Dokumentation

Menschenrechte im digitalen Zeitalter

Aktueller Forschungs- und Diskussionsstand

Menschenrechte im digitalen Zeitalter
Aktueller Forschungs- und Diskussionsstand

Aktenzeichen:	WD 2 - 3000 - 107/18
Abschluss der Arbeit:	3. August 2018 (zugleich Zeitpunkt des letzten Abrufs der Internetquellen)
Fachbereich:	WD 2 - Auswärtiges, Völkerrecht, wirtschaftliche Zusammenarbeit und Entwicklung, Verteidigung, Menschenrechte und humanitäre Hilfe

Inhaltsverzeichnis

1. Einleitung – das digitale Zeitalter

> At present – when most information is spread and carried on in a digital form, when communication technologies such as smartphones and free internet access ubiquity have become part of daily life, when commerce, health and financial services, education and entertainment, social platforms and infrastructures are provided online and in real-time – contemporary life is increasingly moving in the direction of becoming a "transparent society". Information technologies and computing systems that record our every keystroke and physical movement are dissolving the borders between the individual, state and private enterprise. **We live in the, so called, "digital age".**[1]

Der Prozess der Digitalisierung wirkt sich tiefgreifend auf sämtliche Lebensbereiche aus und ist somit auch für die Ausübung der Menschenrechte und die Gestaltung eines wirksamen Menschenrechtsschutzes von erheblicher Relevanz. Die Situation der Menschenrechte im digitalen Zeitalter ist sowohl in der gesellschaftlichen Diskussion als auch in der wissenschaftlichen Literatur jüngst verstärkt in den Blick gerückt und soll daher Gegenstand dieser Dokumentation sein, die die grundlegenden Ansichten und Tendenzen in diesem Kontext strukturiert aufbereitet.[2]

Aufgezeigt werden zunächst die Charakteristika des sog. digitalen Zeitalters (1.), die Bedeutung, historische Entwicklung und Entwicklungsperspektiven der Menschenrechte im Allgemeinen (2.) und das grundlegende Spannungsfeld, in dem sich die Menschenrechte im digitalen Zeitalter bewegen (3.). Anschließend werden die konkreten Transformationsprozesse der Menschenrechte im digitalen Zeitalter dargestellt (4.), wobei neben den strukturellen Veränderungen auf die konkret betroffenen Rechte eingegangen wird, besonders ausführlich auf das Recht auf Privatsphäre. Es folgt schließlich ein Ausblick mit Nennung der konkreten Forderungen aus dem menschenrechtlichen Diskurs und den bereits bestehenden Initiativen.

Zunächst zum **Prozess der Digitalisierung** insgesamt: Der Prozess der Digitalisierung zeichnet sich dadurch aus, dass er gesellschaftliche Verhältnisse in transnationaler Dimension grundlegend wandelt. Dadurch wird insbesondere die Art und Weise verändert, in der Menschen kommunizieren und Informationen austauschen.

> Durch die Digitalisierung aller Lebensbereiche haben sich zahlreiche **soziale und kulturelle Veränderungen** ergeben. Neben diesen spürbaren Auswirkungen auf das Leben jeder einzelnen Person, hat der digitale Wandel aber auch Einfluss [auf] Politik und Recht genommen. Dabei ist es eines der Merkmale der Digitalisierung, dass sie vielfach nicht in nationalen Mustern oder etablierten Strukturen betrachtet werden kann, sondern **über die Grenzen von Ländern und Kulturen hinwegfliesst**. So sind auf der juristischen Ebene auch das Völkerrecht, - und mit ihm die Menschenrechte der Allgemeinen Erklärung von 1948 betroffen. […]

---

1 Damen/Köhler/Woodard, *The Human Right of Privacy in the Digital Age*, Staat, Recht und Politik – Forschungs- und Diskussionspapiere, Bd. 3 (2017), S. 2, verfügbar unter https://publishup.uni-potsdam.de/opus4-ubp/frontdoor/deliver/index/docId/39926/file/srp03.pdf.

