Redigierte Vorabfassung

Verteilung: Allgemein
30. Juni 2014
Deutsch
Original: Englisch

Menschenrechtsrat
Siebenundzwanzigste Tagung
Tagesordnungspunkte 2 und 3
Jahresbericht der Hohen Kommissarin der Vereinten Nationen für Menschenrechte und Berichte des Amtes des Hohen Kommissars und des Generalsekretärs

Förderung und Schutz aller Menschenrechte, der bürgerlichen, politischen, wirtschaftlichen, sozialen und kulturellen Rechte, einschließlich des Rechts auf Entwicklung

Das Recht auf Privatheit im digitalen Zeitalter

Bericht des Amtes des Hohen Kommissars der Vereinten Nationen für Menschenrechte

Zusammenfassung

In ihrer Resolution 68/167 ersuchte die Generalversammlung die Hohe Kommissarin der Vereinten Nationen für Menschenrechte, dem Menschenrechtsrat auf seiner siebenundzwanzigsten Tagung und der Generalversammlung auf ihrer neunundsechzigsten Tagung einen Bericht über den Schutz und die Förderung des Rechts auf Privatheit im Kontext des innerstaatlichen und extraterritorialen Überwachens und/oder Abfangens von digitaler Kommunikation und Sammelns personenbezogener Daten, namentlich in massivem Umfang, samt Auffassungen und Empfehlungen zur Prüfung durch die Mitgliedstaaten vorzulegen. Diesem Ersuchen wird mit dem vorliegenden Bericht entsprochen. Das Amt des Hohen Kommissars wird den Bericht auch der Generalversammlung auf ihrer neunundsechzigsten Tagung vorlegen, gemäß dem Ersuchen der Versammlung.

Inhalt

I. Einleitung

1. Digitale Kommunikationstechnologien wie das Internet, Smartphones und WiFi-fähige Geräte sind heute Teil des täglichen Lebens. Die Innovationen der Kommunikationstechnologie haben durch die enorme Verbesserung des Zugangs zu Informationen und Kommunikation in Echtzeit das Recht der freien Meinungsäußerung gestärkt, die weltweite Debatte erleichtert und die demokratische Teilhabe gefördert. Diese leistungsstarken Technologien, die die Stimme von Menschenrechtsverteidigern verstärken und ihnen neue Instrumente zur Dokumentierung und Aufdeckung von Missbräuchen an die Hand geben, versprechen Verbesserungen beim Genuss der Menschenrechte. Da sich heute ein immer größerer Teil des Lebens online abspielt, ist das Internet nicht nur allgegenwärtig, sondern erfasst auch immer intimere Lebensbereiche.

2. Im digitalen Zeitalter verstärken die Kommunikationstechnologien auch die Fähigkeit von Regierungen, Wirtschaftsunternehmen und Personen, Daten zu überwachen, abzufangen und zu sammeln. Wie der Sonderberichterstatter über die Förderung und den Schutz der Meinungsfreiheit und des Rechts auf freie Meinungsäußerung feststellte, führen die technologischen Fortschritte dazu, dass der Effektivität der Durchführung staatlicher Überwachungsmaßnahmen durch Aspekte wie Umfang oder Zeitdauer keine Grenzen mehr gesetzt sind. Die sinkenden Kosten für Technologie und Datenspeicherung haben finanzielle oder praktische Erschwernisse für die Durchführung von Überwachungsmaßnahmen beseitigt. Der Staat verfügt heute über größere Fähigkeiten als je zuvor, gleichzeitige, invasive, gezielte und ausgedehnte Überwachungsmaßnahmen durchzuführen.[1] Mit anderen Worten, die technologischen Plattformen, auf die sich das politische, wirtschaftliche und soziale Leben weltweit zunehmend stützt, sind nicht nur anfällig für Massenüberwachung, sondern fördern diese vielleicht sogar.

3. Die Aufdeckung von Politiken und Praktiken, die sich die Anfälligkeit der digitalen Kommunikationstechnologien für elektronisches Überwachen und Abfangen zunutze machen, in Ländern auf der ganzen Welt wird mit tiefer Besorgnis registriert. Die Beispiele für offene und verdeckte digitale Überwachung in Staaten rund um die Welt werden immer zahlreicher, und staatliche Massenüberwachung wird immer mehr zu einer gefährlichen Gewohnheit, anstatt eine außergewöhnliche Maßnahme zu bleiben. Es liegen Berichte vor, wonach Regierungen gedroht haben, die Dienste von Telekommunikations- und Mobilfunkunternehmen zu verbieten, falls ihnen kein direkter Zugang zum Kommunikationsverkehr ermöglicht wird, dass sie Glasfaserkabel zu Überwachungszwecken angezapft und von Unternehmen systematisch verlangt haben, Masseninformationen über Kunden und Mitarbeiter offenzulegen. Einige Regierungen sollen die Überwachung von Telekommunikationsnetzen gezielt gegen Mitglieder der politischen Opposition und/oder politische Dissidenten genutzt haben. In einigen Staaten werden Berichten zufolge routinemäßig alle Telefongespräche aufgezeichnet und zu Analysezwecken auf Vorrat gespeichert; Gaststaaten globaler Veranstaltungen sollen die dabei stattfindende Kommunikation überwacht haben. Die Behörden eines bestimmten Staates sollen es zur Auflage gemacht haben, dass alle in dem Land verkauften Personalcomputer mit einer Filter-Software ausgestattet werden, die zusätzliche Überwachungsfunktionen enthalten könnte. Selbst über nichtstaatliche Gruppen wird berichtet, dass sie raffinierte digitale Überwachungskapazitäten entwickeln. Die Technologien für Massenüberwachung sind auf dem Weltmarkt angekommen, mit dem einhergehenden erhöhten Risiko, dass sich digitale Überwachungsaktivitäten der staatlichen Kontrolle entziehen.

4. Die Besorgnis hat sich noch verstärkt, nachdem 2013 und 2014 enthüllt wurde, dass die National Security Agency (NSA) in den Vereinigten Staaten von Amerika und das Government Communications Headquarters (GCHQ) im Vereinigten Königreich von Großbritannien und Nordirland zusammen offenbar Technologien entwickelt haben, die den Zugang zu einem gro-

[1] A/HRC/23/40, Ziff. 33.

ßen Teil des weltweiten Internetverkehrs, zu Anrufdaten in den Vereinigten Staaten, zu den elektronischen Adressverzeichnissen von Einzelpersonen und zu riesigen Mengen anderer digitaler Kommunikationsinhalte ermöglichen. Laut Berichten werden diese Technologien im Rahmen eines transnationalen Netzwerks eingesetzt, das sich auf strategische nachrichtendienstliche Verbindungen zwischen Regierungen, regulatorische Kontrollen privater Unternehmen und kommerzielle Vertragsbeziehungen stützt.

5. Infolge der Besorgnisse der Mitgliedstaaten und anderer Interessenträger über die nachteiligen Auswirkungen dieser Überwachungspraktiken auf die Menschenrechte verabschiedete die Generalversammlung im Dezember 2013 ohne Abstimmung die Resolution 68/167 über das Recht auf Privatheit im digitalen Zeitalter. In dieser von 57 Mitgliedstaaten miteingebrachten Resolution erklärte die Versammlung, dass die gleichen Rechte, die Menschen offline haben, auch online geschützt werden müssen, und forderte alle Staaten auf, das Recht auf Privatheit bei der digitalen Kommunikation zu achten. Sie forderte die Staaten ferner auf, ihre Verfahren, Praktiken und Rechtsvorschriften betreffend die Überwachung von Kommunikation, ihr Abfangen und das Sammeln personenbezogener Daten zu überprüfen, und sie betonte, dass die Staaten die vollständige und wirksame Umsetzung ihrer Verpflichtungen nach den internationalen Menschenrechtsnormen sicherstellen müssen.

6. Außerdem ersuchte die Generalversammlung in Resolution 68/167 die Hohe Kommissarin der Vereinten Nationen für Menschenrechte, dem Menschenrechtsrat auf seiner siebenundzwanzigsten Tagung und der Generalversammlung auf ihrer neunundsechzigsten Tagung einen Bericht über den Schutz und die Förderung des Rechts auf Privatheit im Kontext des innerstaatlichen und extraterritorialen Überwachens und/oder Abfangens von digitaler Kommunikation und Sammelns personenbezogener Daten, namentlich in massivem Umfang, samt Auffassungen und Empfehlungen zur Prüfung durch die Mitgliedstaaten vorzulegen. Diesem Ersuchen wird mit dem vorliegenden Bericht entsprochen. Gemäß dem mit Resolution 68/167 erteilten Mandat wird das Amt des Hohen Kommissars den Bericht auch der Generalversammlung auf ihrer neunundsechzigsten Tagung vorlegen.

II. Hintergrund und Methodik

7. Eingedenk der Resolution 68/167 nahm das Amt des Hohen Kommissars an einer Reihe von Veranstaltungen teil und sammelte Informationen aus einer Vielzahl von Quellen. Am 24. Februar 2014 hielt die Hohe Kommissarin den Leitvortrag auf einem Sachverständigenseminar zum Thema „Das Recht auf Privatheit im digitalen Zeitalter“, das von Brasilien, Deutschland, Liechtenstein, Mexiko, Norwegen, Österreich und der Schweiz gemeinsam veranstaltet und von der Genfer Akademie für humanitäres Völkerrecht und Menschenrechte gefördert wurde.

