Internationale Arbeitsgruppe
für Datenschutz in
der Telekommunikation

675.54.10

Arbeitspapier

zu internationalen Grundsätzen oder Instrumenten zur Regulierung der nachrichtendienstlichen Informationsbeschaffung

61. Meeting, 24.–25. April 2017, Washington D.C. (USA)

Umfang

Die Forderungen nach einem internationalen Instrument, das vereinbarte Grundsätze für nachrichtendienstliche Aktivitäten etabliert, werden immer lauter. Dieses Arbeitspapier gibt einen Überblick über einige dieser Forderungen und erläutert, warum Datenschutzbehörden sich an der Debatte zu diesem Thema beteiligen sollten. Zudem enthält das Arbeitspapier erste Vorschläge für einen Katalog an Grundsätzen, die – so die Hoffnung – die Grundlage für ein solches Instrument bilden können.

Die jüngsten Entwicklungen im Überblick

In der Vergangenheit fanden nachrichtendienstliche Tätigkeiten im Verborgenen statt und Regierungen haben oft weder den Umstand als solches noch den Umfang dieser Aktivitäten bestätigt. Sie unterlagen international vereinbarten Standards und wurden oft im Rahmen undurchsichtiger rechtlicher Befugnisse ausgeübt.

In den vergangenen Jahren, zum Teil aufgrund der Enthüllungen von Edward Snowden im Jahr 2013, ist das Spannungsverhältnis zwischen der nationalen Sicherheit und dem Recht auf Privatsphäre ins Bewusstsein einer breiteren Öffentlichkeit gerückt und hat eine hitzige globale Debatte darüber angefacht, wie ein angemessenes Gleichgewicht zwischen Sicherheit und Privatsphäre geschaffen werden kann. Im Verlauf der öffentlichen Diskussion kristallisierten sich einige Schlüsselthemen heraus, wie etwa der Wunsch, den Einsatz von technischen Instrumenten zur Erhebung personenbezogener Daten für Nachrichtendienste zu beschränken, den Einsatz von Telekommunikationstechnik und den Zugriff auf Netzwerke durch Nachrichtendienste zu regulieren und zu kontrollieren, sowie vorhandene Möglichkeiten auszuloten, einen globalen Konsens über die Förderung und den Schutz des Rechts auf Privatsphäre angesichts solcher Entwicklungen herzustellen.

Die Mitgliedstaaten der Vereinten Nationen (United Nations, UN) zeigten sich besorgt wegen der Enthüllungen über die Praktiken von Nachrichtendiensten zur Erhebung, Speicherung, Vorhaltung und Nutzung von Telekommunikationsdaten, einschließlich der elektronischen Kommunikation über das Internet.[1] Die Besorgnis über diese Enthüllungen wurde dadurch verstärkt, dass unklar war, ob Nachrichtendienste bei ihren Aktivitäten in der digitalen Welt Rücksicht auf bestehende internationale Menschrechtsstandards (z. B. das Recht auf Privatsphäre) nehmen. Vor diesem

[1] Siehe, als Bespiel, die Debatte der UN-Generalversammlung und des UN-Menschenrechtsrats über das Recht auf Privatheit im digitalen Zeitalter (2013).

Hintergrund verabschiedete die UN-Generalversammlung Ende 2014 die Resolution „*Das Recht auf Privatsphäre im digitalen Zeitalter*“[2] und schuf das Mandat eines Sonderberichterstatters zum „Recht auf Privatsphäre“.

Seit der Einberufung des Sonderberichterstatters wurden von der UN zwei substanzielle Resolutionen angenommen: eine durch die UN-Generalversammlung im Dezember 2016 (A/RES/71/199[3]) und die andere durch den UN-Menschenrechtsrat im März 2017 (A/HRC/34/7[4]). Diese Resolutionen bauen auf zuvor vereinbarter Sprache auf und legen den Umfang der Pflichten von Staaten in Bezug auf Handlungen von Unternehmen fest. In der Resolution des UN-Menschenrechtsrates wird zum ersten Mal auch anerkannt, dass jegliche Grundlagen für das Eingreifen in das Recht auf Privatsphäre mit den Grundsätzen der Rechtmäßigkeit, Notwendigkeit und Verhältnismäßigkeit in Einklang stehen müssen.