2 Hervorhebungen in den Zitaten wurden nachträglich hinzugefügt. Rechtschreib- und Grammatikfehler in den Zitaten wurden überwiegend nicht korrigiert. Erfolgte Korrekturen sind durch eckige Klammern gekennzeichnet.

> Die Digitalisierung dringt zunehmend in jeden Aspekt unseres Lebens. Unsere Kommunikation, unsere politische Willensbildung, und die Gestaltung unseres Privatlebens finden immer häufiger und umfassender mit elektronischer Unterstützung statt. Das macht diese Kommunikation einfacher, schneller und für mehr Menschen zugänglich. Es ermöglicht den leichteren Austausch und die Verbreitung von Informationen bei geringeren Kosten. Wir können so Dinge und Interessen schneller und leichter koordinieren, kontrollieren und dokumentieren. Vernetzung lässt zusätzlich vieles transparenter werden und geographische Entfernungen weniger ins Gewicht fallen.
>
> Im Jahr 2013 waren schätzungsweise 41,3 Prozent der Haushalte weltweit mit dem Internet verbunden und 38,8 Prozent der Weltbevölkerung waren regelmäßig online. Mobilfunkabonnements erreichen sogar 96 Prozent der globalen Bevölkerung. Die zunehmende Verbreitung von Mobiltelefonen und Smartphones stellt dabei einen großen Bereich der Online-Abdeckung in sog. Entwicklungsländern. […] Diese Zahlen lassen die Eingriffstiefe der Digitalisierung nur erahnen.
>
> Diese Entwicklungen sind ganz konkret auch für die Menschenrechte relevant.[3]

2. Bedeutung und Entwicklungsoffenheit der Menschenrechte

2.1. Begriff und Schutzdimensionen der Menschenrechte

Unter Menschenrechten versteht man allgemein **die universellen, natürlichen – also im Sinne eines Naturrechts angeborenen – und unveräußerlichen Rechte**, die dem Einzelnen gegenüber dem Staat alleine aufgrund seines Menschseins zustehen und im Völkerrecht verbrieft sind.[4] Die Rechte sind konkret in völkerrechtlichen Verträgen kodifiziert oder durch Völkergewohnheitsrecht anerkannt.[5]

Ihnen liegt das aufklärerische Prinzip zugrunde, dass jeder Mensch von Geburt an im Besitz eines unantastbaren, unveräußerlichen Rechts ist, das ihn als Individuum vor jeder willkürlichen oder menschenunwürdigen Behandlung schützt, die ihn zu einem bloßen Objekt fremden Tuns werden lässt.[6] Parallele Rechte sind häufig auch in den nationalen Verfassungen verbrieft. Diese Grundrechte unterscheiden sich von den Menschenrechten jedoch dadurch, dass sie nicht per se

---

3 Karst, *Menschenrechte im digitalen Zeitalter*, der Freitag, 25. Februar 2015, verfügbar unter https://www.freitag.de/autoren/mike-karst/menschenrchte-im-digitalen-zeitalter.

4 Buergenthal, "Human Rights" (2007), *Max Planck Encyclopedia of Public International Law*, verfügbar unter: http://opil.ouplaw.com/home/EPIL; Engelmann, *Menschenrechte und Vereinte Nationen*, UN Basis-Informationen 40 (Deutsche Gesellschaft für die Vereinten Nationen) (2011), S. 1; Krennerich, *Menschenrechte - ein allgemeiner Einstieg*, Handbuch der Menschenrechtsarbeit 2014/2015 (Friedrich-Ebert-Stiftung), S. 7, 7.

5 Buergenthal, "Human Rights" (2007), *Max Planck Encyclopedia of Public International Law*.

6 Duden-Redaktion, „Menschenrechte", *Duden Recht A-Z* (3. Aufl. 2015), verfügbar unter http://www.bpb.de/nachschlagen/lexika/recht-a-z/22559/menschenrechte.

universell, also für alle Menschen gelten und erst durch ihre Normierung gültig werden.[7] Menschenrechte können durch ihre Normierung demgegenüber lediglich als vorhanden anerkannt werden.[8] Dies kommt etwa in Art. 1 Abs. 2 GG zum Ausdruck, wonach sich das deutsche Volk zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt bekennt.

