Eric Töpfer

Wie das Menschenrecht auf Privatheit in seiner Krise an Profil gewinnt

In den Gremien der Vereinten Nationen haben die Enthüllungen Edward Snowdens über die massenhafte Überwachung der „Five Eyes“ eine rege Diskussion um die Bedeutung und Reichweite des Menschenrechts auf Privatheit im digitalen Zeitalter ausgelöst. Auch wenn angesichts der widerstreitenden nationalen Interessen keine Wunder zu erwarten sind, schärft die Debatte doch das Profil eines bislang schwer zu fassenden Menschenrechts. Eric Töpfer zeichnet in seinem Beitrag die Diskussionen um das Recht auf Privatheit in den verschiedenen UN-Gremien nach.

1 Einleitung

Eher zufällig fand das Recht auf Privatheit im Jahr 1948 Eingang in die Allgemeine Erklärung der Menschenrechte (Artikel 12) und 18 Jahre später in den Internationalen Pakt über bürgerliche und politische Rechte (Artikel 17).[1] Kein Mitglied der Vereinten Nationen garantierte nach dem Ende des Zweiten Weltkriegs einen umfassenden Schutz des Privatlebens in seiner Verfassung. Als „das vielleicht am schwersten zu definierende aller Menschenrechte“[2] fristete das Recht auf Privatheit lange Zeit ein Schattendasein.

Nur in einer knappen, zweiseitigen Allgemeinen Bemerkung erläuterte der Menschenrechtsausschuss, zuständig für das Monitoring und die Interpretation des Pakts über bürgerliche und politische Rechte (Zivilpakt) im Jahr 1988 seine Lesart dessen, was es heißt, dass „[n]iemand [...] willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden“ darf. In zwei Absätzen adressierte der Ausschuss damals die Themen Kommunikationsüberwachung und automatisierte Datenverarbeitung.[3]

Erst ein Bericht des ehemaligen UN-Sonderberichterstatters für die Achtung der Menschenrechte bei der Terrorismusbekämpfung, Martin Scheinin, wies 2009 auf die dramatische Erosion des Rechts auf Privatheit angesichts wachsender staatlicher

Überwachungsvollmachten und neuer Technologien hin und empfahl Maßnahmen gegen Machtmissbrauch und zur besseren Regulierung des Austauschs von Daten mit Dritten. Hierzu regte er unter anderem die Modernisierung der Allgemeinen Bemerkung zu Artikel 17 des Zivilpaktes durch den Menschenrechtsausschuss an und schlug dem Menschenrechtsrat vor, die Arbeit an einem Entwurf für eine globale Datenschutz-Erklärung aufzunehmen.[4]

Verstärkung erhielt Scheinin von seinem Kollegen Frank La Rue, der als UN-Sonderberichterstatter für das Recht auf Meinungsfreiheit im April 2013 einen viel beachteten Bericht zur Internetüberwachung vorlegte, in dem er vor den bedrohlichen Folgen einer wachsenden Ausforschung des Internet für das Recht auf Meinungsfreiheit, das Recht auf Privatheit und die Grundlagen einer demokratischen Gesellschaft warnte. Der Bericht La Rues enthielt einen umfangreichen Katalog mit Empfehlungen, die von einer Stärkung der Regulierung staatlicher Überwachung über die Förderung von Verschlüsselung und Anonymisierung bis hin zur Einhegung der privatwirtschaftlichen Datensammlung reichten.[5]

Als kaum zwei Monate später die bis heute nicht abreißende Serie von Enthüllungen über die massenhafte Überwachung der globalen Telekommunikation durch die *National Security Agency* (NSA) und alliierter Geheimdienste begann, lagen die möglichen Antworten internationaler Menschenrechtsgremien somit bereits auf dem Tisch.

2 Die Resolution der Generalversammlung zum „Recht auf Privatheit im digitalen Zeitalter“

In Deutschland reagierte die Bundesregierung auf die Berichte zur Überwachung durch die „Five Eyes“ fast umgehend mit einem Acht-Punkte-Plan.[6] Unter anderem sollte eine UN-Vereinbarung zum Datenschutz erreicht werden. Zwar blieb die Idee, ein Zusatzprotokoll zu Artikel 17 des Zivilpaktes zu verhandeln, in den Kinderschuhen stecken. Gleichwohl gelang es, eine Koalition europäischer Staaten zu mobilisieren, um auf UN-Ebene aktiv zu werden.