8. Von November 2013 bis März 2014 führte die Universität der Vereinten Nationen im Auftrag des Amtes des Hohen Kommissars ein Forschungsprojekt durch, das die Anwendung der internationalen Menschenrechtsnormen auf die nationalen Aufsichtsregime für staatliche digitale Überwachung zum Gegenstand hatte. Das Amt des Hohen Kommissars ist der Universität dankbar und würdigt den wichtigen Sachbeitrag, den sie durch ihr Forschungsprojekt zur Ausarbeitung des vorliegenden Berichts geleistet hat.

9. Im Rahmen einer am 27. Februar 2014 abgehaltenen offenen Konsultation unterbreitete das Amt des Hohen Kommissars den Mitgliedstaaten über ihre Ständigen Vertretungen in Genf und New York, den internationalen und regionalen Organisationen, den nationalen Menschenrechtsinstitutionen, den nichtstaatlichen Organisationen sowie privatwirtschaftlichen Unternehmen einen Fragebogen. Darin erbat das Amt Beiträge zu den von der Generalversammlung in ihrer Resolution 68/167 behandelten Themen. Das Amt richtete eine spezielle Website ein, um den Fragebogen und alle Beiträge öffentlich zugänglich zu machen und weitere Beiträge zu ermöglichen. 29 Mitgliedstaaten aus allen Regionen, fünf internationale und/oder regionale Or-

ganisationen, drei nationale Menschenrechtsinstitutionen, 16 nichtstaatliche Organisationen und zwei privatwirtschaftliche Initiativen übermittelten Beiträge.[2]

10. Viele dieser Beiträge gingen ausführlich auf die bestehenden nationalen Rechtsrahmen und auf andere Maßnahmen zur Sicherung der Achtung und des Schutzes des Rechts auf Privatheit im digitalen Zeitalter sowie Initiativen zur Einrichtung und Anwendung von Verfahrungsgarantien und einer wirksamen Aufsicht ein. Manche Beiträge beschrieben Probleme, die bei der Umsetzung des Rechts auf Privatheit im digitalen Zeitalter auftreten, und enthielten Vorschläge für Initiativen auf internationaler Ebene. Vorgeschlagen wurden unter anderem eine Anregung an den Menschenrechtsausschuss, seine maßgeblichen Allgemeinen Bemerkungen, insbesondere zu Artikel 17 des Internationalen Paktes über bürgerliche und politische Rechte, zu aktualisieren, ferner die Einrichtung eines Mandats für ein Sonderverfahren zum Recht auf Privatheit durch den Menschenrechtsrat und/oder die Mitwirkung der Mandatsträger bestehender einschlägiger Sonderverfahren an gemeinsamen oder einzelnen Initiativen, die sich mit Fragen im Zusammenhang mit dem Recht auf Privatheit im Kontext der digitalen Überwachung befassen und Leitlinien für bewährte Verfahren erarbeiten.

11. Gemäß dem Ersuchen in Resolution 68/167 der Generalversammlung präsentiert dieser Bericht Überlegungen und Empfehlungen, die sich auf die Bewertung der zum Zeitpunkt seiner Abfassung verfügbaren Informationen stützen und außerdem das umfangreiche Material einbeziehen, das in dem breiten Spektrum der eingegangenen Beiträge enthalten ist.

III. Fragen im Zusammenhang mit dem Recht auf Privatheit im digitalen Zeitalter

12. Die Generalversammlung hat in ihrer Resolution 68/167 daran erinnert, dass die internationalen Menschenrechtsnormen den universellen Rahmen bilden, innerhalb dessen jeder Eingriff in das Recht des Einzelnen auf Privatheit zu bewerten ist. In Artikel 12 der Allgemeinen Erklärung der Menschenrechte heißt es: „Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.“ Artikel 17 des Internationalen Paktes über bürgerliche und politische Rechte, der bislang von 167 Staaten ratifiziert wurde, schreibt vor: „Niemand darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden.“ Ferner heißt es dort: „Jedermann hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.“

13. Andere internationale Menschenrechtsübereinkünfte enthalten ähnliche Bestimmungen. Rechtsvorschriften auf regionaler und nationaler Ebene berücksichtigen ebenfalls das Recht aller Menschen auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihres Schriftverkehrs oder auch das Recht auf Anerkennung und Achtung ihrer Würde, ihrer persönlichen Unversehrtheit oder ihres Rufes. Mit anderen Worten, die grundlegende Bedeutung und andauernde Relevanz des Rechts auf Privatheit und die Notwendigkeit, seinen Schutz im Gesetz und in der Praxis zu gewährleisten, werden allgemein anerkannt.

14. Wenngleich der Schwerpunkt des Mandats für diesen Bericht auf dem Recht auf Privatheit liegt, sollte unterstrichen werden, dass Massenüberwachung, das Abfangen digitaler Kommunikation und die Erhebung personenbezogener Daten auch andere Rechte beeinträchtigen können. Dazu gehören das Recht auf Meinungsfreiheit und freie Meinungsäußerung, das Recht, Informationen sich zu beschaffen, zu empfangen und weiterzugeben, das Recht, sich friedlich zu versammeln und zu Vereinigungen zusammenzuschließen, und das Recht auf Familienleben

[2] Alle Beiträge sind unter http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx abrufbar.

– alle diese Rechte hängen eng mit dem Recht auf Privatheit zusammen und werden zunehmend über digitale Medien ausgeübt. Andere Rechte, wie etwa das Recht auf Gesundheit, können ebenfalls durch Praktiken der digitalen Überwachung beeinträchtigt werden, wenn es beispielsweise eine Person aus Furcht vor einer Verletzung ihrer Anonymität unterlässt, sich sensible gesundheitsbezogene Informationen zu beschaffen oder sie weiterzugeben. Es liegen glaubwürdige Hinweise darauf vor, dass digitale Techniken für die Beschaffung von Informationen genutzt wurden, die in der Folge zu Folter und anderer Misshandlung führten. Ferner gibt es Berichte, wonach Metadaten aus elektronischer Überwachung analysiert wurden, um den Aufenthaltsort der Zielpersonen tödlicher Drohnenangriffe zu ermitteln. Solche Angriffe geben weiterhin zu schweren Bedenken Anlass, was die Einhaltung internationaler Menschenrechtsnormen und des humanitären Völkerrechts und die Rechenschaft für Verstöße angeht. Die Zusammenhänge zwischen Massenüberwachung und diesen anderen Auswirkungen auf die Menschenrechte überschreiten zwar den Rahmen dieses Berichts, verdienen jedoch eine weitere Untersuchung.

A. Das Recht auf Schutz vor willkürlichen oder rechtswidrigen Eingriffen in das Privatleben, die Familie, die Wohnung und den Schriftverkehr

15. Mehrere Beiträge hoben hervor, dass die Überwachung elektronischer Kommunikationsdaten, wenn sie in Übereinstimmung mit dem Gesetz, einschließlich der internationalen Menschenrechtsnormen, erfolgt, eine notwendige und wirksame Maßnahme zu legitimen Zwecken der Strafverfolgung oder nachrichtendienstlichen Zwecken darstellen kann. Die Enthüllungen über digitale Massenüberwachung werfen jedoch die Frage auf, inwieweit solche Maßnahmen mit den internationalen Rechtsnormen im Einklang stehen und ob es im Bereich der Überwachung stärkerer Schutzvorschriften gegen Verletzungen der Menschenrechte bedarf. Insbesondere dürfen Überwachungsmaßnahmen nicht dazu führen, dass der Einzelne willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr ausgesetzt wird. Die Regierungen müssen konkrete Maßnahmen ergreifen, um rechtlichen Schutz vor solchen Eingriffen zu gewährleisten.

16. Eine Durchsicht der eingegangenen Beiträge ergab, dass zur Behandlung dieser Fragen zunächst bewertet werden muss, was im Kontext der digitalen Kommunikation einen Eingriff in die Privatsphäre darstellt, was unter „willkürlich und rechtswidrig“ zu verstehen ist und wessen Rechte wo durch die internationalen Menschenrechtsnormen geschützt sind. Die folgenden Abschnitte behandeln Fragen, die in den verschiedenen Beiträgen in den Vordergrund gestellt wurden.