Es ist höchste Zeit, dass Datenschutzbehörden sich einmal mehr mit diesen Themen auseinandersetzen und Ansätze für eine verbesserte Regulierung der nachrichtendienstlichen Informationsbeschaffung fördern, die sich daran orientieren, rechtmäßige Bedürfnisse zur Herstellung nationaler Sicherheit mit dem Recht auf Privatsphäre in Einklang zu bringen.

Forderungen nach einem Konsens über internationale Standards und das Recht auf Privatsphäre im digitalen Zeitalter

Es wurden bereits Maßnahmen zur Förderung eines Konsenses über die Anwendung von Völkerrecht auf das Recht auf Privatsphäre im digitalen Zeitalter ergriffen, wie etwa durch die Implementierung angemessener Mechanismen, um die Aktivitäten von Nachrichtendiensten zu kontrollieren.

So richteten die Vereinten Nationen im Jahr 2013 beispielsweise eine Expertengruppe aus Regierungsvertretern (GGE) im Bereich der Information und Telekommunikation vor dem Hintergrund internationaler Sicherheit ein. Die GGE erstattete der Generalversammlung im Juli 2015 Bericht über ihre Vorschläge für Verhaltensregeln und andere Themen, die für die internationale Sicherheit im Cyberspace von Bedeutung sind,[5] einschließlich der folgenden Aspekte:

- *Bei der Nutzung von Informations- und Kommunikationstechnologien (IKT) müssen Staaten neben anderen Grundsätzen des Völkerrechts auch die Prinzipien der staatlichen Souveränität, der friedlichen Beilegung von Streitigkeiten und des Verbots des Eingreifens in interne Angelegenheiten eines Staates beachten.*
- *Vorhandene völkerrechtliche Verpflichtungen gelten auch für die Nutzung von Informations- und Kommunikationstechnologie durch Staaten und die Staaten müssen ihrer Verpflichtung zur Wahrung und zum Schutz der Menschenrechte und Grundfreiheiten nachkommen.*

---

[2] Vereinte Nationen Generalversammlung, 18. Dezember 2013, A/RES/ 68/167; verfügbar unter http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167

[3] Vereinte Nationen Generalversammlung, Resolution 71/199 – “The right to privacy in the digital age”; verfügbar unter http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/71/199

[4] Vereinte Nationen Generalversammlung, Menschenrechtsrat, Resolution A/HRC/34/7 – “The right to privacy in the digital age“; verfügbar unter http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/34/L.7/Rev.1&Lang=E

[5] Vereinte Nationen, Bericht der „UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security“, 22. Juli 2015, A/70/714. Verfügbar unter http://undocs.org/A/70/174

- *Staaten dürfen keine Rechnernetze einsetzen, die mithilfe von Informations- und Kommunikationstechnologie völkerrechtswidrige Handlungen vornehmen, und sie dürfen nicht zulassen, dass ihr Territorium von nicht staatlichen Akteuren für derartige Handlungen missbraucht wird.*
- *Die Vereinten Nationen sollten eine führende Rolle im Dialog über die Sicherheit bei der Anwendung von Informations- und Kommunikationstechnologie durch Staaten einnehmen und die Entwicklung eines gemeinsamen Verständnisses für die Anwendung völkerrechtlicher Gesetze und Normen sowie Regelungen und Grundsätze für ein verantwortungsvolles Verhalten der Staaten vorantreiben.*

Der Bericht der GGE wurde in der Vereinbarung zur Cybersicherheit zwischen China und den USA (2015) begrüßt. Die Vereinbarung sieht die Einrichtung einer Senior-Expertengruppe vor, die sich mit den Themen weiter auseinandersetzen soll.[6] Die GGE muss der Generalversammlung das nächste Mal im Jahr 2017 Bericht erstatten. Dabei wird es um folgende Themen gehen:

- Ausbildung eines gemeinsamen Verständnisses bestehender und potenzieller Bedrohungen im Bereich der Informationssicherheit
- Mögliche gemeinsame Gegenmaßnahmen
- Gültigkeit des Völkerrechts in Bezug auf die Anwendung von IKT durch Staaten, einschließlich Regelungen, Normen und Grundsätze für ein verantwortungsvolles Verhalten von Staaten.