Dort waren im August 2013 bereits die lateinamerikanischen MERCOSUR-Staaten, vertreten von Argentinien, beim Sicherheitsrat vorstellig geworden, um ihren Protest gegen die US-Spionage in der Region kundzutun, nachdem nicht nur das Flugzeug von Boliviens Präsident Evo Morales auf Suche nach dem flüchtigen Snowden gestoppt, sondern auch über umfangreiche NSA-Überwachungsprogramme in der Region berichtet worden war.[7] Als dann im Herbst noch bekannt wurde, dass sowohl die Kommunikation von Bundeskanzlerin Angela Merkel als auch der brasilianischen Präsidentin Dilma Rousseff von der NSA abgehört worden war, kündigten Deutschland und Brasilien am 24. Oktober 2013 an, gemeinsam eine UN-Resolution zum „Recht auf Privatsphäre im digitalen Zeitalter“ auf den Weg zu bringen.[8]

Der gemeinsame Entwurf beider Staaten vom 1. November[9] wurde bis zu seiner endgültigen Annahme durch die Generalversammlung der Vereinten Nationen am 18. Dezember auf Druck insbesondere der USA in einigen Punkten deutlich abgeschwächt,[10] gleichwohl war es das erste Mal, dass die Generalversammlung in aller

Deutlichkeit feststellte, dass die Menschenrechte und insbesondere das Recht auf Privatsphäre „offline“ und „online“ gleichermaßen gelten. Darüber hinaus wurden alle Staaten aufgefordert:

- das Recht auf Privatsphäre auch im Kontext digitaler Kommunikation zu achten und zu schützen,
- Maßnahmen zu ergreifen, um Rechtsverletzungen zu beenden bzw. zu verhindern,
- ihr nationales Recht und die Praktiken der Kommunikationsüberwachung zu überprüfen und in Einklang mit internationalen Menschenrechtsverpflichtungen zu bringen sowie
- unabhängige und effektive Aufsichtsmechanismen einzurichten, damit eine angemessene Transparenz und Kontrollierbarkeit staatlicher Überwachung gewährleistet ist.

Zudem wurde die UN-Menschenrechtskommissarin aufgefordert, dem Menschenrechtsrat und der Generalversammlung für ihre Sitzungen in der zweiten Jahreshälfte 2014 einen Bericht zum Thema vorzulegen.[11]

3 Der Bericht von UN-Menschenrechtskommissarin Navi Pillay

Sieben Monate später präsentierte die scheidende UN-Hochkommissarin für Menschenrechte, Navi Pillay, in Genf den Bericht ihres Büros.[12] Auf Grundlage der Ergebnisse von Workshops mit Fachleuten, einer Studie der United Nations University und einer offenen Konsultation, an der sich 29 Staaten, unter anderen die USA, das Vereinigte Königreich und Deutschland, aber auch der Ausschuss für Terrorismusbekämpfung des UN-Sicherheitsrates, der Europarat, die Artikel-29-Arbeitsgruppe europäischer Datenschützer und der Europäische Datenschutzbeauftragte sowie zahlreiche Menschenrechtsorganisationen beteiligt hatten, ist der Bericht eine konzise Stellungnahme zum menschenrechtlichen Rahmen des Schutzes der Privatsphäre im digitalen Zeitalter. Der Bericht zieht eine ernüchternde Bilanz der gegenwärtigen Rechtswirklichkeit: Die digitale Kommunikation, von der das globale politische, wirtschaftliche und gesellschaftliche Leben zunehmend abhängig ist, ermögliche eine nahezu unbegrenzte Massenüberwachung, die nicht länger Ausnahme sei, sondern sich zu einer „gefährlichen Gewohnheit“ entwickle (Rn. 3).