1. Eingriff in die Privatsphäre

17. Internationale und regionale Menschenrechtsvertragsorgane, Gerichte, Kommissionen und unabhängige Experten haben maßgebliche Leitlinien zum Umfang und Inhalt des Rechts auf Privatheit aufgestellt, die sich auch mit der Bedeutung des Begriffs „Eingriff“ in das Privatleben des einzelnen Menschen befassen. In seiner Allgemeinen Bemerkung Nr. 16 unterstrich der Menschenrechtsausschuss, dass es für die Einhaltung von Artikel 17 des Allgemeinen Paktes über bürgerliche und politische Rechte erforderlich ist, dass die Unversehrtheit und der vertrauliche Charakter des Schriftverkehrs rechtlich und faktisch gewährleistet sind. „Die Korrespondenz muss dem Adressaten, ohne abgefangen zu werden, ungeöffnet und ohne andere Art der Kenntnisnahme ihres Inhalts ausgehändigt werden“.[3]

18. Einige vertreten die Auffassung, dass die Weitergabe und der Austausch personenbezogener Informationen auf elektronischem Weg Teil eines bewusst eingegangenen Kompromisses

[3] *Official Records of the General Assembly, Forty-third Session, Supplement No. 40* (A/43/40), Anhang VI, Ziff. 8.

ist, bei dem der Einzelne als Gegenleistung für den digitalen Zugang zu Waren, Dienstleistungen und Informationen freiwillig Informationen über sich selbst und seine Verhältnisse preisgibt. Dies wirft jedoch ernsthafte Fragen danach auf, in welchem Ausmaß die Konsumenten sich tatsächlich bewusst sind, welche Daten sie wie und an wen weitergeben und wofür diese Daten genutzt werden. In einem der Berichte heißt es: „Es gehört zu der Realität von Massendaten, dass es sehr schwierig sein kann, einmal erhobene Daten anonym zu halten. Zwar gibt es vielversprechende Forschungsarbeiten dazu, wie persönlich identifizierbare Informationen innerhalb großer Datenbestände unkenntlich gemacht werden können, doch richten sich derzeit erheblich fortgeschrittenere Anstrengungen darauf, augenscheinlich „anonyme“ Daten wieder zuordenbar zu machen. Die kollektiven Investitionen in die Fähigkeit zur Datenfusion sind um ein Vielfaches höher als die Investitionen in Technologien, die die Privatsphäre stärken sollen.“ Die Autoren des Berichts stellten fest, dass „die Fokussierung auf die Kontrolle der Erhebung und Vorratsspeicherung personenbezogener Daten zwar wichtig ist, wahrscheinlich aber nicht mehr ausreicht, um die Privatsphäre des Einzelnen zu schützen“, zum Teil deshalb, weil „die enormen Datenmengen neue, nicht offensichtliche, unerwartet wirkungsvolle Formen der Datennutzung ermöglichen.“[4]

19. Eine ähnliche Auffassung lautete, dass das Abfangen oder Sammeln von Daten über eine Kommunikation, nicht aber des Inhalts der Kommunikation für sich allein noch keinen Eingriff in die Privatsphäre darstelle. Unter dem Blickwinkel des Rechts auf Privatheit ist diese Unterscheidung jedoch nicht überzeugend. Die Zusammenführung von üblicherweise als „Metadaten“ bezeichneten Informationen kann Einsichten in das Verhalten des Einzelnen, seine sozialen Beziehungen, privaten Präferenzen und seine Identität liefern, die sogar noch über das hinausgehen, was durch den Zugriff auf den Inhalt einer privaten Kommunikation offenbart wird. Wie der Europäische Gerichtshof vor kurzem feststellte, können „aus der Gesamtheit“ dieser Kommunikations-Metadaten „sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert wurden, gezogen werden.“[5] Die Erkenntnis dieser Entwicklung hat zu Initiativen geführt, die die bestehenden Politiken und Praktiken reformieren wollen, um einen stärkeren Schutz der Privatsphäre zu gewährleisten.

20. Daraus folgt, dass jede Erfassung von Kommunikationsdaten potenziell einen Eingriff in die Privatsphäre darstellt und dass des Weiteren die Sammlung und Vorratsspeicherung von Kommunikationsdaten einem Eingriff in die Privatsphäre gleichkommt, ungeachtet dessen, ob diese Daten in der Folge abgefragt oder genutzt werden. Sogar die bloße Möglichkeit der Erfassung von Kommunikationsinformationen bewirkt einen Eingriff in die Privatsphäre[6], der einen abschreckenden Effekt auf andere Rechte, namentlich die der freien Meinungsäußerung und der Vereinigungsfreiheit, ausüben kann. Daher stellt schon allein die Existenz eines Programms zur Massenüberwachung einen Eingriff in die Privatsphäre dar. Die Beweislast dafür, dass ein solcher Eingriff weder willkürlich noch rechtswidrig ist, würde beim Staat liegen.

2. Was ist „willkürlich“ oder „rechtswidrig“?

21. Eingriffe in das Recht eines Menschen auf Privatheit sind nach den internationalen Menschenrechtsnormen nur zulässig, wenn sie weder willkürlich noch rechtswidrig sind. In seiner Allgemeinen Bemerkung Nr. 16 erläuterte der Ausschuss, dass der Begriff „rechtswidrig“ be-

[4] Exekutivbüro des Präsidenten der Vereinigten Staaten, “Big Data: Seizing Opportunities, Preserving Values”, Mai 2014 (abrufbar unter http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf), S. 54.

[5] Gerichtshof der Europäischen Union, Urteil in den verbundenen Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland und Seitlinger u.a., Urteil vom 8. April 2014, Ziff. 26-27, und 37. Siehe auch Exekutivbüro des Präsidenten “Big Data and Privacy: A Technological Perspective” (abrufbar unter http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_may_2014.pdf), S. 19.

[6] Siehe Europäischer Gerichtshof für Menschenrechte, Weber und Saravia, Ziff. 78; Malone v. UK, Ziff. 64.

deutet, dass kein Eingriff stattfinden darf „außer in den vom Gesetz vorgesehenen Fällen. Die von Staaten erlaubten Eingriffe dürfen nur aufgrund eines Gesetzes erfolgen, welches seinerseits mit den Bestimmungen, Zwecken und Zielen des Paktes vereinbar ist.“[7] Mit anderen Worten, ein Eingriff, der nach dem innerstaatlichen Recht zulässig ist, kann dennoch „rechtswidrig“ sein, wenn die innerstaatlichen Rechtsvorschriften im Widerspruch zu den Bestimmungen des Internationalen Paktes über bürgerliche und politische Rechte stehen. Der Ausdruck „willkürlicher Eingriff“ kann sich auch auf vom Gesetz vorgesehene Fälle erstrecken. Der Ausschuss erläuterte, dass mit der Einführung dieses Konzepts „gewährleistet werden soll, dass auch ein gesetzlich vorgesehener Eingriff mit den Bestimmungen, Zwecken und Zielen des Paktes übereinstimmen und in jedem Fall angesichts der besonderen Umstände angemessen sein muss.“[8] Der Begriff der Angemessenheit wurde vom Ausschuss dahingehend ausgelegt, dass „jeder Eingriff in die Privatsphäre in Bezug auf das angestrebte Ziel verhältnismäßig und in Anbetracht der Umstände des jeweiligen Falles notwendig sein muss”.[9]

22. Im Gegensatz zu einigen anderen Bestimmungen des Paktes enthält Artikel 17 keine ausdrückliche Einschränkungsklausel. Orientierung zur Bedeutung der qualifizierenden Begriffe „willkürlich oder rechtswidrig“ findet sich jedoch in den Syrakus-Prinzipien zu Bestimmungen des Internationalen Paktes über bürgerliche und politische Rechte, die Einschränkungen oder die Außerkraftsetzung von Rechten zulassen[10], in der Praxis des Menschenrechtsausschusses, wie sie in seinen Allgemeinen Bemerkungen, namentlich den Nummern 16, 27, 29, 34, und 31, den Feststellungen zu Mitteilungen von Einzelpersonen[11] und den abschließenden Bemerkungen[12] ihren Niederschlag findet, in der regionalen und nationalen Rechtssprechung[13] sowie in den Auffassungen unabhängiger Experten[14]. In seiner Allgemeinen Bemerkung Nr. 31 über die Natur der den Vertragsstaaten des Paktes auferlegten allgemeinen rechtlichen Verpflichtung legt der Menschenrechtsausschuss beispielsweise fest, dass „die Vertragsstaaten Verletzungen der durch den Pakt anerkannten Rechte unterlassen müssen und dass jegliche Einschränkungen der Paktrechte nach den entsprechenden Bestimmungen des Paktes zulässig sein müssen. Soweit Einschränkungen gemacht werden, müssen die Staaten deren Notwendigkeit darlegen, und sie dürfen nur solche Maßnahmen ergreifen, die im Hinblick auf die Verfolgung legitimer Ziele verhältnismäßig sind, um den stetigen und effektiven Schutz der Paktrechte zu gewährleisten.“[15] Der Ausschuss unterstrich ferner: „In keinem Fall dürfen Einschränkungen derart angewendet oder geltend gemacht werden, dass sie den Wesensgehalt eines der Rechte aus dem Pakt berühren.”

23. Diese maßgebenden Quellen weisen auf die übergeordneten Grundsätze der Rechtmäßigkeit, der Notwendigkeit und der Verhältnismäßigkeit hin, deren Bedeutung auch in vielen der eingegangenen Beiträge hervorgehoben wurde. Zunächst muss jede Einschränkung des in

[7] *Official Records of the General Assembly* (siehe Fußnote 3), Ziff. 3.

[8] Ebd., Ziff. 4.

[9] Mitteilung Nr. 488/1992, Toonan v. Australien, Ziff. 8.3; siehe auch Mitteilungen Nr. 903/1999, Ziff. 7.3 und 1482/2006, Ziff. 10.1 und 10.2.

[10] Siehe E/CN.4/1985/4, Anlage.

[11] Zum Beispiel Mitteilung Nr. 903/1999, 2004, Van Hulst v. Niederlande.

[12] CCPR/C/USA/CO/4.

[13] Zum Beispiel Europäischer Gerichtshof für Menschenrechte, Uzun v. Deutschland, 2. September 2010, und Weber und Soravia v. Deutschland, Ziff. 4, und Interamerikanischer Gerichtshof für Menschenrechte, Escher v. Brasilien, Urteil , 20. Nov. 2009.

[14] Siehe A/HRC/13/37 und A/HRC/23/40. Siehe auch International Principles on the Application of Human Rights to Communications Surveillance, abrufbar unter https://en.necessaryandproportionate.org/text bzw. (deutsche Fassung von 2013) Internationale Grundsätze für die Anwendung der Menschenrechte in der Kommunikationsüberwachung, abrufbar unter https://de.necessaryandproportionate.org/text.