Im Jahr 2013 gab die Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation ein Arbeitspapier zum Recht auf vertrauliche Telekommunikation heraus, mit dem sie folgende Forderungen an Regierungen richtete:

1. das Telekommunikationsgeheimnis als wesentlichen Teil des weltweit garantierten Menschenrechts auf Schutz der Privatsphäre anzuerkennen;
2. das Telekommunikationsgeheimnis als Menschenrecht in einem völkerrechtlichen Vertrag zu stärken. Einschränkungen sollten darauf begrenzt werden, was in einer demokratischen Gesellschaft unbedingt notwendig ist;
3. sich auf internationale Regeln zu verständigen, mit denen der Zugriff staatlicher Stellen auf Daten bei Internetanbietern und der Einsatz von nachrichtendienstlichen Mitteln im Internet begrenzt wird;
4. für größere Transparenz und öffentliche Rechenschaftspflicht von Regierungsstellen bezüglich der Ergebnisse rechtmäßiger Überwachungsmaßnahmen zu sorgen; dies schließt transparente Regeln zur Klassifizierung und Deklassifizierung ein;
5. sicherzustellen, dass jeder betroffene Mensch unabhängig von seiner Nationalität das Recht auf nachträgliche Benachrichtigung, auf Löschung oder Korrektur seiner Daten und auf Zugang zu den Gerichten hat;
6. den Bürgerinnen und Bürgern zu gestatten, dass sie frei Werkzeuge zur sicheren Kommunikation erforschen, schaffen, verteilen und nutzen, und sie dazu zu ermutigen; kein Bürger und keine Bürgerin sollte allein deshalb überwacht werden, weil er oder sie solche Werkzeuge nutzt;

[6] The White House, Fact Sheet, President Xi Jinping State Visit, 25. September 2015; verfügbar unter: https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

7. eine effektive und unabhängige Kontrolle von Überwachungstätigkeiten sicherzustellen, die von der Polizei, Nachrichtendiensten oder in ihrem Auftrag von privaten Datenverarbeitern durchgeführt werden.[7]

Ebenfalls im Jahr 2013 rief die Internationale Konferenz der Datenschutzbeauftragten Regierungen dazu auf, sich für die Aufnahme eines Zusatzprotokolls zu Artikel 17 des „International Convenant on Civil and Political Rights (ICCPR)“ einzusetzen.[8]

Einsatz von Technologie durch Nachrichtendienste

Bei der ersten Sitzung des „Internationalen Forums zur Kontrolle von Nachrichtendiensten“ (International Intelligence Oversight Forum, IIOF) im Jahr 2016, welches von dem UN-Sonderberichterstatter zum Recht auf Privatsphäre veranstaltet wurde, wurde der Schluss gezogen, dass viele Themen im Zusammenhang mit dem Einsatz von Technologien durch Nachrichtendienste entstehen. Diese umfassen z. B. den Bedarf an standardisierten Begrifflichkeiten und Formulierungen, die Notwendigkeit eines vertraulichen und offenen Dialogs für ein besseres Verständnis nationaler Systeme, ihrer Gemeinsamkeiten und ihrer Unterschiede (einschließlich der Benennung vorbildlicher und unangebrachter Praktiken), den Bedarf an einer anspruchsvolleren und offeneren Diskussion über die Arbeit von Nachrichtendiensten und Möglichkeiten für deren effektive Kontrolle und die Notwendigkeit von Garantien und Rechtsbehelfen – idealerweise auf internationaler Ebene (einschließlich Rechenschaftspflicht und Transparenz). Das nächste IIOF Ende 2017 soll auf diesen Erkenntnissen aufbauen.