3.1 Privatsphäre als universelles Menschenrecht

Mit Verweis auf Artikel 12 der Allgemeinen Erklärung für Menschenrechte, Artikel 17 des UN-Zivilpaktes sowie auf die regionalen Menschenrechtsinstrumente, die – mit Ausnahme der Afrikanischen Menschenrechtskonvention – alle das Recht auf Privatsphäre garantieren, betont der Bericht eingangs die „universelle Anerkennung der

fundamentalen Bedeutung und andauernden Relevanz des Rechts auf Privatsphäre und der Notwendigkeit seines gesetzlichen und praktischen Schutzes“ (Rn. 13). Zudem wird unterstrichen, dass Massenüberwachung auch andere Rechte beeinträchtigen könne, insbesondere das Recht auf freie Meinungsäußerung und Informationsfreiheit sowie die Versammlungs- und Vereinigungsfreiheit. Aber auch das Recht auf Gesundheit könnte betroffen sein, wenn Menschen aus Furcht vor Ausspähung zum Beispiel darauf verzichten, in sensiblen Fragen gesundheitlichen Rat zu suchen. Erinnert wird schließlich an die zahlreichen Hinweise darauf, dass durch Massenüberwachung gewonnene Informationen zu Folter und gezielten Tötungen durch Drohnenangriffe geführt hätten.

3.2 Jede Form der Kommunikationsüberwachung ist ein Eingriff in die Privatsphäre

Klare Position bezieht der Bericht in der Diskussion darum, wann Überwachung eigentlich einen Eingriff in die Privatsphäre darstellt: So wird das Argument, dass Menschen ihre persönlichen Daten „freiwillig“ für den digitalen Zugang zu Dienstleistungen, Gütern und Informationen tauschten, damit gekontert, dass Betroffene nicht immer wirklich wüssten, welche Daten sie wie und an wen preisgeben, und dass häufig nicht abzusehen sei, für welche Zwecke die Daten letztlich verwendet würden – was sich mit „Big Data“, den immer ausgefeilteren Analysen der ständig wachsenden Datenmassen, noch deutlich verschärfe. Bezugnehmend auf das Urteil des Europäischen Gerichtshofes zur EU-Vorratsdatenspeicherungsrichtlinie wird auch dem Versuch eine Absage erteilt, die Sammlung von Verkehrs- beziehungsweise Metadaten im Gegensatz zu Inhalten von Telekommunikation als unproblematisch abzutun: „Aus der Perspektive des Rechts auf Privatsphäre ist diese Unterscheidung nicht überzeugend. Das Aggregieren von Informationen, die üblicherweise als ‚Metadaten‘ bezeichnet werden, kann Aufschlüsse über das Verhalten, die sozialen Beziehungen, die privaten Vorlieben und die Identität eines Individuums geben, die weit über jene hinausgehen, die sich aus dem Zugriff auf den Inhalt privater Kommunikation ablesen lassen.“ (Rn. 19) Zusammenfassend wird festgestellt, dass jede Sammlung von Kommunikationsdaten sowie ihre Speicherung auf Vorrat – und selbst die bloße Möglichkeit einer solchen Erfassung – Menschenrechte tangiere: „Die bloße Existenz eines Programms zur Massenüberwachung stellt daher einen Eingriff in die Privatsphäre dar. Die Beweislast liegt beim Staat zu demonstrieren, dass ein solcher Eingriff weder willkürlich noch widerrechtlich ist.“ (Rn. 20)

3.3 Der Zweck heiligt nicht die Mittel – entgrenzte Überwachung ist zu maßregeln

Obwohl es in Artikel 12 des UN-Zivilpaktes nur heißt, dass niemand „willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben“ ausgesetzt sein darf und eine Begrenzungsklausel fehlt, welche wie Artikel 8 der Europäischen Menschenrechtskon-

vention abschließend die Zwecke auflistet, die einen Eingriff in die Privatsphäre rechtfertigen, macht der Bericht insbesondere mit Bezug zur Spruchpraxis des Menschenrechtsausschusses deutlich, dass es nicht allein ausreiche, Massenüberwachung einfach per Gesetz zu legalisieren. Vielmehr müssten solche nationalen Gesetze dem Geist des Zivilpaktes entsprechend und den jeweiligen Umständen angemessen sein. Jede Einschränkung des Rechts auf Privatsphäre müsse also eine gesetzliche Grundlage haben, die hinreichend zugänglich und bestimmt ist; jede Einschränkung müsse notwendig zur Erreichung legitimer Ziele sein sowie im Verhältnis zum Zweck stehen und die geringst mögliche Eingriffstiefe haben. Auch wenn die Überwachung zu Zwecken nationaler Sicherheit oder der Terrorismusbekämpfung ein legitimes Ziel verfolge, müsse die Tiefe des Eingriffs sich an der Notwendigkeit der Maßnahme und ihren Erfolgen messen lassen: „In anderen Worten, es wird nicht genug sein, dass Maßnahmen darauf abzielen, Nadeln im Heuhaufen zu finden; das rechte Maß ist die Wirkung der Maßnahmen auf den Heuhaufen im Verhältnis zum drohenden Schaden.“ (Rn. 25) Bezweifelt wird entsprechend, dass der Zwang zur Vorratsdatenspeicherung von Kommunikationsdaten durch Telefongesellschaften und Internetdienstleister notwendig und verhältnismäßig sei.