[15] CCPR/C/21/Rev.1/Add.13, Ziff. 6.

Artikel 17 umschriebenen Rechts auf Privatheit gesetzlich vorgesehen sein, und die entsprechenden Rechtsvorschriften müssen ausreichend zugänglich, klar und präzise sein, damit der Einzelne sich über ihren Inhalt informieren und feststellen kann, wer zur Durchführung einer Datenüberwachung autorisiert ist und unter welchen Umständen eine solche stattfinden kann. Die Einschränkung muss zur Erreichung eines legitimen Ziels notwendig und in Bezug auf das Ziel verhältnismäßig sein und den mildestmöglichen Eingriff darstellen.[16] Darüber hinaus muss nachgewiesen werden, dass die vorgenommene Einschränkung des Rechts auf Privatheit (zum Beispiel ein Eingriff zum Zweck des Schutzes der nationalen Sicherheit oder des Rechts auf Leben anderer Personen) eine gewisse Chance bietet, das angestrebte Ziel zu erreichen. Die Beweislast dafür, dass die Einschränkung mit einem legitimen Ziel verknüpft ist, liegt bei den Behörden, die das Recht einschränken möchten. Ferner darf eine Einschränkung des Rechts auf Privatheit nicht dazu führen, dass dieses Recht seinen Wesensgehalt verliert, und sie muss mit anderen Menschenrechten, einschließlich des Diskriminierungsverbots, vereinbar sein. Erfüllt eine Einschränkung diese Kriterien nicht, wäre sie rechtswidrig und/oder der Eingriff in das Recht auf Privatheit wäre willkürlich.

24. Staaten rechtfertigen Programme zur Überwachung der digitalen Kommunikation häufig mit dem Argument der nationalen Sicherheit, insbesondere der Terrorismusgefahr. Mehrere Beiträge wiesen darauf hin, dass die digitalen Kommunikationstechnologien für kriminelle Zwecke eingesetzt werden können und tatsächlich eingesetzt werden (namentlich zur Anwerbung für terroristische Handlungen, zu ihrer Finanzierung und zu ihrer Begehung) und dass deswegen die rechtmäßige, gezielte Überwachung der digitalen Kommunikation eine notwendige und wirksame Maßnahme der Nachrichtendienste und/oder der Strafverfolgungsbehörden darstellen kann, sofern sie in Übereinstimmung mit dem Völkerrecht und den innerstaatlichen Rechtsvorschriften durchgeführt wird. Für die Bewertung unter dem Blickwinkel des Artikels 17 des Paktes kann eine Überwachung aus Gründen der nationalen Sicherheit oder zur Verhütung von Terrorismus oder anderen Straftaten ein „legitimes Ziel“ darstellen. Der Umfang des Eingriffs muss jedoch gegenüber der Notwendigkeit der Maßnahme zur Erreichung des Ziels und dem für den Zweck tatsächlich erzielten Nutzen abgewogen werden.

25. Zur Bewertung der Notwendigkeit einer Maßnahme betonte der Menschenrechtsausschuss in seiner Allgemeinen Bemerkung Nr. 27 zu Artikel 12 des Internationalen Paktes über bürgerliche und politische Rechte, dass „die Einschränkungen nicht den Wesensgehalt des Rechts beeinträchtigen dürfen […], das Verhältnis von Recht und Beschränkung, von Norm und Ausnahme darf nicht umgekehrt werden.“[17] Der Ausschuss erläuterte weiter, „dass es nicht ausreichend ist, wenn die vorgesehenen Beschränkungen zulässigen Zwecken dienen; sie müssen vielmehr auch notwendig sein, um diese zu schützen.“ Darüber hinaus müssen solche Maßnahmen verhältnismäßig sein: „sie müssen das mildeste Mittel unter denen sein, die geeignet sind, das gewünschte Ergebnis zu erreichen”.[18] Sofern ein legitimes Ziel verfolgt wird und angemessene Garantien vorhanden sind, könnte es zulässig sein, dass ein Staat durchaus einschneidende Überwachungsmaßnahmen durchführt; die Beweislast dafür, dass der Eingriff sowohl notwendig als auch in Bezug auf die konkrete Gefahr, die abgewehrt werden soll, verhältnismäßig ist, liegt jedoch beim Staat. Programme zur Massenüberwachung können daher sogar dann als willkürlich angesehen werden, wenn sie einem legitimen Ziel dienen und auf der Grundlage zugänglicher Rechtsvorschriften beschlossen wurden. Mit anderen Worten, es genügt nicht, dass die Maßnahmen darauf ausgerichtet sind, die Stecknadel im Heuhaufen zu finden; die geeignete Richtschnur ist die Auswirkung der getroffenen Maßnahmen auf den Heuhaufen im Verhältnis zu dem drohenden Schaden, also die Notwendigkeit und Verhältnismäßigkeit der Maßnahme.

[16] CCPR/C/21/Rev.1/Add.9, Ziff. 11-16. Siehe auch A/HRC/14/46, Anhang, Gute Praxis 20.

[17] CCPR/C/21/Rev.1/Add.9, Ziff. 11-16. Siehe auch Europäischer Gerichtshof für Menschenrechte, Handyside v. Vereinigtes Königreich, Ziff.48; und Klass v. Deutschland, Ziff. 42.

[18] CCPR/C/21/Rev.1./Add.9, Ziff. 11-16.

26. Besorgnisse darüber, ob der Zugang zu Daten und ihre Nutzung auf spezifische legitime Ziele zugeschnitten sind, werfen auch Fragen zu der Praxis der Staaten auf, sich zunehmend auf Akteure des Privatsektors zu stützen, die Daten auf Vorrat speichern, „nur für den Fall", dass sie zu staatlichen Zwecken benötigt werden. Die verpflichtende Vorratsdatenspeicherung durch Dritte – ein häufiger Bestandteil von Überwachungsregimen in vielen Staaten, in denen Regierungen den Telefongesellschaften und Internetanbietern vorschreiben, Metadaten über den Kommunikationsverkehr und den Standort ihrer Kunden für einen späteren Zugriff durch Strafverfolgungsbehörden und Nachrichtendienste zu speichern – erscheint weder notwendig noch verhältnismäßig.[19]

27. Einer der Faktoren, die bei der Bewertung der Verhältnismäßigkeit zu beachten sind, ist die Frage, was mit den Massendaten geschieht und wer zu ihnen Zugang hat, nachdem sie einmal erfasst wurden. In vielen Ländern sehen die rechtlichen Rahmenbedingungen keine „Nutzungseinschränkungen" vor, sondern lassen das Sammeln von Daten für ein bestimmtes legitimes Ziel zu, wobei die Daten in der Folge auch für andere Ziele genutzt werden können. Das Fehlen wirksamer Nutzungseinschränkungen macht sich seit dem 11. September 2011 verschärft bemerkbar, da die Trennlinie zwischen Strafgerichtsbarkeit und Schutz der nationalen Sicherheit stark verwischt wurde. Es besteht daher die Gefahr, dass der resultierende Datenaustausch zwischen Strafverfolgungsbehörden, Nachrichtendiensten und anderen staatlichen Organen gegen Artikel 17 des Paktes verstößt, weil Überwachungsmaßnahmen zwar für ein bestimmtes legitimes Ziel notwendig und verhältnismäßig sein können, dies für andere Zwecke aber möglicherweise nicht mehr gilt. Eine Überprüfung der Praxis einzelner Länder hinsichtlich des staatlichen Zugriffs auf Daten Dritter kam zu folgendem Schluss: „Das Zusammentreffen von Faktoren wie der erhöhten Leichtigkeit des Zugriffs von nationalen Sicherheitsbehörden und Strafverfolgungsbehörden auf Daten des privaten Sektors und der zunehmenden Freiheit zum Austausch dieser Informationen zwischen diesen Stellen und zu ihrer Nutzung für andere Zwecke als ursprünglich vorgesehen bedeutet eine erhebliche Schwächung des traditionellen Datenschutzes."[20] In mehreren Staaten wurden auf dieser Grundlage Datenaustauschregelungen nach einer gerichtlichen Überprüfung aufgehoben. Andere vertreten die Meinung, dass solche Nutzungseinschränkungen, verbunden mit sinnvollen Sanktionen für Verstöße, eine gute Praxis darstellen, um die wirksame Erfüllung der Verpflichtungen eines Staates nach Artikel 17 des Paktes zu gewährleisten[21].

B. Rechtlicher Schutz

28. Artikel 17 Absatz 2 des Internationalen Paktes über bürgerliche und politische Rechte legt ausdrücklich fest, dass jedermann Anspruch auf rechtlichen Schutz gegen willkürliche oder rechtswidrige Eingriffe in sein Privatleben hat. Dies bedeutet, dass jedes Programm zur Kommunikationsüberwachung auf der Grundlage eines öffentlich zugänglichen Gesetzes durchgeführt werden muss, das seinerseits mit der Verfassungsordnung des betreffenden Staates und den internationalen Menschenrechtsnormen im Einklang stehen muss.[22] „Zugänglichkeit" erfordert nicht nur, dass das Gesetz veröffentlicht wurde, sondern dass es so präzise formuliert ist,

[19] Siehe Schlussantrag des Generalanwalts Cruz Villalón des Gerichtshofs der Europäischen Union in den verbundenen Strafsachen C-293/12 und C-594/12, der die Auffassung vertritt, dass die Richtlinie 2006/24/EU (über die Vorratsspeicherung von Daten, die bei der Bereitstellung elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden) „in ihrer Gesamtheit" gegen die Charta der Grundrechte der Europäischen Union verstößt, weil sie keine strengen Beschränkungen für diese Vorratsdatenspeicherung vorschreibt. Siehe auch CCPR/C/USA/CO/4, Ziff. 22.

