbefugnis über die nationalen Nachrichtendienste und die vom Außenminister erteilten Ermächtigungen für die Durchführung einer verdeckten Überwachung vorlegen. Zusätzlich gibt es ein spezielles Gericht für die Entschädigung betroffener Personen.

- Ein gesondertes Gesetz sieht die Zusammenarbeit zwischen dem speziellen Aufsichtsgremium und der allgemeinen Datenschutzbehörde vor: Ein unabhängiger Rechtsschutzbeauftragter muss die Genehmigung erteilen, wenn die Geheim- oder Nachrichtendienste bestimmte Operationen durchführen wollen (z. B. verdeckte Ermittlungen, Videoüberwachung bestimmter Personen). Der Rechtsschutzbeauftragte ist darüber hinaus verpflichtet, bei der Datenschutzbehörde Beschwerde einzulegen, sofern er der Ansicht ist, dass Rechte aus dem allgemeinen Datenschutzgesetz verletzt wurden.

Die Datenschutzbehörde ist mit gewissen Einschränkungen zur Aufsicht über die Nachrichtendienste befugt, während ein spezielles parlamentarisches Gremium dafür zuständig ist, die Überwachung der Kommunikation zu beaufsichtigen und Beschwerden zu bearbeiten. Die Mitglieder des entsprechenden Ausschusses werden vom parlamentarischen Kontrollausschuss ernannt. Der Vorsitzende muss über die Befähigung zur Ausübung einer richterlichen Tätigkeit verfügen.

5. Empfehlungen

A. Mehr Transparenz

1. Es ist mehr Transparenz in Bezug auf die Funktionsweise der Programme und die Tätigkeiten und Entscheidungen der Aufsichtsbehörden geboten.

Die Datenschutzgruppe ist der Ansicht, dass die Mitgliedstaaten in Bezug auf ihre Rolle bei der Erfassung nachrichtendienstlicher Daten und die Mitnutzung von Programmen größtmögliche Transparenz herstellen sollten, und zwar vorzugsweise gegenüber der Öffentlichkeit, gegebenenfalls jedoch zumindest gegenüber ihren nationalen Parlamenten und den zuständigen Aufsichtsbehörden. Datenschutzbehörden wird empfohlen, ihr Fachwissen im Interesse der Wiederherstellung des Gleichgewichts zwischen nationalen Sicherheitsinteressen und dem Grundrecht auf Achtung der Privatsphäre des Einzelnen auf nationaler Ebene einzubringen.

Es sollte in irgendeiner Form ganz allgemein über Überwachungsaktivitäten berichtet werden, nicht zuletzt um den Transparenzverpflichtungen nachzukommen, die den Mitgliedstaaten dem EGMR zufolge obliegen.[21] Jeder Eingriff in die Grundrechte muss vorhersehbar sein, weshalb diese Programme auf klaren, spezifischen und zugänglichen Rechtsvorschriften basieren müssen. Die nationalen Datenschutzbehörden sind aufgefordert, ihren jeweiligen Regierungen diesen Standpunkt zur Kenntnis zu bringen.

2. Mehr Transparenz seitens der für die Datenverarbeitung Verantwortlichen

Unternehmen müssen für ein möglichst hohes Maß an Transparenz sorgen und sicherstellen, dass sich Betroffene im Klaren darüber sind, dass sobald ihre personenbezogenen Daten auf der Grundlage der für diese Übermittlungen verfügbaren Instrumente an unsichere Drittstaaten übermittelt wurden, sie von Drittstaatsbehörden überwacht werden können oder diese Zugangsrechte haben können, sofern derartige Ausnahmen in diesen Instrumenten vorgesehen sind. Die Datenschutzgruppe ist sich bewusst, dass Datenverarbeiter angewiesen worden sein können, die Betroffenen nicht über die von einer Behörde ergangene Anordnung zu unterrichten. Sie begrüßt die jüngsten Bemühungen um eine bessere und genauere Unterrichtung der Betroffenen über eingegangene Anfragen und ermutigt die Unternehmen, die Informationspolitik weiter zu verbessern.