Zudem würde sich die Verhältnismäßigkeit einer Überwachungsmaßnahme auch daraus ergeben, welche Mechanismen zur Zweckbindung und Zugriffsbeschränkung vorhanden sind. Insbesondere die seit 9/11 wachsende Entgrenzung von polizeilicher und nachrichtendienstlicher Arbeit riskiere das Recht auf Privatsphäre zu verletzen. Überwachungsmaßnahmen, die in dem einen Feld legitim, notwendig und verhältnismäßig sind, müssen dies nicht auch zwangsläufig für ein anderes Feld sein.

3.4 Die Autorisierung von Kommunikationsüberwachung muss öffentlich zugänglich sein

Mit Bezug auf Artikel 17 Absatz 2 UN-Zivilpakt, wo es heißt, dass jeder Mensch „Anspruch auf rechtlichen Schutz“ gegen Eingriffe in seine Privatsphäre hat, erklärt der Bericht, dass jedes Gesetz zur Autorisierung von Kommunikationsüberwachung öffentlich zugänglich sein müsse. Dies heiße nicht nur, dass das Gesetz veröffentlicht, sondern auch, dass es so präzise – mit anderen Worten: normenklar und bestimmt – formuliert sein muss, dass jede betroffene Person die Auswirkungen des Gesetzes abschätzen und ihr Verhalten entsprechend anpassen kann. Geheimes Recht, geheime – auch richterliche – Interpretationen der Regeln hätten nicht die notwendige Qualität von „Recht“. Das gleiche gelte auch für Gesetze, die Geheimdiensten exzessive Ermessensspielräume einräumten, da die Auswirkungen des Rechts andernfalls nicht absehbar wären. Zusätzlich sei es wünschenswert, dass die Vollmachten der Nachrichtendienste nicht durch exekutive Verwaltungsvorschriften, sondern durch primäre Gesetzgebung definiert würden – schließlich verbriefe Artikel 25 UN-Zivilpakt, allen Bürgerinnen und Bürger eines Staates das Recht, an der Gestaltung der öffentlichen Angelegenheiten direkt oder indirekt teilzunehmen.

Im Hinblick der Meldungen über einen „Ringtausch“, bei dem Nachrichtendienste rechtliche Hürden im eigenen Land dadurch umgehen, dass sie sich Informationen

über befreundete Dienste beschaffen, die sich an solche Auflagen nicht gebunden fühlen, macht der Bericht deutlich, dass solche Praktiken gegen Artikel 5 UN-Zivilpakt verstoßen, der eine Auslegung der Bestimmungen des Paktes untersagt, die auf die Abschaffung der verbrieften Rechte und Freiheiten zielt.

3.5 Extraterritoriale Geltung des Rechts auf Privatsphäre?

Artikel 2 UN-Zivilpakt verpflichtet die Staaten zu Achtung und Gewährleistung der Menschenrechte auf ihrem Territorium und gegenüber Personen unter ihrer Herrschaftsgewalt. „Macht" und „Kontrolle" seien Indikatoren dafür, ob und wo ein Staat „Herrschaftsgewalt" im Sinne von Artikel 2 ausübe, so der Bericht in Anlehnung an die Interpretationen von Menschenrechtsausschuss und Internationalem Gerichtshof. Die menschenrechtliche Bindung des Rechts auf Privatheit ende deshalb nicht an der Staatsgrenze. Ebenso wenig würde ein Outsourcing von Überwachung an fremde Staaten oder auswärts agierende Unternehmen die Staaten aus der Pflicht entlassen, das Recht auf Privatsphäre zu achten. Auch sei die Unterscheidung zahlreicher Überwachungsregime zwischen Staatsangehörigen und Ausländern unvereinbar mit dem Diskriminierungsverbot aus Artikel 26 UN-Zivilpakt.