Forschung

Die aktuellen Entwicklungen haben auch diverse Forschungsinitiativen auf den Plan gerufen. Die Agentur der Europäischen Union für Grundrechte (FRA) beispielsweise hat auf Anfrage des Europäischen Parlaments begonnen zu untersuchen, wie die Gesetze zu nationalen Nachrichtendiensten in sieben Mitgliedstaaten implementiert sind: Belgien, Deutschland, Italien, Frankreich, die Niederlande, Schweden und das Vereinigte Königreich.[9] Die Bestandsaufnahme der Rechtsrahmen wurde 2015 veröffentlicht und soll im Oktober 2017 durch einen Bericht ergänzt werden, der eine Analyse der betreffenden Gesetze sowie deren praktische Umsetzung beinhalten und auf Möglichkeiten für einen besseren Schutz der Grundrechte einschließlich des Rechts auf Privatsphäre eingehen wird.[10]

Aufbauend auf Forschungsvorhaben der Universität von Groningen begann der UN-Sonderberichterstatter im Jahr 2016, sich dem sog. MAPPING-Projekt[11] zu widmen, in dessen

[7] „Arbeitspapier zum Recht auf vertrauliche Telekommunikation“, 2013; https://datenschutz-berlin.de/attachments/993/WP_Human_Right.pdf?1382357419

[8] „Resolution on anchoring data protection and the protection of privacy in international law“, Warschau, 2013; https://icdppc.org/wp-content/uploads/2015/02/International-law-resolution.pdf

[9] Siehe http://fra.europa.eu/en/project/2014/national-intelligence-authorities-and-surveillance-eu-fundamental-rights-safeguards-and

[10] FRA: „*National intelligence authorities and surveillance in the EU: Fundamental rights, safeguards and remedies“;* http://fra.europa.eu/en/project/2014/national-intelligence-authorities-and-surveillance-eu-fundamental-rights-safeguards-and

[11] Das Akronym “MAPPING” steht für „Managing Alternatives for Privacy, Property and Internet Governance“. Das Projekt wird gemäß Zuschussvereinbarung Nr. 612345 über das 7. EU-

Rahmen untersucht werden soll, ob es möglich ist, ein spezielles Rechtsinstrument für die Überwachungsaktivitäten von Regierungsbehörden zu entwickeln (sowohl für Strafverfolgungsbehörden als auch Nachrichtendienste). Die Arbeit an diesem Projekt wird auch im Jahr 2018 weiter fortgeführt.

Nationale Initiativen

Auf nationaler Ebene werden neue Gesetze in Bezug auf nachrichtendienstliche Tätigkeiten erlassen, die auch Grundsätze für die Kontrolle derartiger Aktivitäten umfassen. In den USA hat der CIA (Central Intelligence Agency) beispielsweise Grundsätze für die Fernmeldeaufklärung (Signals Intelligence) aufgestellt , die mit Presidential Policy Directive 28: Signals Intelligence Activities[12].[13] einhergehen. In Neuseeland wurde ein neues Gesetz verabschiedet, um die Aktivitäten von Nachrichtendiensten transparenter zu machen und Kontrollmaßnahmen zu modernisieren.[14]

Zivilgesellschaft und private Initiativen

Zivilgesellschaftliche Gruppen aus aller Welt haben Bedenken bezüglich des rechtlichen Rahmens für den Datenschutz im Zusammenhang mit elektronischer Kommunikation geäußert. Der Bericht „The Web Index" von 2014 kam zu dem Ergebnis, dass 83 Prozent der Länder über schwachen oder unzureichenden Daten- und Privatsphärenschutz verfügen, einschließlich mangelnder Transparenz in Bezug auf Art und Umfang strafverfolgungsbehördlicher und nachrichtendienstlicher Überwachung und mangelnden Schutzes elektronischer Kommunikation.[15] Es waren unter anderem diese Zweifel, die von Multi-Stakeholder- und zivilgesellschaftlichen Initiativen zu Forderungen nach Chartas für digitale Rechte geführt haben. Als solche ist z. B. die „Internet Charter of Rights and Freedoms" zu nennen, ein Produkt des „Internet Governance Forums" der Vereinten Nationen.[16] Alle diese Initiativen äußerten, mal mehr, mal weniger konkret, Bedenken gegenüber den Aktivitäten von Nachrichtendiensten und verlangten mehr Klarheit über die Pflichten der Regierungen in Bezug auf geheimdienstliche Tätigkeiten.[17] Erst kürzlich forderte die Web Foundation, Herausgeber des Web Index, eine Grundrechtecharta für das Internet, welche einen internationalen Konsens über Kernprinzipien der internetbezogenen Regulierung herstellen sollte.[18]