[20] Fred H. Cate, James X. Dempsey und Ira S. Rubinstein, "Systematic government access to private – sector data", *International Data Privacy Law*, Vol. 2, Nr. 4, 2012, S. 198.

[21] Siehe A/HRC/14/46, Anhang, Gute Praxis 23.

[22] Siehe ebd., Anhang.

dass eine betroffene Person in der Lage ist, ihr Verhalten danach auszurichten und die Folgen eines bestimmten Handelns abzusehen. Der Staat muss sicherstellen, dass jeder Eingriff in das Recht auf Privatleben, Familie, Wohnung oder Schriftverkehr auf Gesetzen beruht, die a) öffentlich zugänglich sind, b) Bestimmungen enthalten, die sicherstellen, dass die Erhebung von Kommunikationsdaten, der Zugang zu diesen Daten und ihre Nutzung auf spezifische legitime Ziele zugeschnitten sind, c) ausreichend präzise sind und im Einzelnen festlegen, unter welchen genauen Umständen ein Eingriff zulässig sein kann, welche Genehmigungsverfahren dafür erforderlich sind, welche Kategorien von Personen überwacht werden können, welche zeitliche Begrenzung für die Dauer der Überwachungsmaßnahmen besteht und welche Verfahren für die Nutzung und Speicherung der erfassten Daten gelten, und d) wirksame Garantien gegen Missbrauch vorsehen.[23]

29. Geheime Vorschriften und geheime Auslegungen – selbst geheime gerichtliche Auslegungen – erfüllen daher nicht die Merkmale eines „Gesetzes“.[24] Dies ist auch nicht der Fall bei Gesetzen oder Vorschriften, die Exekutivbehörden, also etwa den Sicherheits- und Nachrichtendiensten, einen übermäßigen Ermessenspielraum einräumen; der Umfang und die Art und Weise der Ausübung des behördlichen Ermessensspielraums müssen (im Gesetzestext selbst oder in verbindlichen, veröffentlichten Leitlinien) mit hinreichender Klarheit bestimmt sein. Ein Gesetz, das zugänglich ist, dessen Wirkungen jedoch nicht absehbar sind, ist nicht angemessen. Der geheime Charakter spezifischer Überwachungsbefugnisse bringt ein erhöhtes Risiko mit sich, dass Ermessen willkürlich ausgeübt wird, woraus sich wiederum die Notwendigkeit größerer Präzision der Regeln für die Ermessensausübung sowie zusätzlicher Aufsicht ergibt. Mehrere Staaten schreiben außerdem vor, dass der rechtliche Rahmen durch Primärrecht festgelegt wird, das Gegenstand parlamentarischer Beratung war, und nicht einfach durch subsidiäre, von der Exekutive erlassene Verordnungen – ein Erfordernis, das dazu beiträgt, dass der rechtliche Rahmen für die betroffene Öffentlichkeit nicht erst nach seiner Verabschiedung, sondern schon im Verlauf seiner Ausarbeitung zugänglich ist, entsprechend Artikel 25 des Internationalen Paktes über bürgerliche und politische Rechte.[25]

30. Das Erfordernis der Zugänglichkeit ist auch für die Bewertung der sich herausbildenden Praxis der Staaten, Überwachungsaufgaben an Dritte auszulagern, von Relevanz. Glaubwürdige Informationen deuten darauf hin, dass manche Regierungen die Erhebung und Analyse von Daten systematisch in Staaten vornehmen lassen, in denen die Vorschriften zum Schutz der Privatsphäre weniger streng sind. Berichten zufolge unterhalten einige Regierungen ein transnationales Netz von Nachrichtendiensten unter Ausnutzung ineinandergreifender Rechtslücken, verbunden mit der Koordinierung von Überwachungspraktiken zu dem Zweck, innerstaatliche Schutzvorschriften zu umgehen. Eine solche Praxis wird einer Rechtmäßigkeitsprüfung möglicherweise nicht standhalten, weil durch sie, wie in einigen Beiträgen zu diesem Bericht unterstrichen wurde, die Arbeitsweise der Überwachungssysteme für diejenigen, die davon betroffen sind, nicht mehr vorhersehbar ist. Sie wird möglicherweise den Wesensgehalt des durch Artikel 17 des Internationalen Paktes über bürgerliche und politische Rechte geschützten Rechtes untergraben und wäre daher aufgrund von Artikel 5 des Paktes verboten. Manche Staaten haben es außerdem unter Verstoß gegen ihre eigenen Menschenrechtsverpflichtungen versäumt, wirksame Maßnahmen zum Schutz von Personen in ihrem Hoheitsbereich vor illegalen Überwachungspraktiken anderer Staaten oder von Wirtschaftsunternehmen zu ergreifen.

---

[23] CCPR/C/USA/CO/4, Ziff. 22. Siehe auch Europäischer Gerichtshof für Menschenrechte, Malone v. Vereinigtes Königreich, Nr. 8691/79, 2. August 1984, Ziff. 67 und 68; und Weber und Saravia v. Deutschland, Klageschrift Nr. 54934/00, 29. Juni 2006, in der der Gerichtshof die gesetzlich festzulegenden Mindestgarantien aufführt.

[24] Siehe CCPR/C/USA/CO/4, Ziff. 22.

[25] Siehe auch A/HRC/14/46.

C. Wer ist wo geschützt?

31. Mehrere der eingegangenen Beiträge befassten sich mit der extraterritorialen Anwendung des Internationalen Paktes über bürgerliche und politische Rechte auf die digitale Überwachung. Während klar ist, dass beispielsweise bestimmte Aspekte der vor kurzem enthüllten Überwachungsprogramme sich auf die Verpflichtungen der die Überwachung durchführenden Staaten im eigenen Hoheitsgebiet auswirken werden, wurden zusätzliche Besorgnisse in Bezug auf die Überwachung und das Abfangen von Kommunikation außerhalb des eigenen Hoheitsgebiets geäußert.

32. In Artikel 2 des Internationalen Paktes über bürgerliche und politische Rechte wird jeder Vertragsstaat dazu verpflichtet, die in dem Pakt anerkannten Rechte zu achten und sie allen in seinem Gebiet befindlichen und seiner Herrschaftsgewalt unterstehenden Personen ohne Unterschied wie insbesondere der Rasse, der Hautfarbe, des Geschlechts, der Sprache, der Religion, der politischen oder sonstigen Anschauung, der nationalen oder sozialen Herkunft, des Vermögens, der Geburt oder des sonstigen Status zu gewährleisten. Der Menschenrechtsausschuss erklärte in seiner Allgemeinen Bemerkung Nr. 31, dass in Artikel 2 Absatz 1 „von den Vertragsstaaten verlangt wird, die Paktrechte zu achten und sie allen in ihrem Gebiet befindlichen und ihrer Herrschaftsgewalt unterstehenden Personen zu gewährleisten. Dies bedeutet, dass ein Vertragsstaat die im Pakt niedergelegten Rechte achten und sie jeder Person, die seiner Gewalt oder tatsächlichen Kontrolle unterliegt, gewährleisten muss, auch wenn sie sich nicht im Gebiet des Vertragsstaats befindet.“[26] Dies erstreckt sich auch auf Personen, die sich im „Zuständigkeitsbereich“ der Vertragsstaaten befinden.[27]

33. Der Menschenrechtsausschuss hat sich von dem schon in seinen frühesten Entscheidungen geäußerten Grundsatz leiten lassen, dass ein Staat sich seinen Verpflichtungen auf dem Gebiet der internationalen Menschenrechte nicht entziehen kann, indem er außerhalb seines Hoheitsgebiets Maßnahmen vornimmt, die ihm „im eigenen Land“ untersagt wären.[28] Diese Position stimmt überein mit den Auffassungen des Internationalen Gerichtshofs, der erklärt hat, dass der Internationale Pakt über bürgerliche und politische Rechte auf Handlungen anwendbar ist, die ein Staat „in Ausübung seiner Herrschaftsgewalt außerhalb seines eigenen Hoheitsgebiets“ unternimmt[29], sowie mit den Artikeln 31 und 32 des Wiener Übereinkommens über das Recht der Verträge. Die Begriffe „Gewalt“ und „tatsächliche Kontrolle“ sind Indikatoren dafür, ob ein Staat „Herrschaftsgewalt“ oder hoheitliche Befugnisse ausübt, deren Missbrauch durch Vorschriften zum Schutz der Menschenrechte eingeschränkt werden soll. Ein Staat kann sich seinen menschenrechtlichen Verantwortlichkeiten nicht einfach dadurch entziehen, dass er es unterlässt, Befugnisse dieser Art rechtlich einzugrenzen. Ein anderer Schluss würde nicht nur die Universalität und den Wesensgehalt der durch die internationalen Menschenrechtsnormen geschützten Rechte untergraben, sondern möglicherweise auch strukturelle Anreize für Staaten schaffen, Überwachungsaktivitäten wechselseitig auszulagern.