3.6 Effektive Kontrolle und individuelle Beschwerderechte

Die Rechtsschutzgarantie aus Artikel 17 Absatz 2 UN-Zivilpakt erschöpfe sich nicht in Gesetzestexten. Diese müssten mit Leben gefüllt werden durch Verfahrenssicherheiten sowie effektive und angemessen ausgestattete Aufsichtsmechanismen. Dabei sollten interne Kontrollen staatlicher Überwachung durch eine von der Exekutive unabhängige Aufsicht ergänzt werden. Allerdings seien weder Richtervorbehalte noch parlamentarische Kontrollgremien ein Wundermittel. Der Richtervorbehalt sei nicht selten zur pro-forma Übung („rubber-stamping") verkommen, und parlamentarischen Gremien fehlten mitunter die Unabhängigkeit, der Wille als auch die Ressourcen für eine effektive Aufsicht. Entsprechend favorisiert der Bericht Modelle einer gemischten Aufsicht durch Verwaltung, Judikative und Parlamente, zeigt sich aber darüber hinaus interessiert an Ideen, Vertreter des „öffentlichen Interesses" und dritter Parteien, wie zum Beispiel Internetdienstleister, in die Verfahren zur Genehmigung von Überwachung mit einzubeziehen.

Zur Eröffnung effektiver Beschwerdemöglichkeiten seien, erstens, das Wissen um die Beschwerdewege und die Zulässigkeit von Beschwerden auch im Falle mangelnder Pflichten, Betroffene über die Überwachung zu informieren, unabdingbar; zweitens eine zügige, gründliche und unparteiische Ermittlung von mutmaßlichen Verletzungen des Rechts auf Privatsphäre (insbesondere hier sieht der Bericht eine besondere Rolle für unabhängige Aufsichtsgremien). Drittens müsse im Falle einer Rechtsverletzung Abhilfe durch Löschung der gespeicherten Daten oder andere Formen des Schadensersatzes garantiert sein. Viertens müssten im Falle von massenhaften Rechtsverletzungen auch strafrechtliche Konsequenzen folgen.

3.7 Zur menschenrechtlichen Verantwortung der Informations- und Kommunikationsunternehmen

Nicht zuletzt sieht der Bericht eine Verantwortung bei den privaten Unternehmen, ohne deren Kooperation eine staatliche Massenüberwachung in den meisten Fällen nicht denkbar wäre. Auch wenn es legitime Gründe für das staatliche Anzapfen privater Infrastrukturen gebe und die Konzerne häufig per Gesetz zur Zusammenarbeit verpflichtet seien, machten sie sich doch mitschuldig, wenn sie staatlichen Forderungen nachkämen, die das Menschenrecht auf Privatsphäre verletzten. Daher erinnert der Bericht an die UN-Leitprinzipien für Wirtschaft und Menschenrechte von 2011 und die dort deklarierte Verantwortung der Unternehmen, Menschenrechte bei ihrer gesamten Geschäftstätigkeit und unabhängig vom Standort ihrer Kunden zu achten. In der Praxis könne dies bedeuten, dass die Unternehmen staatliche Forderungen nach Überwachungskooperation möglichst eng auslegen, eine Klärung ihrer Reichweite und Rechtsgrundlage verlangen oder Transparenz gegenüber den Kunden herstellen.

4 Reaktionen auf den Bericht und eine neue Resolution der Generalversammlung

Am 12. September 2014 wurde der Bericht von Fachleuten und Staatenvertretern in Genf diskutiert. Im freundlichen und nicht selten heuchlerischen Diplomatensprech bekannten sich letztere einstimmig zum Menschenrecht auf Privatheit und betonten dessen grundlegende Bedeutung im digitalen Zeitalter. Insbesondere Länder des globalen Südens zeigten sich jedoch besorgt über die extraterritorialen Überwachungsaktivitäten einiger „großer Staaten“, ohne die USA namentlich zu nennen. Die Volksrepublik China machte deutlich, dass sie darin nicht nur eine Gefahr für die Menschenrechte ihrer Bürger_innen sehe, sondern auch für ihre staatliche Souveränität, und schlug einen zwischenstaatlichen Verhaltenskodex vor. Ähnlich nannte auch Russland „digitale Spionage“ eine „gefährliche Gewohnheit“. Westliche Staaten wie Kanada prangerten hingegen die Überwachung durch autoritäre Regime an; und die USA – sekundiert vom Vereinigten Königreich – beharrten hartnäckig auf ihrer Rechtsauffassung, dass Staaten außerhalb ihres Territoriums nur in Ausnahmefällen an die Menschenrechte gebunden seien. Allerdings erklärte der Vertreter Washingtons, dass sich seine Regierung mit der Frage auseinandersetze, wie die Rechte von Nicht-US-Bürger_innen zu schützen seien. Ob er sich damit auf den mittlerweile gescheiterten „Freedom Act“ zur Reform der NSA-Überwachung bezog oder generelle Überlegungen meinte, blieb unklar. Zudem spielte er die Frage zurück, wie effektive Kontrolle und Transparenz gewährleistet werden könne, wenn Geheimhaltung notwendig sei.[13]