Die Privatwirtschaft äußert weiterhin Bedenken gegen ihre rechtlichen Verpflichtungen im Hinblick auf Anforderungen der Nachrichtendienste und im Hinblick auf ihre Pflichten, im Zusammenhang mit Cyberbedrohungen Maßnahmen zu ergreifen. Der private Sektor unterstützt deshalb Initiativen, die nach neuen internationalen Vereinbarungen in diesem Bereich verlangen. Anfang 2017 entfachte Microsoft Inc. eine erneute Debatte über ein internationales für die Regierungen verbindliches Abkommen und forderte eine „Digitale Genfer Konvention", die Gegenmaßnahmen für staatlich

---

Forschungsrahmenprogramm für Forschung, technologische Entwicklung und Demonstration finanziert. Mehr Informationen unter: https://mappingtheinternet.eu/

[12] https://www.cia.gov/library/reports/Policy-and-Procedures-for-CIA-Signals-Intelligence-Activities.pdf

[13] http://www.globalsecurity.org/intell/library/policy/national/ppd-28_signals-intelligence-activities_140117.htm

[14] Siehe beispielsweise New Zealand Intelligence and Security Act 2017.

[15] „The Web Index" (2014), http://thewebindex.org/report/#6.1_privacy_and_surveillance

[16] Siehe „The Dynamic Coalition on Internet Rights and Principles", www.intgovforum.org

[17] Siehe z. B. Rodriguez K, „A Principled Fight Against Surveillance", Global Society Information Watch, (2014), Hivos and Association for Progressive Communications, 11.

[18] Siehe https://webwewant.org/news/category/internet-charters/

gestützte Cyberangriffe auf Zivilisten in Zeiten des Friedens regeln und Richtlinien für die Rolle von Technologieunternehmen bei der Reaktion auf derartige Angriffe festlegen sollte.[19] Es war auch die Rede von einer „neutralen digitalen Schweiz“ und einer unabhängigen Organisation nach dem Vorbild des Roten Kreuzes, die den öffentlichen und den privaten Sektor umfassen und für den Schutz von Zivilisten vor staatlich gestützten Cyberangriffen in Zeiten des Friedens sorgen soll.

Entstehende Debatte über neue Standards für nachrichtendienstliche Tätigkeiten

Es hat sich eine spezifische Diskussion darüber entwickelt, welche neuen Prinzipien speziell für Nachrichtendienste aufgestellt werden können. Einige dieser neuen Grundsätze wurden im Rahmen von Multi-Stakeholder-Prozessen entwickelt, wie etwa die „Tshwane-Prinzipien“ (weltweite Grundsätze zur Nationalen Sicherheit und dem Recht auf Informationen)[20] und die Internationalen Grundsätze für die Anwendung der Menschenrechte in der Kommunikationsüberwachung[21]). Andere beziehen sich speziell auf Datenschutzbehörden, z. B. die beiden Verlautbarungen in der Deklaration von Amsterdam zu den Themen genetische und gesundheitsbezogene Daten und die Herausforderungen von morgen (Genetic and Health Data, Challenges for Tomorrow) sowie Datenschutzkontrolle von Sicherheitsbehörden und Nachrichtendiensten (Data protection oversight of security and intelligence).[22] Weitere sind, wie oben bereits erwähnt, derzeit im Gespräch.

Die verschiedenen Initiativen unterscheiden sich in Tiefe und Umfang sehr stark, aber die Kernpunkte der Grundsätze sind im Wesentlichen dieselben: die Forderung nach Transparenz, Rechenschaftspflicht, Beachtung der Rechtsstaatlichkeit (mit klaren Ermächtigungsgrundlagen), Verhältnismäßigkeit, Datenvorhaltung und Kontrolle der Datennutzung, Nutzung von möglichst wenig in die Privatsphäre eingreifenden Datenerhebungsmethoden, angemessene Rechtsbehelfe, Whistleblower-Schutz, Objektivität, Integrität von Systemen und eine klarere Definition von nationaler Sicherheit, um den Umfang der Aktivitäten von Behörden zu steuern (z. B. um den Einsatz von Nachrichtendiensten für die Informationsbeschaffung zu wirtschaftlichen Zwecken auszuschließen).

