

für Menschenrechte

Zusammenfassung

In ihrer Resolution 68/167 ersuchte die Generalversammlung die Hohe Kommissarin der Vereinten Nationen für Menschenrechte und 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

	Paragraf	Seite
I. Einleitung.....	1-6	3
II. Hintergrund und Methodik.....	7-11	4
III. Fragen im Zusammenhang mit dem Recht auf Privatheit im digitalen Zeitalter	12-41	5
A. Das Recht auf Schutz vor willkürlichen oder rechtswidrigen Eingriffen in das Privatleben, die Familie, die Wohnung und den Schriftverkehr.....	15-27	6
B. Rechtlicher Schutz.....	28-30	10
C. Wer ist wo geschützt?.....	31-36	12
D. Verfahrensgarantien und wirksame Aufsicht.....	37-38	13
E. Rechtauf wirksamen Rechtsschutz.....	39-41	14
IV. Die Rolle des Privatsektors.....	42-46	16
V. Schlussfolgerungen und Empfehlungen.....	47-51	17

I. Einleitung

1. Digitale Kommunikationstechnologien wie das Internet, Smartphones und Tablets sind heute Teil des täglichen Lebens. Die Innovationen der Kommunikationstechnologie haben durch die enorme Verbesserung des Zugangs zu Information 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 Durchführungsmaßnahmen 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. Mit anderen Worten, die technologischen Plattformen, auf die sich das politische, wirtschaftliche und soziale Leben weltweit stützt, sind nicht nur anfällig für Massenüberwachung, sondern fördern dies sogar.

3. Die Aufdeckung von Politiken und Praktiken, die sich die Anfälligkeit der digitalen Kommunikationstechnologien für elektronisches Überwachen und Gefährdungen ausnutzen, 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 globalen Praxis.

ßen Teil des weltweiten Internetverkehrs, zu Anrufrufen in den Vereinigten Staaten, zu den elektronischen Adressverzeichnissen 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 mangelhaften Auswirkungen dieser Überwachungspraktiken auf die Menschenrechte beschloss 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, im Abfagen 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.

Iss an- [(u)-4wn

ganisationen, drei nationale Menschenrechtsinstitutionen, 16 staatliche Organisationen und zwei privatwirtschaftliche Initiativen übermittelten Beiträge.

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 Verfassungsgarantien und einer wirksamen Aufsicht ein. Manche Beiträge beschrieben Probleme, die bei der Umsetzung des Rechts auf Privatheit im digitalen Zeitalter auftreten könnten, und schickten 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 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.

26. Besorgnisse darüber, ob der Zugang zu Daten und ihre Nutzung auf spezifische Weise legi

dass eine betroffene Person in der Lage ist, ihr Verhalten anzubringen 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 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, wie den Sicherheits- und Nachrichtendienst, einen übermäßigen Ermessensspielraum 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
anixwi73(n)513.57j 0.002

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 ~~Bezüge~~ ^{Besorgnis} 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~~ ^{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~~ ^{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 ~~Vertrag~~ ^{Vertrag} staaten 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~~ ^{Person} ~~unter~~ ^{unter} ~~liegend~~ ^{liegend} ~~gewährleisten~~ ^{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 ~~Entscheidung~~ ^{Entscheidung} geäußerten Grundsatz leiten lassen, dass ein Staat sich seinen Verpflichtungen ~~auf dem~~ ^{auf dem} Gebiet der internationalen Menschenrechte nicht entziehen kann, indem er außerhalb ~~des~~ ^{des} Hoheitsgebiets Maßnahmen vornimmt, die ihm „im eigenen Land“ untersagt wären.

walt oder tatsächlicher Kontrolle in Bezug auf digitale Kommunikationsinfrastruktur, gleich wo

griffe oder Beeinträchtigungen hat. Dieser „rechtliche Schluss durch wirksame Verfahrensgarantien, einschließlich effektiver, mit ausreichenden Mitteln ausgestatteter nationaler 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 ein

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. Darüber hinaus ist die Beendigung einer andauernden Verletzung ein wesentliches Element des Rechts auf wirksamen Rechtsschutz.

40.

nichtgerichtliche Rechtsschutzmaßnahmen nicht mehr ausreichen; in solchen Fällen ist eine strafrechtliche Verfolgung erforderlich.³⁸

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 wachsenden

möglich ausgelegt werden, dass von den staatlichen Stellen eine Klarstellung des Inhalts 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, sei es 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 informierte 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,