In der Debatte wurden die wesentlichen Streitpunkte deutlich: Wann sind Eingriffe in das Recht auf Privatheit verhältnismäßig? Wie kann eine effektive Kontrolle gewährleistet werden? Wie ist extraterritoriale Überwachung durch Staaten oder multi-

nationale Konzerne zu behandeln? Und nicht zuletzt implizit: Wo verlaufen die Grenzen zur Cyberkriegsführung, für die es eigene völkerrechtliche Kontrollabkommen braucht.

Rückendeckung erhielt der Bericht der UN-Menschenrechtskommissarin vom gegenwärtigen UN-Sonderberichterstatter für die Achtung der Menschenrechte bei der Terrorismusbekämpfung, Ben Emmerson, der Ende September seinen Jahresbericht zum Schwerpunktthema Massenüberwachung vorlegte.[14] Doch obwohl Emmerson, ein US-Amerikaner, in zahlreichen Punkten, wie der Notwendigkeit effektiver Kontrolle, der Sensibilität von Metadaten oder der Verantwortung der Diensteanbieter, mit dem Pillay-Bericht übereinstimmt, bleibt er in einem entscheidenden Punkt widersprüchlich und zaghaft, wenn er einerseits schreibt: „Die harte Wahrheit ist, dass die Nutzung massenhafter Überwachung letztlich das Recht auf Privatheit von Kommunikation im Internet vollständig entsorgt“ (Rn. 12), und andererseits schlussfolgert: „Die Prävention und Repression von Terrorismus ist ein Gebot des öffentlichen Interesses von höchster Bedeutung und kann im Prinzip die Grundlage bilden für eine diskutierbare Rechtfertigung für die Massenüberwachung des Internet.“ (Rn. 59) Auch wenn er erhebliche Zweifel an der Verhältnismäßigkeit solcher Maßnahmen äußert, will er letztlich nicht ausschließen, dass es Umstände geben kann, die eine flächendeckende Überwachung rechtfertigen. Damit unterscheidet sich der Tenor von Emmersons Bericht deutlich von jenem des Pillay-Berichtes. Allerdings empfiehlt auch er, wie schon seine Kollegen Martin Scheinin und Frank La Rue, dem Menschenrechtsausschuss, die Allgemeine Bemerkung zu Artikel 17 zu aktualisieren.

Aufbauend auf den diversen Vorarbeiten lancierte eine von europäischen und südamerikanischen Ländern dominierte Staatengruppe, wieder unter Führung Deutschlands und Brasiliens, im Dritten Ausschuss der Generalversammlung eine neue Resolution zum Recht auf Privatheit im digitalen Zeitalter,[15] die schließlich auf den Tag genau ein Jahr nach Verabschiedung ihrer Vorgängerresolution am 18. Dezember 2014 ohne Abstimmung von der Generalversammlung angenommen wurde.[16] In weiten Teilen ähnelt der Text jenem von 2013: Wieder wird bestätigt, dass Menschenrechte offline ebenso wie online zu gelten haben, und willkürliche Überwachung ein Verstoß gegen das Menschenrecht auf Privatheit sei. Neu und deutliche Referenz gegenüber den Arbeiten Pillays und Emmersons sind aber die Verweise darauf, dass aggregierte Metadaten personenbezogene Informationen enthüllen können, und auf die menschenrechtliche Verantwortung von Unternehmen. Neu ist außerdem der Appell an die UN-Mitglieder, den Zugang zu einem effektiven Rechtsbehelf zu garantieren, wenn Menschen von willkürlichen Überwachungsmaßnahmen betroffen waren. Abschließend wird der Menschenrechtsrat „ermutigt“, sich weiterhin mit dem Thema zu beschäftigen und einen Sonderberichterstatter einzusetzen, um Prinzipien, Standards und „Best Practices“ zum Schutz der Privatheit zu identifizieren und zu präzisieren.