Herausforderungen

Datenschutzbehörden stehen vor der Herausforderung, diese Entwicklungen zu überwachen und festzulegen, wie sie am besten auf sie reagieren können. Einige der Initiativen sind unbrauchbar, andere vielleicht konzeptionell verfehlt oder zu ehrgeizig. Es ist jedoch ein deutlicher Trend erkennbar: Der politische Diskurs über den staatlichen Zugriff auf Kommunikationsnetzwerke und -systeme zur Beschaffung von Inhalten und Metadaten der Bürger des eigenen Landes oder anderer Länder verschärft sich und diverse Gesichtspunkte dieses Themas werden in zahlreichen internationalen Foren diskutiert und untersucht. Ein Kernaspekt dieses Diskurses ist die

[19] Smith, B.: „The need for a digital convention”, Microsoft Inc., 14. Februar 2017; verfügbar unter: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.00001euw80bnrgexcs4mntuoy2nwn

[20] Open Justice Initiative: „The Global Principles on National Security and the Right to Information”; verfügbar unter: https://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles

[21] Verfügbar unter: https://necessaryandproportionate.org/principles

[22] Siehe „The role of Data Protection Authorities in a changing society“, 2015; https://icdppc.org/wp-content/uploads/2015/02/Amsterdam-Declaration-.pdf

Rechtmäßigkeit von Datenbeschaffungsaktivitäten, die Staaten durchführen, um ihren Verpflichtungen zum Schutz der nationalen Sicherheit und zum Schutz der Bürger nachzukommen.

Eine weitere Herausforderung ergibt sich durch die Einrahmung dieses besonderen Rechtsdiskurses. Der Bericht des UN-Sonderberichterstatters aus dem Jahr 2017 befasst sich z. B. mit zwei polarisierenden Ansichten, d. h. jenen, die jegliche Art von „Überwachung“ durch den Staat grundsätzlich negativ bewerten, und anderen Ansichten von Vertretern aus der Nachrichtendienstgemeinschaft, die die Verwendung des Begriffs „Überwachung“ im Zusammenhang mit ihren Aktivitäten nicht akzeptieren wollen. Sie lehnen es ab, dass die Speicherung von Telekommunikationsdaten oder Massendatensammlung mit Massenüberwachung oder überhaupt Überwachung gleichgesetzt wird.

Für solche Nachrichtendienste ist es schwierig, sich an Diskussionen über neue internationale Vereinbarungen zu beteiligen, da dies voraussetzt, dass sie derartige Bezeichnungen für ihre Tätigkeiten akzeptieren. Gleichzeitig lehnen diejenigen, die die Rechtmäßigkeit der Arbeit von Nachrichtendiensten insgesamt infrage stellen, Entwicklungen ab, die zu vermeintlichen Eingeständnissen führen, indem eine rechtliche Grundlage für solche Aktivitäten geschaffen oder „Überwachung“ als legitim angesehen werden könnte.

Ein solcher polemischer Disput lässt wenig Raum für die Ansichten anderer, einschließlich solcher von Entwicklungsländern. Diese Staaten haben unter Umständen berechtigte Bedenken wegen schwerwiegender Bedrohungen für die innere bzw. Grenz-Sicherheit, sodass aus ihrer Sicht die nachrichtendienstliche Informationsbeschaffung legitim ist. Dieselben Länder werden ggf. mit einem starken Verlangen seitens der Öffentlichkeit nach der Wahrung von Recht und Ordnung konfrontiert und sehen sich internationaler Kritik ausgesetzt, wenn es ihnen nicht gelingt, in ihrer Region für Sicherheit zu sorgen.

In Anbetracht dieser neuen Herausforderungen müssen sich Datenschutzbehörden überlegen, wie sie am besten reagieren können. Wir glauben, dass Datenschutzbehörden aufgrund ihrer Erfahrung und ihres Know-hows im Bereich der Datenregulierung sowie der Förderung und dem Schutz des Rechts auf Privatsphäre im Strafvollstreckungs- und Sicherheitskontext einen einmaligen und wichtigen Beitrag auf diesem noch recht jungen Gebiet leisten können. Sollen tatsächlich neue Grundsätze etabliert werden, ist es unerlässlich, dass Datenschutzbehörden die Diskussion mitgestalten und an der Entwicklung solcher Prinzipien mitwirken, die für nachrichtendienstliche Tätigkeiten gelten sollen.