3. Stärkere Sensibilisierung der Öffentlichkeit

Betroffene müssen über die Auswirkungen der Nutzung von elektronischen Online- und Offline-Kommunikationsdiensten und die Möglichkeiten, sich selbst besser zu schützen, Bescheid wissen. Dafür sind Datenschutzbehörden, andere Behörden, Unternehmen und die Zivilgesellschaft gemeinsam verantwortlich. Daher möchte die Datenschutzgruppe im zweiten Halbjahr 2014 eine Konferenz mit allen Beteiligten abhalten, auf der ein möglicher Ansatz diskutiert werden soll.

[21] Siehe auch Urteil des Europäischen Gerichtshofs für Menschenrechte vom 25. Juni 2013, Fall Nr. 48135/06 – *Youth Initiative for Human Rights/Serbien*, S. 6.

B. Wirkungsvollere Aufsicht

1. Pflege eines kohärenten Rechtssystems für die Nachrichtendienste, einschließlich datenschutzrechtlicher Vorschriften

Die Enthüllungen von Edward Snowden haben vor Augen geführt, dass die Nachrichtendienste der EU-Mitgliedstaaten täglich große Mengen an personenbezogenen Daten verarbeiten. Diese Daten werden mit anderen Diensten innerhalb und außerhalb der EU geteilt. Die Datenschutzgruppe hält es für wichtig, dass die Mitgliedstaaten über einen kohärenten Rechtsrahmen für die Nachrichtendienste, einschließlich Datenverarbeitungsvorschriften im Einklang mit den im EU- und Völkerrecht niedergelegten Datenschutzgrundsätzen, verfügen. Beim Schutz der gefährdeten öffentlichen Interessen sind die Rechte der betroffenen Personen in größtmöglichem Umfang zu gewährleisten.

Die Datenschutzgruppe empfiehlt darüber hinaus, dass der nationale Rechtsrahmen klare Vorschriften für die Zusammenarbeit und den Austausch von personenbezogenen Daten mit Strafverfolgungsbehörden bei der Verhütung, Bekämpfung und Verfolgung von Straftaten enthalten, so auch für die Übermittlung solcher Daten an Behörden in anderen EU-Mitgliedstaaten und in Drittstaaten.

2. Sicherstellung einer wirksamen Aufsicht über die Nachrichtendienste

Im nationalen Rechtsrahmen für die Nachrichtendienste sollte den bestehenden Aufsichtsmechanismen besondere Aufmerksamkeit gewidmet werden. In einer demokratischen Gesellschaft ist eine angemessene, unabhängige und wirksame Aufsicht von höchster Bedeutung. Die Datenschutzgruppe ist daher der Ansicht, dass die nachstehenden bewährten Praktiken, die derzeit in den Mitgliedstaaten innerhalb ihrer verschiedenen Aufsichtsmechanismen angewendet werden, fester Bestandteil der Aufsichtsmechanismen aller Mitgliedstaaten sein sollten. Den nationalen Datenschutzbehörden wird nahegelegt, diese Elemente in die nationale Debatte über die nachrichtendienstliche Aufsicht einzubringen:

- strenge interne Kontrollen der Einhaltung der nationalen Rechtsrahmen zur Gewährleistung von Rechenschaftspflicht und Transparenz;

- wirksame parlamentarische Kontrolle im Einklang mit den nationalen parlamentarischen Traditionen. Parlamente, die bereits über Aufsichtsbefugnisse über die Nachrichtendienste verfügen, sollten von den nationalen Datenschutzbehörden dazu angehalten werden, diese aktiv wahrzunehmen;

- effektive, solide und unabhängige externe Aufsicht, die entweder von einem zuständigen Gremium unter Mitwirkung der Datenschutzbehörden oder von der Datenschutzbehörde selbst wahrgenommen wird, die die Befugnis zum regelmäßigen Zugang zu Daten oder sonstigen einschlägigen Unterlagen auf eigene Initiative (von Amts wegen) sowie die Verpflichtung zur Prüfung eingelegter Beschwerden hat. Die vorherige Zustimmung des zu beaufsichtigenden Nachrichtendienstes darf nicht erforderlich sein.