5 Wie weiter?

Im Vergleich zu Martin Scheinins Idee einer globalen Datenschutz-Erklärung bleiben die Hausaufgaben, die die Generalversammlung dem Menschenrechtsrat nun aufgegeben hat, bescheiden. Doch angesichts des Ausmaßes der Überwachung nicht nur durch die „Five Eyes“ und der enormen Widerstände gegen Reformen hielt schon der Bericht der UN-Menschenrechtskommissarin keine einfachen Antworten parat. Ein dauerhafter und konzertierter „Multi-Stakeholder“-Dialog unter Einbeziehung von Regierungen, Zivilgesellschaft, Unternehmen, wissenschaftlichen und technischen Vereinigungen sowie Menschenrechtsexpert_innen, so hieß es dort, sei wünschenswert, um den technischen Fortschritt für die Verwirklichung der Menschenrechte fruchtbar zu machen.

Mit der Ausrichtung der NETmundial, einer internationalen Konferenz zur Zukunft der Regierung des Internet, hatte Brasilien unter dem Eindruck der NSA-Spionage im April 2014 einen Anlauf zu einem solchen „Multi-Stakeholder“-Dialog gemacht. Dass deren Abschlusserklärung beim Thema Recht auf Privatheit im Prinzip nur den allgemeinen Appell der Resolution der Generalversammlung wiederholte,[17] zeigt, wie weit der Weg zu elaborierten globalen Standards ist.

Bislang haben internationale Instrumente zum Datenschutz – wie die Europarat-Konvention Nr. 108, die EU-Datenschutzrichtlinie, die OECD Privacy Guidelines oder der APEC Privacy Framework – nur eine begrenzte Reichweite und – meist auch – Verbindlichkeit.[18] Flankiert wurden die Bemühungen um globale Harmonisierung fast ausschließlich durch die überschaubare internationale Konferenz der Datenschutzbeauftragten aus etwa 40 Ländern und wenige spezialisierte Nichtregierungsorganisationen wie Privacy International.

Seit dem „Summer of Snowden“ haben sich jedoch auch die großen, global agierenden Menschenrechtsorganisationen wie Amnesty International oder Human Rights Watch das Thema auf die Fahnen geschrieben.[19] Mit der erwartbaren Einsetzung eines UN-Sonderberichterstatters für das Recht auf Privatheit durch den Menschenrechtsrat und der absehbaren Modernisierung der Allgemeinen Bemerkungen zu Artikel 17 des Zivilpaketes durch den Menschenrechtsausschuss besteht daher nun die Hoffnung,[20] dass im Kreis einer wirklich globalen „Community“ das Menschenrecht auf Privatheit zumindest als „soft law“ weiterentwickelt wird.[21] Kaum zu ignorieren wären solche „weichen“ Standards beispielsweise bei zukünftigen Diskussionen im UN-Sicherheitsrat und seinem Ausschuss für Terrorismusbekämpfung. Zudem könnten sie – unter anderem über die regelmäßigen Staatenberichtsverfahren vor den Ausschüssen zur Überwachung der Menschenrechtskonventionen – auch Impulse auf nationaler Ebene setzen.

Davon könnte nicht zuletzt auch die deutsche Diskussion profitieren. Für die Auseinandersetzungen um die Zukunft der Vorratsdatenspeicherung, die Auslandsüberwachung des Bundesnachrichtendienstes, das Trennungsgebot zwischen Polizei und Geheimdiensten, die zögerlichen Spionage-Ermittlungen des Generalbundesanwaltes oder die Aufklärungsbemühungen des NSA-Untersuchungsausschusses bieten die menschenrechtlichen Diskussionen der UN-Gremien gewichtige Argumente, die mit-

unter – wenn es beispielsweise um die grundsätzliche Absage an Geheimgerichte wie im Pillay-Bericht geht – durchaus über den hiesigen Status quo hinausweisen.

ERIC TÖPFER Jahrgang 1970, Politologe, ist wissenschaftlicher Mitarbeiter am Deutschen Institut für Menschenrechte, der unabhängigen nationalen Menschenrechtsinstitution Deutschlands, dort zuständig für den Bereich Menschenrechte im Politikfeld Innere Sicherheit. Zuvor war er wissenschaftlicher Mitarbeiter an der Technischen Universität Berlin und Research Consultant für die britische NGO *Statewatch*. Eine Liste seiner Publikationen findet sich unter: www.emato.de. Der Beitrag gibt die persönliche Ansicht des Autors wieder.