Die nächsten Schritte

Die gegenwärtige Debatte über die Rechtmäßigkeit und die Umstände des Abfangens von Kommunikation – egal ob Sprachnachrichten, elektronische Daten oder andere Arten von Kommunikation – hat dazu geführt, dass ein zunehmender Konsens darüber besteht, dass es international vereinbarter Grundsätze für nachrichtendienstliche Tätigkeiten bedarf. Ein Katalog von Grundsätzen würde die Grundlage für die Rechenschaftspflicht in Bezug auf derartige Aktivitäten schaffen.

Ausgangspunkt für einen solchen Prinzipienkatalog könnte sein, dass staatliche Datenbeschaffungsaktivitäten zum Schutz der Sicherheit des Landes und einzelner Bürger legitim sind, solange sie gemäß internationalen Standards durchgeführt werden.

Fazit

Die Forderungen nach neuen internationalen Grundsätzen zur Verbesserung der Kontrolle von Nachrichtendiensten und deren Methoden zur Beschaffung von Informationen (einschließlich Telekommunikationsdaten) werden immer lauter. Für Datenschutzbehörden ist es keine leichte Aufgabe zu entscheiden, wie sie am besten reagieren und Unterstützung leisten können.

Letztlich glauben wir jedoch, dass Datenschutzbehörden mit ihrem Know-how und ihrer Erfahrung einen einzigartigen und wertvollen Beitrag zu der Ausarbeitung neuer Grundsätze leisten können.

Empfehlungen

Die Arbeitsgruppe empfiehlt, dass Datenschutzbehörden im Rahmen ihrer Kompetenzen:

(a) Initiativen zur Identifizierung, zur Entwicklung und zum Austausch von Best Practices in Bezug auf die Lenkung und Kontrolle der Tätigkeiten von Nachrichtendiensten unterstützen
(b) an der entstehenden Debatte über Grundsätze teilnehmen, die für nachrichtendienstliche Tätigkeiten gelten sollten
(c) folgende Prinzipien beachten und fördern, wenn sie sich an der Diskussion beteiligen:

Legitimität: Alle Staaten sind berechtigt, sich für die Sicherheit des Landes und der Bürger einzusetzen, und wenn sie zu diesem Zweck Nachrichtendienste beauftragen, haben diese ihre Tätigkeiten gemäß dem Prinzip der Rechtsstaatlichkeit auszuführen.

Rechtsstaatlichkeit: Nachrichtendienste müssen auf Grundlage eines klaren gesetzlichen Mandats und Ermächtigungsrechtsrahmens agieren, der die Beachtung aller Menschenrechte, den Schutz des Rechts auf Privatsphäre, Objektivität und das Recht auf angemessenen Rechtsschutz gegen die Handlungen dieser Behörden einbezieht.

Prüfung: Die Tätigkeiten von Nachrichtendiensten müssen einem gründlichen Vorabgenehmigungsprozess sowie einer nachträglichen Prüfung unterzogen werden.

Verhältnismäßigkeit, Erforderlichkeit und möglichst geringer Eingriff in die Privatsphäre: Die Befugnisse der Nachrichtendienste zur Erhebung personenbezogener Daten müssen auf das absolut notwendige Maß beschränkt werden. Zudem sind Erhebungsmethoden anzuwenden, die mit dem geringsten Eingriff in die Privatsphäre verbunden sind.

Aufbewahrung von Daten und Nutzung: Datenschutzregeln wie die Rechte auf Datenminimierung, Löschung und Berichtigung sollten für die Aufbewahrung und Nutzung personenbezogener Daten durch Nachrichtendienste gelten. Diese Rechte sollten nur solchen gesetzlich zulässigen Beschränkungen unterliegen, die in einer demokratischen Gesellschaft notwendig sind.

Rechenschaftspflicht und Transparenz: Für Nachrichtendienste sollten klare, öffentlich zugängliche Rechenschaftspflichtverfahren bestehen (einschließlich der Verfahren, sich gegenüber der Judikative, Exekutive und Legislative zu verantworten) und regelmäßig über ihre Aktivitäten Bericht erstatten.

Kontrolle: Die Arbeit der Nachrichtendienste muss der effektiven Kontrolle durch unabhängige Stellen unterliegen.