Den Menschenrechten werden heute **mehrere Schutzdimensionen** beigemessen: Neben dem abwehrrechtlichen Schutz vor staatlichen Eingriffen (Achtungspflichten bzw. Abwehrrechte; „obligations to respect“) gewährleisten sie staatlichen Schutz vor Eingriffen durch Dritte (Schutzpflichten; „obligations to protect“) und verpflichten die Staaten, die Ausübung eines Rechts durch positive Maßnahmen überhaupt erst zu ermöglichen (Gewährleistungspflichten; „obligations to fulfill“).[9]

2.2. Historie und Entwicklungsoffenheit der Menschenrechte im digitalen Zeitalter

2.2.1. Kurzüberblick über die Historie der Menschenrechte

Der **historische Ursprung** der Menschenrechte reicht ins 18. Jahrhundert zurück. In ihrer Anfangszeit haben Menschenrechte zunächst nur in die nationalen Verfassungen Eingang gefunden, etwa in die Virginia Bill of Rights und die amerikanische Unabhängigkeitserklärung von 1776 und die französische Erklärung der Menschen- und Bürgerrechte von 1789, und waren dadurch vorrangig an die Staatsbürgerschaft gekoppelt.[10]

Der moderne Menschenrechtsschutz beginnt im Wesentlichen erst mit der Charta der Vereinten Nationen von 1945 und der Allgemeinen Erklärung der Menschenrechte der Vereinten Nationen (AEMR) von 1948.

> **Die AEMR** – eigentlich besser übersetzt als „Universelle Erklärung der Menschenrechte“ – ist hierbei von überragender Bedeutung und entwickelte eine damals kaum für möglich gehaltene moralische, politische und inzwischen auch rechtliche Wirkkraft. Ursprünglich als völkerrechtlich unverbindliche Erklärung verabschiedet, enthält sie allgemeine Rechtsprinzipien und Garantien, die

---

7 Engelmann, *Menschenrechte und Vereinte Nationen*, UN Basis-Informationen 40 (Deutsche Gesellschaft für die Vereinten Nationen) (2011), S. 1.

8 Duden-Redaktion, „Menschenrechte“, *Duden Recht A-Z* (3. Aufl. 2015).

9 Krennerich, *Menschenrechte - ein allgemeiner Einstieg*, Handbuch der Menschenrechtsarbeit 2014/2015 (Friedrich-Ebert-Stiftung), S. 7, 15, verfügbar unter http://handbuchmenschenrechte.fes.de/files/fes_hdmr/pdf-files/Handbuch__MR_Gesamt.pdf.

10 Ebd.

heute völkergewohnheitsrechtlich anerkannt sind. Sie ist der wichtigste Referenzpunkt für Menschenrechtsbewegungen weltweit und bildet die Grundlage für viele Menschenrechtsabkommen, die im Geiste der AEMR erarbeitet wurden.

Die allermeisten Rechte der AEMR wurden später in zwei völkerrechtlich verbindliche Verträge überführt: den **Internationalen Pakt über bürgerliche und politische Rechte** sowie den **Internationalen Pakt über wirtschaftliche, soziale und kulturelle Rechte** (wsk-Rechte), die beide 1966 verabschiedet wurden und 1976 in Kraft traten. Sie wurden im Laufe der Zeit durch eine Reihe internationaler Abkommen ergänzt. Diese garantieren nicht einfach neue Menschenrechte. Vielmehr konkretisieren und erweitern sie die bereits zuvor verankerten Menschenrechte aus der spezifischen Sicht bestimmter Bevölkerungsgruppen (Frauen, Kinder, Wanderarbeiter_innen, Menschen mit Behinderung) und nehmen besondere menschenrechtliche Probleme in den Blick (Rassismus, Folter, „Verschwindenlassen“).[11]

Davon ausgehend hat sich der Menschenrechtsschutz in vielfältiger Hinsicht weiterentwickelt:

Zusätzlich wurden in Europa, Amerika und Afrika **regionale Menschenrechtsschutzsysteme** entwickelt. Zugleich wirkte die Entwicklung des internationalen Menschenrechtsschutzes **auf die nationale Ebene** zurück. Vor allem jüngere Verfassungen umfassen ein breites Spektrum an Grund- und Menschenrechten. Dynamisch entwickelte sich in den vergangenen Jahren auch das internationale Strafrecht, das durch die Gründung des Internationalen Strafgerichtshofes erheblich an Bedeutung gewann und Völkermord, Verbrechen gegen die Menschlichkeit und Kriegsverbrechen ahndet.[12]

Heute werden drei Generationen von Menschenrechten unterschieden, um den Wandel in ihrer Ausrichtung zu systematisieren:

Rechte der ersten „Generation“ bezeichnen die klassischen bürgerlichen und politischen Freiheits- und Beteiligungsrechte. Dazu gehören das Recht auf Leben, die Verbote der Folter, der Sklaverei und der Zwangsarbeit, sodann u. a. die Rechte auf persönliche Freiheit und Sicherheit, Gedanken-, Religions-, Meinungs-, Versammlungs-, Vereinigungsfreiheit sowie justizbezogene Rechte (Gleichheit vor dem Gesetz, Unschuldsvermutung, faires Verfahren etc.). Die nationalen und internationalen Schutzsysteme für bürgerlich-politische Rechte sind bislang am stärksten ausgebaut.

Rechte der zweiten „Generation“ umfassen die lange Zeit vernachlässigten wirtschaftlichen, sozialen und kulturellen Menschenrechte, wie die Rechte auf und in Arbeit, auf soziale Sicherheit, Ernährung, Wohnen, Wasser, Gesundheit und Bildung. Seit den 1990er Jahren wurden der Inhalt und die Verletzungstatbestände dieser Rechte erheblich konkretisiert. Inzwischen werden sie weithin politisch eingefordert und gelten ihrem Wesen nach auch als einklagbar. Entsprechende rechtliche Durchsetzungsmechanismen auf nationaler und internationaler Ebene sind indes noch zu stärken.

---

11 Ebd.

12 Krennerich, *Zehn Fragen zu Menschenrechten*, Dossier Menschenrechte, Bundeszentrale für politische Bildung (2009), verfügbar unter http://www.bpb.de/internationales/weltweit/menschenrechte/38627/zehn-fragen.

Rechte der dritten „Generation“ sind jüngeren Datums und bezeichnen allgemeine, noch kaum in Vertragswerken konkretisierte Rechte wie etwa die Rechte auf Entwicklung, Frieden oder saubere Umwelt.[13]

2.2.2. Entwicklungsoffenheit der Menschenrechte, insbesondere im digitalen Zeitalter

Spezifische **Fragen der Digitalisierung** haben sich in dieser Differenzierung noch nicht niedergeschlagen. Es ist auch nicht zwingend zu erwarten, dass das Zeitalter der Digitalisierung tatsächlich eine neue Generation von Menschenrechten hervorbringen wird. Der Schwerpunkt des Transformationsprozesses wird stattdessen überwiegend auf dem Feld der bereits bestehenden Menschenrechte gesehen, die sich im digitalen Zeitalter einer radikal veränderten Lebenswirklichkeit vieler Menschen gegenüber sehen und auf diese reagieren müssen. Inhaltlich neue Rechte werden demgegenüber nur vereinzelt ins Spiel gebracht.

Der Wandel der Menschenrechte folgt generell keinem bestimmten Mechanismus, sondern kann sich auf unterschiedliche Weise vollziehen:

> Als Ergebnis geschichtlicher Prozesse unterliegen die völkerrechtlich verankerten Menschenrechte auch weiterhin einem Wandel. Selbst wenn die „Normsetzung“ weit vorangeschritten ist, kann der **„Katalog“ der Menschenrechte verändert und erweitert werden**. In den vergangenen Jahrzehnten wurden zahlreiche Menschenrechtsabkommen erarbeitet, welche die in der AEMR postulierten Rechte ausdifferenzierten und auf verletzliche Bevölkerungsgruppen und besondere menschenrechtliche Probleme hin konkretisierten. Prinzipiell ist anzunehmen, dass neue Unrechtserfahrungen und künftige Veränderungen in den menschlichen Lebensbedingungen und Sozialbeziehungen (etwa im Bereich der Gentechnik oder der **digitalen Kommunikation**), verbunden mit der Kritik an Unzulänglichkeiten des bestehenden Menschenrechtsschutzes, auch **weiterhin neue Menschenrechte hervorbringen** werden.
>
> Zugleich stellen **Menschenrechtsabkommen „living instruments“** dar. Das Verständnis der bereits normierten, in Menschenrechtsabkommen verankerten Rechte ist nicht starr. Viele völkerrechtliche und politische Debatten kreisen gegenwärtig weniger um die Festschreibung neuer Menschenrechte als um eine **zeitgemäße Auslegung bestehender Rechte**. Ein Beispiel hierfür sind die sozialen Menschenrechte. Durch ihre inhaltliche Konkretisierung und Weiterentwicklung, gerade auf der VN-Ebene, haben sich das Verständnis und die Bedeutung dieser Rechte seit den 1990er Jahren erheblich verändert. Soziale Menschenrechte werden dementsprechend auch nicht mehr als vage, unverbindliche Programmsätze wahrgenommen, sondern als näher bestimmte, einforderbare und einklagbare Rechte.
>
> Die **historische Entwicklungsoffenheit** der Menschenrechte bedeutet allerdings nicht Beliebigkeit: Die Festschreibung neuer und die Neu-Interpretation bestehender Menschenrechte sind zwar notwendig, um sich ändernden Gegebenheiten und Problemen Rechnung zu tragen, doch sind sie stets

13 Ebd.

> daraufhin zu prüfen, ob sie sich inhaltlich-systematisch in das Gefüge des bestehenden Menschenrechtsschutzes einbetten.[14]

Damit ist die Herausforderung umrissen, der sich die Menschenrechte im digitalen Zeitalter nach verbreiteter Einschätzung im Kern gegenübersehen: Es geht darum, die **Menschenrechte über ihren historischen Entstehungskontext hinaus auf die heutige digitalisierte Welt zu beziehen**, um mit einem etablierten Instrumentarium auf neue Herausforderungen reagieren zu können.

Grundlage dessen können nicht nur völkerrechtliche Normen sein. Vielmehr muss ein gesellschaftlicher, politischer und juristischer **Diskurs** über die Frage stattfinden, welcher Gehalt den Menschenrechten unter den veränderten Lebensumständen der Menschen beizumessen und wie dieser weiterzuentwickeln ist:

> In die konkrete Ausgestaltung und Weiterentwicklung der Menschenrechte gehen ideengeschichtliche und verfassungsrechtliche Traditionen ebenso ein wie konkrete historische Erfahrungen von Unterdrückung und Not.
>
> Allerdings wurden und werden die Menschenrechte so allgemein formuliert, dass sie in ihrem Geltungsanspruch weit über die historischen Entstehungszusammenhänge hinausweisen und sie offen sind für unterschiedliche Begründungen und für unter schiedliche Kontexte, mit je eigenen Traditionen und Unrechtserfahrungen. Dabei tragen sie stets einen moralischen Gehalt in sich.
>
> Die Frage, was als Menschenrecht faktisch anerkannt wird, hängt daher nicht nur von der völkerrechtlichen Normsetzung ab, sondern **auch von der moralischen Begründung sowie der politischen und gesellschaftlichen Anerkennung der Menschenrechte**, die ihnen zuteil wird. Hierzu ist ein **offener Menschenrechtsdiskurs** vonnöten, der letztlich die Grundlage dafür bildet, was als Menschenrecht tatsächlich anerkannt wird.[15]

3. Grundlegendes Spannungsfeld zur Situation der Menschenrechte im digitalen Zeitalter: Chancen und Risiken

Während Einigkeit hinsichtlich der Einschätzung besteht, dass die weitreichende Entwicklung von Informationstechnologie Fragen der Menschenrechte in vielerlei Hinsicht beeinflusst, fällt die Bewertung dieser Entwicklung unterschiedlich aus. Die Debatten bewegen sich dabei grundlegend im Spannungsfeld zwischen Vorteilen und Chancen und Nachteilen und Risiken.