34. Daraus folgt, dass digitale Überwachungsmaßnahmen die Menschenrechtsverpflichtungen eines Staates berühren können, wenn die Überwachung mit der Ausübung staatlicher Ge-

[26] CCPR/C/21/Rev.1/Add.13, Ziff. 10.

[27] Siehe *Official Records of the General Assembly, Thirty-sixth Session, Supplement No. 40* (A/36/40), Anhang XIX, Ziff. 12.2; siehe auch Anhang XX. Siehe auch CCPR/CO/78/ISR, Ziff. 11; CCPR/CO/72/NET, Ziff. 8; CCPR/CO/81/BEL, Ziff. 6; und Interamerikanische Menschenrechtskommission, Coard u.a. v. Vereinigte Staaten, Rechtssache Nr. 10.951, Bericht Nr. 109/99, 29. September 1999, Ziff. 37, 39, 41 und 43.

[28] Siehe *Official Records of the General Assembly, Thirty-sixth Session* (siehe Fußnote 27), Anhang XIX, Ziff. 12.2-12.3, und Anhang XX, Ziff. 10.3.

[29] Gutachten des Internationalen Gerichtshofs vom 9. Juli 2004, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (A/ES-10/273 und Corr.1), Ziff. 107-111. Siehe auch Internationaler Gerichtshof, Rechtssache *Armed Activities on the Territory of the Congo* (Demokratische Republik Kongo v. Uganda), Urteil, 2005, S. 168.

walt oder tatsächlicher Kontrolle in Bezug auf digitale Kommunikationsinfrastruktur, gleich wo sich diese befindet, durch den Staat verbunden ist, beispielsweise durch direktes Abhören oder durch Eindringen in diese Infrastruktur. Ebenso gilt, dass dort, wo der Staat Regulierungsbefugnisse gegenüber einem Dritten ausübt, der die Daten physisch kontrolliert, dieser Staat ebenfalls durch den Pakt auferlegte Verpflichtungen hätte. Wenn ein Land versucht, Hoheitsbefugnisse in Bezug auf die Daten privater Wirtschaftsunternehmen geltend zu machen, weil diese Unternehmen in dem betreffenden Land gegründet wurden, dann muss der Menschenrechtsschutz auch auf diejenigen ausgedehnt werden, in deren Privatsphäre eingegriffen wird, sei es im Gründungsstaat oder darüber hinaus. Dies gilt unabhängig davon, ob eine solche Ausübung von Hoheitsbefugnissen überhaupt rechtmäßig ist oder ob sie die Souveränität eines anderen Staates tatsächlich verletzt.

35. Dieser Schlussfolgerung kommt gleichermaßen Bedeutung zu in Anbetracht der aktuellen Diskussion darüber, ob „Ausländer“ und „Staatsangehörige” im Rahmen der Aufsichtsregime für die nationale Sicherheitsüberwachung gleichen Anspruch auf Schutz der Privatsphäre haben sollen. Mehrere Rechtsordnungen unterscheiden zwischen den Verpflichtungen gegenüber den eigenen Staatsangehörigen oder im Hoheitsgebiet des Staates befindlichen Personen und den Verpflichtungen gegenüber Nichtstaatsangehörigen und Personen außerhalb des eigenen Hoheitsgebiets[30] oder sehen anderweitig ein geringeres Schutzniveau für Auslands- bzw. externe Kommunikation vor. Wenn Ungewissheit darüber besteht, ob es sich um Auslands- oder Inlandsdaten handelt, behandeln die Nachrichtendienste solche Daten häufig als ausländische (da digitale Kommunikation regelmäßig an irgendeinem Punkt über das Ausland geleitet wird) und erlauben so ihre Sammlung und Vorratsspeicherung. Das Ergebnis ist ein erheblich schwächerer – oder womöglich inexistenter – Schutz der Privatsphäre für Ausländer und Nichtstaatsangehörige gegenüber dem Schutz, den Staatsangehörige genießen.

36. Die internationalen Menschenrechtsnormen sind in Bezug auf den Grundsatz der Nichtdiskriminierung explizit. In Artikel 26 des Internationalen Paktes über bürgerliche und politische Rechte heißt es: „Alle Menschen sind vor dem Gesetz gleich und haben ohne Diskriminierung Anspruch auf gleichen Schutz durch das Gesetz.“ und ferner: „In dieser Hinsicht hat das Gesetz jede Diskriminierung zu verbieten und allen Menschen gegen jede Diskriminierung, wie insbesondere wegen der Rasse, der Hautfarbe, des Geschlechts, der Sprache, der Religion, der politischen oder sonstigen Anschauung, der nationalen oder sozialen Herkunft, des Vermögens, der Geburt oder des sonstigen Status, gleichen und wirksamen Schutz zu gewährleisten.“ Diese Bestimmungen sind zusammen mit Artikel 17 zu lesen, worin es heißt: „Niemand darf willkürlichen Eingriffen in sein Privatleben … ausgesetzt werden“ und „Jedermann hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen“, sowie mit Artikel 2 Absatz 1. In dieser Hinsicht hat der Menschenrechtsausschuss die Wichtigkeit von Maßnahmen unterstrichen, „die sicherstellen, dass jeder Eingriff in das Recht auf Privatheit mit den Grundsätzen der Rechtsmäßigkeit, Verhältnismäßigkeit und Notwendigkeit im Einklang steht, ungeachtet der Staatsangehörigkeit der Personen, deren Kommunikation direkt überwacht wird, oder des Ortes, an dem sie sich befinden”[31].

D. Verfahrensgarantien und wirksame Aufsicht

37. Artikel 17 Absatz 2 des Internationalen Paktes über bürgerliche und politische Rechte besagt, dass jeder Anspruch auf rechtlichen Schutz gegen rechtswidrige oder willkürliche Ein-

[30] Siehe beispielweise in den Vereinigten Staaten Foreign Intelligence Surveillance Act S1881(a); im Vereinigten Königreich Regulation of Investigatory Powers Act 2000, s8(4); in Neuseeland Government Security Bureau Act 2003, s. 15A; in Australien Intelligence Services Act S. 9; und in Kanada National Defence Act, S. 273.64 (1).

[31] CCPR/C/USA/CO/4, Ziff. 22.

griffe oder Beeinträchtigungen hat. Dieser „rechtliche Schutz“ muss durch wirksame Verfahrensgarantien, einschließlich effektiver, mit ausreichenden Mitteln ausgestatteter institutioneller Regelungen, mit Leben erfüllt werden. Es ist jedoch offensichtlich, dass das Fehlen einer wirksamen Aufsicht auch zu mangelnder Rechenschaft für willkürliche oder rechtswidrige Eingriffe in das Recht auf Privatheit im digitalen Umfeld beigetragen hat. Insbesondere hat sich gezeigt, dass interne Garantien, die nicht mit einer unabhängigen externen Kontrolle verbunden sind, gegen rechtswidrige oder willkürliche Überwachungsmethoden nicht viel ausrichten können. Während solche Garantien vielfältige Formen annehmen können, sind die Beteiligung aller Staatsgewalten an der Aufsicht über die Überwachungsprogramme sowie die Mitwirkung einer unabhängigen zivilen Aufsichtsstelle wesentliche Voraussetzungen für die Gewährleistung eines wirksamen rechtlichen Schutzes.

38. Die Einbeziehung der Gerichte, unter Beachtung internationaler Standards für Unabhängigkeit, Unparteilichkeit und Transparenz, kann die Wahrscheinlichkeit erhöhen, dass die allgemeinen gesetzlichen Regelungen den durch die internationalen Menschenrechtsnormen geforderten Mindeststandards entsprechen. Gleichzeitig sollte die Beteiligung der Gerichte an der Aufsicht nicht als Allheilmittel betrachtet werden: In mehreren Ländern läuft die gerichtliche Anordnung oder Überprüfung der digitalen Überwachungsaktivitäten von Nachrichtendiensten und/oder Strafverfolgungsbehörden letztlich auf eine routinemäßige Absegnung hinaus. Die Aufmerksamkeit verlagert sich daher zunehmend auf Modelle einer gemischten verwaltungsmäßigen, gerichtlichen und parlamentarischen Aufsicht, ein Punkt, der in mehreren Beiträgen zu diesem Bericht hervorgehoben wurde. Besondere Aufmerksamkeit gilt der Schaffung der Position eines „Sachwalters des öffentlichen Interesses“ innerhalb der Verfahren zur Genehmigung von Überwachungsaktivitäten. Angesichts der wachsenden Rolle Dritter, wie etwa von Internetanbietern, müsste möglicherweise auch erwogen werden, diesen Dritten zu gestatten, an der Genehmigung von Überwachungsmaßnahmen, die ihre Interessen berühren, mitzuwirken oder gegen bestehende Maßnahmen Einspruch zu erheben. In der maßgeblichen Rechtsprechung wurde positiv vermerkt, wie nützlich eine unabhängige Beratung, Kontrolle und/oder Überprüfung sein kann, die dazu beiträgt, eine strenge Prüfung der durch ein gesetzliches Überwachungsregime verhängten Maßnahmen sicherzustellen. Auch parlamentarische Ausschüsse können eine wichtige Rolle spielen; allerdings mangelt es ihnen möglicherweise an der Unabhängigkeit, den Ressourcen oder der Bereitschaft, Missbräuche zu entdecken, und es besteht die Gefahr einer Vereinnahmung durch die zu regulierende Branche. In der Rechtsprechung auf regionaler Ebene wurde die Nützlichkeit eines vollkommen unabhängigen Aufsichtsgremiums betont, insbesondere bei der Kontrolle der Durchführung genehmigter Überwachungsmaßnahmen.[32] 2009 schlug der Sonderberichterstatter über die Förderung und den Schutz der Menschenrechte und Grundfreiheiten bei der Bekämpfung des Terrorismus daher vor, „dass es kein geheimes Überwachungssystem geben darf, das nicht von einem unabhängigen Aufsichtsgremium überprüft wird, und dass alle Eingriffe von einem unabhängigen Gremium genehmigt werden müssen.“[33]