Anmerkungen:

1 Oliver Diggelmann, Maria N. Cleis (2014): How the right to privacy became a human right. In: Human Rights Law Review, Vol. 14, S. 441-458.
2 So der Soziologe David Lyon (1994): The Electronic Eye. The Rise of Surveillance Society. Minneapolis, S. 14.
3 Human Rights Committee (1988): CCPR General Comment No. 16 vom 08.04.1988.
4 UN-Dok. A/HRC/13/37 vom 28.12.2009.
5 UN-Dok. A/HRC/23/40 vom 17.04.2013. La Rue vertiefte damit seine Vorarbeiten zum Thema Internet und freie Meinungsäußerung. Siehe hierzu UN-Dok. A/HRC/17/27 vom 16.05.2011.
6 Bundesregierung: NSA-Aufklärung – Deutschland ist ein Land der Freiheit. Pressemitteilung vom 19.07.2013, online unter: http://www.bundesregierung.de/ContentArchiv/DE/Archiv17/Artikel/2013/07/2013-07-19-bkin-nsa-sommerpk.html.
7 Carla Stea: Latin America Condemns US Espionage at United Nations Security Council, 17.08.2013. Online unter: http://www.globalresearch.ca/latin-america-condemns-us-espionage-at-united-nations-security-council/5346120.
8 Colum Lynch: Germany, Brazil turn to U.N. to Restrain American Spies, 24.10.2013. Online unter: http://foreignpolicy.com/2013/10/24/exclusive-germany-brazil-turn-to-u-n-to-restrain-american-spies/.
9 UN-Dok. A/C.3/68/L.45 vom 01.11.2013.
10 UN surveillance resolution goes ahead despite attempts to dilute language, in: The Guardian vom 21.11.2013, online unter: http://www.theguardian.com/world/2013/nov/21/un-surveillance-resolution-us-uk-dilute-language.
11 UN-Dok. A/RES/68/167 vom 18.12.2013.
12 UN-Dok. A/HRC/27/37 vom 16.07.2014.
13 Office of the High Commissioner for Human Rights (2014): Human Rights Council holds panel discussion on the right to privacy in the digital age, Pressemitteilung vom 12.09.2014.
14 UN-Dok. A/69/397 vom 23.09.2014.
15 Danny Palmer: Germany and Brazil propose UN resolution re-write to condemn 'highly intrusive act' of NSA surveillance, 07.11.2014, online unter: http://m.computing.co.uk/ctg/news/2380180/

germany-and-brazil-propose-un-resolution-re-write-to-condemn-highly-intrusive-act-of-nsa-surveillance.

16 UN-Dok. A/RES/69/166. Da das Dokument bis zum Redaktionsschluss noch nicht veröffentlich war, bezieht sich die Darstellung des Inhalts auf den Entwurf UN-Dok. A/C.3/69/L.26/Rev.1 vom 19.11.2014.

17 NETmundial Multi-Stakeholder Statement vom 24.04.2014, online unter: http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

18 Siehe hierzu: Colin J. Bennett und Charles D. Raab (2006): The Governance of Privacy. Policy Instruments in a Global Perspective. Cambridge/London.

19 Siehe z.B. Dinah PoKempner (2014): The Right Whose Time Has Come (Again). Privacy in the Age of Surveillance, in: Human Rights Watch World Report 2014. New York, S. 41.52, online unter: http://www.hrw.org/world-report/2014/essays/privacy-in-age-of-surveillance.

20 Nach den verschiedenen UN-Sonderberichterstattern hat auch die einflussreiche American Civil Liberties Union einen Vorstoß zur Modernisierung der Allgemeinen Bemerkung Nr. 16 unternommen: ACLU (2014): Privacy rights in the digital age. A proposal for a new General Comment on the right to privacy under Article 17 of the International Covenant on Civil and Political Rights. A draft report and General Comment by the American Civil Liberties Union. New York, online unter: https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf.

21 Vgl. das Plädoyer von Anna Crowe: The need for a Special Rapporteur on the Right to Privacy at the UN, online unter: https://www.privacyinternational.org/blog/the-need-for-a-special-rapporteur-on-the-right-to-privacy-at-the-un.