---

14 Krennerich, *Menschenrechte - ein allgemeiner Einstieg*, Handbuch der Menschenrechtsarbeit 2014/2015 (Friedrich-Ebert-Stiftung), S. 7, 24.

15 Ebd., S. 7 f.

3.1. Vorteile und Chancen

Der Blick wird einerseits auf die Vorteile und Chancen der Digitalisierung für die Menschenrechte gerichtet. Hierbei wird vor allem auf die enorm gesteigerten Möglichkeiten hingewiesen, im digitalen Zeitalter breitenwirksam seine Meinung kundzutun und somit an demokratischen Prozessen zu partizipieren, sich zu informieren und globale Debatten zu führen.[16]

> Über das Internet kann man seine Meinung äußern, sich mit anderen organisieren und koordinieren. Weltweit führt es dazu, dass Menschen einfacher ihr Recht auf Meinungs- und auf Versammlungsfreiheit wahrnehmen können. Außerdem erleichtert der Zugang zum Netz die Mitwirkung an öffentlichen Angelegenheiten, die Teilhabe am kulturellen Leben und am wissenschaftlichen Fortschritt und den Zugang zu Bildung, Arbeit und Gesundheit. In abgelegenen Regionen beispielsweise ist so der Zugang zu medizinischer Beratung – und damit zu einer wenn auch eingeschränkten medizinischen Versorgung – oft erst möglich.[17]

Besonders wird außerdem die Möglichkeit herausgestellt, **Menschenrechtsverletzungen durch digitale Medien anzuprangern** und so große Personenkreise auf Missstände im Menschenrechtsbereich aufmerksam zu machen:

> Durch die Verbreitung von Smartphones und Laptops können Verletzungen heute viel schneller und häufiger dokumentiert und berichtet werden, als dies noch vor 20 Jahren der Fall war. Öffentlichkeitsarbeit, die mühsam ausgebaut werden musste, kann heute beispielsweise von Bloggern - zumindest teilweise - selbst durchgeführt werden. Das Aufzeigen von Problemen und das Erarbeiten von Lösungen, ist also deutlich leichter geworden.
>
> Videomaterial kann einfach und unkompliziert auf Plattformen wie Youtube, Vimeo oder anderen platziert, und von Millionen Menschen weltweit gesehen und bewertet werden. Wer seine Videos, oder auch andere Datensätze dabei besonders anonym veröffentlichen möchte, der hat beispielsweise über Wikileaks die Chance dazu. Wir haben somit viel mehr Quellen, die wir miteinander vergleichen können um uns unsere Urteile zu bilden. Selbst „altmodische“ Menschenrechtsorganisationen wie Amnesty International oder Human Rights Watch haben dies bereits erkannt und sind bemüht, nun wiederum Werkzeuge zur Verfügung zu stellen, die den Umgang mit diesen neuen Datenmengen ermöglichen sollen. So hat Amnesty International mit dem Projekt „citizen evidence lab“ Anleitungen veröffentlicht, die erklären wie man die Echtheit von Videos überprüfen kann. Außerdem hat sie ein Programm veröffentlicht, welches zumindest die gängigsten Spähprogramme auf den eigenen Computern entdecken und entfernen soll. Zusätzlich wird mit einem „panic button“ als Handyapplikation versucht, die Arbeit von Menschenrechtsaktivistinnen und -aktivisten

---

16 Bericht des Amtes des Hohen Kommissars der Vereinten Nationen für Menschenrechte, A/HRC/27/37, 30. Juni 2014, *Das Recht auf Privatheit im digitalen Zeitalter*, S. 3, verfügbar unter http://www.un.org/depts/german/menschenrechte/a-hrc-27-37.pdf; Damen/Köhler/Woodard, *The Human Right of Privacy in the Digital Age*, Staat, Recht und Politik – Forschungs- und Diskussionspapiere, Bd. 3 (2017), S. 1; Karst, *Menschenrechte im digitalen Zeitalter*, der Freitag, 25. Februar 2015.