E. Recht auf wirksamen Rechtsschutz

39. Nach dem Internationalen Pakt über bürgerliche und politische Rechte sind die Vertragsstaaten verpflichtet, dafür Sorge zu tragen, dass Opfer von Verletzungen des Paktes über wirksamen Rechtsschutz verfügen. Artikel 2 Absatz 3 Buchstabe b führt aus, dass die Vertragsstaaten des Paktes sich verpflichten, „dafür Sorge zu tragen, dass jeder, der eine solche Beschwerde erhebt, sein Recht durch das zuständige Gerichts-, Verwaltungs- oder Gesetzgebungsorgan oder durch eine andere, nach den Rechtsvorschriften des Staates zuständige Stelle feststellen lassen

[32] Siehe beispielsweise Europäischer Gerichtshofs für Menschenrechte, Ekimdzhiev v. Bulgarien, Klageschrift Nr. 62540/00, 28. Juni 2007.

[33] A/HRC/13/37, Ziff. 62.

kann, und den gerichtlichen Rechtsschutz auszubauen.“ Außerdem müssen die Staaten dafür Sorge tragen, dass die zuständigen Stellen Beschwerden, denen stattgegeben wurde, Geltung verschaffen. Wie der Menschenrechtsausschuss in seiner Allgemeinen Bemerkung Nr. 31 betonte, würde das Versäumnis eines Vertragsstaats, mutmaßliche Verletzungen zu untersuchen, schon für sich genommen eine Verletzung des Paktes darstellen.[34] Darüber hinaus ist die Beendigung einer andauernden Verletzung ein wesentliches Element des Rechts auf wirksamen Rechtsschutz.

40. Wirksamer Rechtsschutz bei Verletzungen der Privatsphäre durch digitale Überwachung kann daher unterschiedliche gerichtliche, legislative oder administrative Formen annehmen. In der Regel weisen wirksame Rechtsbehelfe bestimmte gemeinsame Merkmale auf. Erstens müssen sie allen Personen, die plausibel geltend machen können, dass ihre Rechte verletzt wurden, bekannt und für sie zugänglich sein. Der Inkenntnissetzung (darüber, dass ein allgemeines Überwachungssystem oder konkrete Überwachungsmaßnahmen existieren) sowie der Rechtsstellung des Betroffenen (Berechtigung, solche Maßnahmen anzufechten) kommen daher ausschlaggebende Bedeutung für den Zugang zu wirksamem Rechtsschutz zu. Die Staaten gehen bei der Inkenntnissetzung unterschiedlich vor: Während einige die nachträgliche Benachrichtigung der Zielpersonen nach Abschluss der Ermittlungen verlangen, sehen viele Regime eine solche Benachrichtigung nicht vor. In manchen Staaten ist eine Benachrichtigung bei Strafsachen offiziell vorgeschrieben; dieses Erfordernis scheint in der Praxis jedoch meistens ignoriert zu werden. Auch in der Frage, ob Betroffene die Rechtsstellung zur Anfechtung von Maßnahmen besitzen, gibt es national unterschiedliche Ansätze. Der Europäische Gerichtshof für Menschenrechte entschied, dass die Existenz eines Überwachungsregimes zwar in die Privatsphäre eingreifen könnte, dass jedoch die Behauptung, dies verursache eine Rechtsverletzung, nur dann justiziabel ist, wenn eine Person „mit hinreichender Wahrscheinlichkeit“ tatsächlich einer rechtswidrigen Überwachung ausgesetzt war.[35]

41. Zweitens muss wirksamer Rechtsschutz mit einer umgehenden, gründlichen und unparteilichen Untersuchung der geltend gemachten Verletzungen einhergehen. Dies kann geschehen durch die Bereitstellung eines „unabhängigen Aufsichtsgremiums […] mit ausreichenden rechtsstaatlichen Garantien und gerichtlicher Aufsicht im Rahmen der in einer demokratischen Gesellschaft zulässigen Beschränkungen“.[36] Drittens müssen Rechtsbehelfe, um wirksam zu sein, andauernden Verletzungen ein Ende setzen können, zum Beispiel durch die Anordnung der Löschung von Daten oder eine andere Wiedergutmachung.[37] Die Beschwerdeinstanzen müssen über „vollen und ungehinderten Zugang zu allen relevanten Informationen, die notwendigen Ressourcen und Sachkenntnisse zur Durchführung von Untersuchungen sowie die Fähigkeit, rechtlich bindende Anordnungen zu treffen,“ verfügen.[38] Viertens werden dort, wo Menschenrechte in einem Ausmaß verletzt werden, dass der Tatbestand einer groben Verletzung erfüllt ist,

[34] CCPR/C/21/Rev.1/Add. 13, Ziff. 15.

[35] Siehe Esbester v. Vereinigtes Königreich, Klageschrift Nr. 18601/91, Beschluss der Kommission vom 2. April 1993; Redgrave v. Vereinigtes Königreich, Klageschrift Nr. 202711/92, Beschluss der Kommission vom 1. September 1993; und Matthews v. Vereinigtes Königreich, Klageschrift Nr. 28576/95, Beschluss der Kommission vom 16. Oktober 1996.

[36] “Joint declaration on surveillance programs and their impact on freedom of expression”, herausgegeben vom Sonderberichterstatter über die Förderung und den Schutz der Meinungsfreiheit und des Rechts der freien Meinungsäußerung und dem Sonderberichterstatter über freie Meinungsäußerung bei der Interamerikanischen Menschenrechtskommission, Juni 2013 (abrufbar unter http://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1), Ziff. 9.

[37] Siehe beispielsweise Europäischer Gerichtshof für Menschenrechte, Segerstedt-Wiberg u.a. v. Schweden, Klageschrift Nr. 62332/00, 6. Juni 2006. Siehe auch CCPR/C/21/Rev.1/Add.13, Ziff. 15-17.

[38] A/HRC/14/46.

nichtgerichtliche Rechtsschutzmaßnahmen nicht mehr ausreichen; in solchen Fällen ist eine strafrechtliche Verfolgung erforderlich.[39]

IV. Die Rolle des Privatsektors

42. Es gibt umfangreiche Belege dafür, dass Staaten zunehmend den Privatsektor zur Durchführung und Erleichterung der digitalen Überwachung heranziehen. Auf jedem Kontinent gibt es Beispiele für staatliche Stellen, die sowohl förmliche Rechtsmechanismen als auch verdeckte Methoden einsetzen, um Zugriff auf Kommunikationsinhalte sowie Metadaten zu erhalten. Dieser Prozess wird zunehmend formalisiert: mit der wachsenden Verlagerung der Bereitstellung von Telekommunikationsdiensten vom öffentlichen auf den privaten Sektor kommt es zu einer „Delegation von Strafverfolgungs- und quasigerichtlichen Aufgaben auf Internetvermittler unter dem irreführenden Schlagwort der ‚Selbstregulierung' oder ‚Kooperation'".[40] Der Erlass gesetzlicher Vorschriften, die Unternehmen dazu verpflichten, ihre Netze „abhörfähig" zu machen, ist besonders besorgniserregend, nicht zuletzt deshalb, weil so ein Umfeld geschaffen wird, das weitreichende Überwachungsmaßnahmen erleichtert.

43. Es mag legitime Gründe dafür geben, dass ein Staat von einem Informations- und Kommunikationstechnologieunternehmen verlangt, Nutzerdaten zur Verfügung zu stellen; wenn jedoch ein Unternehmen einem Staat aufgrund einer Aufforderung, die gegen das völkerrechtlich geschützte Recht auf Privatheit verstößt, Daten oder Nutzerinformationen zur Verfügung stellt, wenn ein Unternehmen Staaten ohne das Vorhandensein angemessener Garantien Technik oder Ausrüstung für Massenüberwachung zur Verfügung stellt, oder wenn diese Informationen in anderer Weise unter Verletzung von Menschenrechten eingesetzt werden, dann riskiert das Unternehmen, mittelbar oder auch unmittelbar am Missbrauch von Menschenrechten beteiligt zu sein. Die vom Menschenrechtsrat 2011 gebilligten Leitprinzipien für Wirtschaft und Menschenrechte stellen einen globalen Standard für die Verhütung und Behandlung nachteiliger Auswirkungen von Wirtschaftstätigkeiten auf die Menschenrechte dar. Die Verantwortung für die Achtung der Menschenrechte gilt für die gesamte weltweite Tätigkeit eines Unternehmens, ungeachtet dessen, an welchem Ort sich seine Nutzer befinden, und sie besteht unabhängig davon, ob der Staat seinen eigenen Menschenrechtsverpflichtungen nachkommt.