C. Wirksame Anwendung des geltenden Rechts

1. Durchsetzung der bestehenden Verpflichtungen der EU-Mitgliedstaaten und der EMRK-Vertragsparteien zum Schutz der Rechte auf Achtung des Privatlebens und Datenschutz

Alle Mitgliedstaaten sind Vertragsparteien der Europäischen Menschenrechtskonvention. Daher müssen ihre Überwachungsprogramme den in den Artikeln 7 und 8 EMRK genannten Bedingungen genügen. Doch damit enden ihre Verpflichtungen noch nicht. Artikel 1 EMRK verpflichtet die Vertragsparteien außerdem dazu, allen ihrer Hoheitsgewalt unterstehenden Personen die in der Konvention bestimmten Rechte und Freiheiten zuzusichern. Sowohl als EU-Mitgliedstaaten als auch als EMRK-Vertragsparteien können sie wegen der Verletzung des Rechts auf Achtung des Privatlebens eines EU-Staatsbürgers vor den EGMR gebracht werden.

2. Dem EU-Recht unterliegende Datenverarbeiter müssen die einschlägigen EU-Datenschutzvorschriften einhalten

Datenverarbeiter, die in der EU niedergelassen sind oder Ausrüstung in einem Mitgliedstaat nutzen, müssen ihren EU-rechtlichen Verpflichtungen auch dann nachkommen, wenn die Rechtsvorschriften anderer Länder, in denen sie tätig sind, dem EU-Recht entgegenstehen. Datenschutzbehörden dürfen diesbezüglich nicht unberücksichtigt lassen, dass Daten unter Verstoß gegen das EU-Recht übermittelt werden können. Die Datenschutzgruppe weist daher erneut darauf hin, dass die Datenschutzbehörden gemäß den nationalen und EU-Datenschutzbestimmungen den Datenfluss innerhalb der Übermittlungsinstrumente aussetzen können, wenn eine hohe Wahrscheinlichkeit besteht, dass Datenschutzgrundsätze verletzt werden und die fortgesetzte Datenübermittlung für die betroffene Personen das unmittelbare Risiko eines schweren Schadens schaffen würde. Die nationalen Datenschutzbehörden sollten entsprechend ihrer nationalen Zuständigkeit entscheiden, ob Sanktionen in einer konkreten Situation angezeigt sind.

D. Verbesserung des Schutzes auf europäischer Ebene

1. Annahme des Datenschutz-Reformpakets

Um wesentliche Datenschutzgarantien in Europa bieten zu können, müssen die Verhandlungen über das Datenschutz-Reformpaket unbedingt zum Abschluss gebracht werden, denn die neue Datenschutz-Grundverordnung und die Richtlinie über den Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit sollen nicht nur den Datenschutz für Privatpersonen verbessern, sondern auch ihren Anwendungsbereich klarstellen und die Durchsetzungsbefugnisse der Datenschutzbehörden stärken. Insbesondere durch die Möglichkeit, – als letztes Mittel – (Geld)Strafen zu verhängen, soll der Druck auf die Datenverarbeiter erhöht werden. Die Datenschutzgruppe begrüßt den Vorschlag des Europäischen Parlaments, Personen verpflichtend zu informieren, wenn einer Behörde innerhalb der letzten zwölf Monate Zugriff auf Daten gewährt wurde. Durch Transparenz bei diesen Handlungen wird das Vertrauen enorm gestärkt. Die Datenschutzgruppe fordert den

Rat und das Europäische Parlament daher auf, sich an ihren vereinbarten Zeitplan zu halten[22] und dafür zu sorgen, dass beide Rechtsinstrumente im Laufe des Jahres 2014 angenommen werden können.

2. Präzisierung des Anwendungsbereichs der Ausnahmeregelung aus Gründen der nationalen Sicherheit

Es herrscht derzeit keine Einigkeit darüber, was unter nationaler Sicherheit zu verstehen ist. Weder hat der europäische Gesetzgeber eine klare Begriffsbestimmung vorgenommen, noch ist die Rechtsprechung der europäischen Gerichte schlüssig. Dessen ungeachtet darf sich die Ausnahmeregelung nicht auf die Verarbeitung personenbezogener Daten zu gegen das Gesetz verstoßenden Zwecken erstrecken.

Es stellt sich auch die Frage, inwieweit eine auf nationale Sicherheitsinteressen ausgerichtete Ausnahmeregelung noch der Realität entspricht, da nun offenbar geworden ist, dass die Tätigkeit der Nachrichtendienste mehr denn je mit der Tätigkeit der Strafverfolgungsbehörden verflochten ist und mit ihr mehrere unterschiedliche Zwecke verfolgt werden. Daten werden kontinuierlich und weltweit ausgetauscht, wobei es keine Rolle spielt, wessen nationale Sicherheit von der Analyse dieser Daten profitiert. Die Datenschutzgruppe fordert den Rat, die Kommission und das Parlament daher auf, sich auf eine Definition des Begriffs der nationalen Sicherheit zu verständigen und schlüssig zu klären, was in die ausschließliche Zuständigkeit der Mitgliedstaaten fällt. Bei der Definition des Begriffs der nationalen Sicherheit sollten die Überlegungen der Datenschutzgruppe, einschließlich der Darlegungen in dieser Stellungnahme, gebührend berücksichtigt werden. Die EU-Organe sollten in dem Datenschutz-Reformpaket zudem klarstellen, dass der Schutz der nationalen Sicherheit von Drittstaaten allein kein Ausschlussgrund für die Anwendbarkeit des EU-Rechts sein kann.

E. Internationaler Schutz für in der EU ansässige Personen

1. Einforderung hinreichender Garantien für den Austausch nachrichtendienstlicher Daten

Die Behörden von Drittstaaten und insbesondere deren Nachrichtendienste dürfen keinen unmittelbaren Zugriff auf in der EU verarbeitete private Daten haben. Wenn sie im Einzelfall und bei begründetem Verdacht Zugriff auf solche Daten verlangen, müssen sie gegebenenfalls gemäß internationaler Übereinkünfte einen entsprechenden Antrag stellen und für angemessene Datenschutzgarantien sorgen. Beim Austausch nachrichtendienstlicher Informationen haben die Mitgliedstaaten sicherzustellen, dass die nationalen Rechtsvorschriften eine spezifische Rechtsgrundlage für diesen Austausch sowie hinreichende Garantien für den Schutz personenbezogener Daten vorsehen. Aus Sicht der Datenschutzgruppe erfüllen geheime Kooperationsvereinbarungen zwischen Mitgliedstaaten und/oder Drittstaaten nicht die Anforderungen des EGMR an eine klare und zugängliche Rechtsgrundlage.

[22] http://euobserver.com/justice/122853

2. Aushandlung internationaler Abkommen zur Gewährleistung angemessener Datenschutzgarantien

Das Konzept eines Rahmenabkommens, wie es derzeit zwischen den USA und der EU ausgehandelt wird, ist ein Schritt in die richtige Richtung. Ein solches Abkommen könnte allerdings in zweierlei Hinsicht unzulänglich sein: So wären Fälle, in denen es um die nationale Sicherheit geht, – zumindest aus europäischer Sicht – ausgenommen, da das Abkommen ausschließlich auf EU-Recht basieren soll. Zudem legt sein Aufbau nahe, dass es nur für Daten gelten soll, die zwischen Behörden der USA und der EU ausgetauscht werden, und nicht für von privaten Einrichtungen erhobene Daten. Dies geht auch aus dem Bericht der Hochrangigen Kontaktgruppe EU-USA (HLCG) für den Informationsaustausch und den Schutz der Privatsphäre und der personenbezogenen Daten[23] hervor, der den Verhandlungen über das Rahmenabkommen zugrundeliegt. Die Datenschutzgruppe betont, dass in dem Rahmenabkommen festgeschrieben werden sollte, dass die Verarbeitung der übermittelten Daten in der EU und den USA zum selben Zweck erfolgt. Es wäre nicht hinnehmbar, wenn von EU-Strafverfolgungsbehörden gesammelte Daten später von US-Geheimdiensten für nationale Sicherheitsbelange verwendet werden könnten, solange der EU nicht die gleichen Möglichkeiten offen stehen.