44. Zahlreiche Interessenträger haben wichtige Anstrengungen unternommen, um die Anwendung der Leitprinzipien im Kommunikations- und Informationstechnologiesektor zu klären. Unternehmen, die Inhalte oder Internetdienste anbieten oder Technologie und Ausrüstung liefern, die digitale Kommunikation ermöglicht, sollten beispielsweise eine klare Grundsatzerklärung abgeben, in der sie ihr Bekenntnis zur Achtung der Menschenrechte bei sämtlichen Tätigkeiten des Unternehmens zum Ausdruck bringen. Sie sollten außerdem über angemessene Regelungen für die Einhaltung der Sorgfaltspflicht verfügen, um nachteilige Auswirkungen zu ermitteln, zu bewerten, zu verhüten und abzumildern. Die Unternehmen sollten bewerten, wie und ob ihre Nutzungsbedingungen oder ihre Regelungen für die Erhebung und Weitergabe von Kundendaten sich nachteilig auf die Menschenrechte ihrer Nutzer auswirken könnten.

45. Wenn Unternehmen sich mit Forderungen staatlicher Stellen nach Zugriff auf Daten konfrontiert sehen, die nicht mit den internationalen Menschenrechtsnormen im Einklang stehen, wird von ihnen erwartet, dass sie sich darum bemühen, die Menschenrechtsprinzipien in größtmöglichem Umfang einzuhalten, und dass sie den Nachweis für fortlaufende Anstrengungen in dieser Hinsicht erbringen können. Dies kann bedeuten, dass Anfragen dieser Stellen so eng wie

[39] Grundprinzipien und Leitlinien betreffend das Recht der Opfer von groben Verletzungen der internationalen Menschenrechtsnormen und schweren Verstößen gegen das humanitäre Völkerrecht auf Rechtsschutz und Wiedergutmachung (Resolution 60/147 der Generalversammlung, Anlage).

[40] Siehe European Digital Rights, "The Slide from 'Self-Regulation' to Corporate Censorship", Brüssel, Januar 2011, abrufbar unter http://www.edri.org/files/EDRI_selfreg_final_20110124.pdf.

möglich ausgelegt werden, dass von den staatlichen Stellen eine Klarstellung des Umfangs und der Rechtsgrundlage für den geforderten Zugriff verlangt wird, dass zur Erfüllung der Datenanforderung eine gerichtliche Anordnung verlangt wird und dass die Nutzer in transparenter Weise über Risiken und über die Erfüllung der Forderungen der staatlichen Stellen unterrichtet werden. Es gibt positive Beispiele für diesbezügliche Maßnahmen der Branche, sowohl seitens einzelner Unternehmen als auch durch Initiativen einer größeren Zahl von Interessenträgern.

46. Bei der in den Leitprinzipien beschriebenen menschenrechtlichen Sorgfaltspflicht spielen sinnvolle Konsultationen mit betroffenen Interessenträgern eine zentrale Rolle. Im Kontext der Informations- und Kommunikationstechnologieunternehmen gehört dazu auch, dass den Nutzern wirkliche Transparenz darüber zugesichert wird, wie ihre Daten gesammelt, gespeichert, genutzt und möglicherweise an andere weitergegeben werden, sodass sie in der Lage sind, Probleme anzusprechen und fundierte Entscheidungen zu treffen. Die Leitprinzipien stellen klar, dass Unternehmen, die feststellen, dass sie nachteilige Auswirkungen auf die Menschenrechte verursacht oder dazu beigetragen haben, eine Verantwortung tragen, für Wiedergutmachung zu sorgen, indem sie direkte Abhilfe schaffen oder bei rechtmäßigen Verfahren zu diesem Zweck kooperieren. Um eine möglichst frühzeitige Wiedergutmachung zu ermöglichen, sollten die Unternehmen Beschwerdemechanismen auf operativer Ebene einrichten. Solchen Mechanismen kann besondere Bedeutung zukommen, wenn die Unternehmen in Ländern tätig sind, in denen Rechte nicht ausreichend geschützt sind oder der Zugang zu gerichtlichen und außergerichtlichen Rechtsbehelfen nicht gegeben ist. Zusätzlich zu Elementen wie Entschädigung und Restitution sollten Abhilfemaßnahmen auch Informationen darüber umfassen, welche Daten an die staatlichen Behörden weitergegeben wurden und auf welche Weise.

V. Schlussfolgerungen und Empfehlungen

47. **Die internationalen Menschenrechtsnormen bieten einen klaren und universellen Rahmen für die Förderung und den Schutz des Rechts auf Privatheit, auch im Zusammenhang mit innerstaatlicher und extraterritorialer Überwachung, dem Abfangen digitaler Kommunikation und der Erhebung personenbezogener Daten. Die in zahlreichen Staaten angewandten Praktiken lassen jedoch einen Mangel an angemessenen innerstaatlichen Rechtsvorschriften und/oder ihrer Durchsetzung, schwache Verfahrensgarantien und eine ineffektive Aufsicht erkennen, Faktoren, die ihrerseits zu einem Mangel an Rechenschaftspflicht für willkürliche oder rechtswidrige Eingriffe in das Recht auf Privatheit beitragen.**

48. **Was die Behebung der beträchtlichen Lücken bei der Umsetzung des Rechts auf Privatheit anlangt, sind zwei Bemerkungen angebracht. Erstens tauchen immer wieder neue Informationen über Politiken und Praktiken auf dem Gebiet innerstaatlicher und extraterritorialer Überwachungsmaßnahmen auf. Es finden Untersuchungen statt mit dem Ziel, Informationen über elektronische Überwachung und das Sammeln und Speichern personenbezogener Daten zu gewinnen und die Auswirkungen auf die Menschenrechte zu beurteilen. Auf nationaler und regionaler Ebene befassen sich Gerichte mit der Prüfung der Rechtmäßigkeit von Politiken und Maßnahmen der elektronischen Überwachung. Bei jeder Beurteilung von Überwachungspolitiken und -praktiken nach dem Kriterium der internationalen Menschenrechtsnormen ist notwendigerweise der sich verändernde Charakter dieser Frage zu berücksichtigen. Eine zweite, damit zusammenhängende Bemerkung gilt dem beunruhigenden Mangel an staatlicher Transparenz bei den die Überwachung betreffenden Politiken, Rechtsvorschriften und Praktiken, der die Bemühungen behindert, ihre Übereinstimmung mit den internationalen Menschenrechtsnormen zu beurteilen und für Rechenschaft zu sorgen.**

49. **Um die Probleme im Zusammenhang mit dem Recht auf Privatheit im Kontext der modernen Kommunikationstechnologie wirksam anzugehen, bedarf es einer fortlaufen-**

den und abgestimmten Mitwirkung der verschiedenen Interessenträger. Dieser Prozess sollte einen Dialog unter Beteiligung aller Interessenträger beinhalten, der Mitgliedstaaten, der Zivilgesellschaft, Vertretern aus Wissenschaft und Technik, der Wirtschaft, der Hochschulen und Menschenrechtsexperten. In Anbetracht der ständigen Weiterentwicklung der Kommunikationstechnologien wird Führungsgeschick unerlässlich sein, um sicherzustellen, dass diese Technologien in einer Weise eingesetzt werden, die das ihnen innewohnende Potenzial zur Verbesserung des Genusses der völkerrechtlich verankerten Menschenrechte zur Entfaltung bringt.

50. **Aus diesen Bemerkungen ergibt sich die klare und vordringliche Notwendigkeit, wachsam zu sein und durch die Erarbeitung wirksamer Garantien gegen Missbräuche sicherzustellen, dass jede Überwachungspolitik oder -praxis mit den internationalen Menschenrechtsnormen, einschließlich des Rechts auf Privatheit, im Einklang steht. Als Sofortmaßnahme sollten die Staaten ihre eigenen nationalen Rechtsvorschriften, Politiken und Praktiken überprüfen, um ihre volle Übereinstimmung mit den internationalen Menschenrechtsnormen sicherzustellen. Wo Defizite vorhanden sind, sollten die Staaten Schritte zu ihrer Behebung ergreifen, insbesondere durch die Schaffung eines klaren, präzisen, zugänglichen, umfassenden und nichtdiskriminierenden Rechtsrahmens. Durch entsprechende Schritte sollte sichergestellt werden, dass wirksame und unabhängige Aufsichtsregeln und -praktiken vorhanden sind, die auch das Recht der Opfer auf wirksamen Rechtsschutz berücksichtigen.**

51. **Im digitalen Zeitalter stehen der Förderung und dem Schutz des Rechts auf Privatheit eine Reihe bedeutender praktischer Probleme entgegen. Aufbauend auf einer ersten Erkundung einiger dieser Probleme im vorliegenden Bericht sind weitere Diskussionen sowie eine eingehende Untersuchung von Fragen erforderlich, die mit einem wirksamen Schutz durch das Gesetz, Verfahrensgarantien, effektiver Aufsicht und Rechtsschutz zusammenhängen. Eine gründliche Analyse dieser Fragen würde dazu beitragen, weitere, auf den internationalen Menschenrechtsnormen gründende praktische Orientierungshilfen zu den Prinzipien der Notwendigkeit, der Verhältnismäßigkeit und der Rechtmäßigkeit in Bezug auf Überwachungspraktiken, zu Maßnahmen für eine wirksame, unabhängige und unparteiliche Aufsicht und zu Abhilfemaßnahmen abzuleiten. Weitere Analysen würden auch Wirtschaftsunternehmen helfen, ihrer Verantwortung für die Achtung der Menschenrechte, einschließlich der Sorgfaltspflicht und Garantien für Risikomanagement, sowie für die Wahrnehmung ihrer Rolle bei der Schaffung wirksamer Abhilfe gerecht zu werden.**