Da das Rahmenabkommen nicht allen Bürgern vollständigen Schutz bieten wird, bedarf es eines internationalen Abkommens, das angemessenen Schutz vor willkürlicher Überwachung gewährleistet. Auch der derzeitige Widerstreit der Rechtsprechung in Bezug auf Teile der enthüllten Überwachungstätigkeiten ließe sich entschärfen, wenn der Überwachung durch solch ein Abkommen klare Grenzen gesetzt würden. Dieses Abkommen wäre allerdings direkt an die Ausnahmeregelung aus Gründen der nationalen Sicherheit gekoppelt und fiele damit nicht in den Anwendungsbereich des EU-Rechts. Die Mitgliedstaaten müssen daher koordinierte Verhandlungen einleiten. Es sollte eindeutig festgestellt werden, welche der genannten Überwachungstätigkeiten tatsächlich unter die nationale Sicherheit fallen und welche eher mit der Strafverfolgung und außenpolitischen Zwecken in Verbindung stehen und damit unter EU-Recht fallende Bereiche berühren. Dies würde den EU-Organen die Möglichkeit zur stärkeren Beteiligung eröffnen, sollten Schritte in dieser Richtung unternommen werden.

Dieses neue Abkommen darf nicht geheim sein. Es muss veröffentlicht werden und sollte Verpflichtungen für die Vertragsparteien in Bezug auf die erforderliche Aufsicht über die Überwachungsprogramme, die Transparenz, die Gleichbehandlung zumindest der Bürger aller Vertragsparteien, die Rechtsbehelfsmechanismen und andere Datenschutzrechte enthalten. Die Beteiligten sollten zudem ermutigt werden, für eine regelmäßige Unterrichtung ihrer Parlamente über die Anwendung und den Nutzen des geschlossenen Abkommens zu sorgen.

[23] Ratsdokument Nr. 15851/09 vom 23. November 2009.

3. Entwicklung eines weltweiten Instruments zum Schutz der Privatsphäre und personenbezogener Daten

Die Datenschutzgruppe unterstützt die Entwicklung eines weltweiten Instruments, das durchsetzbare Grundsätze für den Schutz der Privatsphäre und des Datenschutzes auf einem hohem Niveau vorschreibt, wie sie auf der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre in ihrer Erklärung von Madrid vereinbart wurden.[24] In diesem Zusammenhang könnte die Annahme eines Zusatzprotokolls zu Artikel 17 des Internationalen Pakts der Vereinten Nationen über bürgerliche und politische Rechte in Erwägung gezogen werden. In solch einem internationalen Rechtsakt müsste sichergestellt werden, dass die gewährten Garantien allen Betroffenen zugutekommen. Zudem ist eine allgemein gültige Auslegung des Begriffs „Datenverarbeitung" notwendig, da weltweit sehr unterschiedliche Auffassungen dazu bestehen.

Die Datenschutzgruppe unterstützt die Initiative der deutschen Regierung und den Aufruf der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre.[25,26] Zudem befürwortet sie auch weiterhin den Beitritt von Drittstaaten zur Konvention Nr. 108 des Europarates.

[24] Internationale Standards zum Schutz personenbezogener Daten und zum Schutz der Privatsphäre, angenommen von der 31. Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre in Madrid.
[25] http://www.bundesregierung.de/ContentArchiv/DE/Archiv17/Artikel/2013/07/2013-07-19-bkin-nsa-sommerpk.html
[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.