17 Amnesty International, *Menschenrechte im digitalen Zeitalter*, 4. Juni 2015, verfügbar unter https://www.amnesty.de/2015/6/4/digitalisierung-und-menschenrechte.

> sicherer zu machen. Dieses Programm übermittelt die Position seines Benutzers an einen Computer, um ihn oder sie im Falle einer Einführung oder Gefangennahme schnell auffinden zu können (Vgl. auch Art. 9, 13 AEMR). [18]

Einzelne Autoren heben in diesem Zusammenhang darüber hinaus gar auf gesetzesgemäß durchgeführte digitale **Überwachungsmaßnahmen** ab, die als effektives Werkzeug dem Schutz der Menschenrechte dienen könnten.[19]

> One side of the discussion argues that present technologies improve the realization of human rights. The United Nations High Commissioner for Human Rights (UNHCR) outlines the ways digital communication technologies have "improved enjoyment of human rights" inasmuch as the Information Age has "boosted freedom of expression, facilitated global debate and fostered democratic participation" (UN 2014a, A/HRC/27/37, 3). Moreover, especially in the debate about terrorism and security, when conducted in compliance with the law, surveillance of electronic communications data can be an effective and operational tool for legitimate law enforcement in order to protect human rights.[20]

3.2. Nachteile und Risiken

Andererseits werden die Nachteile, Gefahren und Risiken für die Menschenrechte in den Blick genommen, die sich im digitalen Zeitalter ergeben. Diese Dimension bildet den klaren Schwerpunkt der Debatte. Konkret wird hierbei primär die **Datenschutz-Problematik** diskutiert, die durch den Hochkommissar für Menschenrechte der Vereinten Nationen wie folgt eingeordnet wird:

> 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. Mit anderen Worten, die technologischen Plattformen, auf die sich das politische, wirtschaftliche und

---

18 Karst, *Menschenrechte im digitalen Zeitalter*, der Freitag, 25. Februar 2015.

19 Damen/Köhler/Woodard, *The Human Right of Privacy in the Digital Age*, Staat, Recht und Politik – Forschungs- und Diskussionspapiere, Bd. 3 (2017), S. 1.

20 Ebd.

soziale Leben weltweit zunehmend stützt, sind nicht nur anfällig für Massenüberwachung, sondern fördern diese vielleicht sogar. [21]

Auch in der Literatur liegt der **Fokus auf der Frage des Datenschutzes**:

> Das Internet, und insbesondere das World Wide Web können so einerseits als ein Katalysator für die Menschenrechte verstanden werden - sie sind aber auch eine enorme Bedrohung, wenn man versteht, dass das Recht auf Privatsphäre eine Grundvoraussetzung vieler anderer Rechte darstellt. [22]

> Conversely, these technologies have become a threat to human rights by facilitating surveillance, interception and collection of personal data. Worldwide, entities in government, the public, and private sector have become perpetrator and victim of invasive digital surveillance. Though espionage and surveillance have always been a part of sociopolitical reality, the introduction of powerful personal computation technologies to the consumer market have brought the same tactics of interference and manipulation to the individual level, redefining the contemporary frontier of human rights. "[...] the technological platforms upon which global political, economic and social life are increasingly reliant are not only vulnerable to mass surveillance, they may actually facilitate it" (UN 2014a, A/HRC/27/37, 3). In light of the 2013 revelations by Edward Snowden, detailing mass surveillance by US National Security Agency, the right to privacy and its protection seem to be seriously endangered and create new levels of debate (ibid., 3f). Indeed "one of the most discussed and worried-about aspects of today's Information Age is the subject of privacy" (Waldo et al. 2007, 19). [23]

Die Menschenrechte werden durch die **umfangreichen Datensammlungen** als in vielerlei Hinsicht bedroht betrachtet:

> Diejenigen Akteure, die andere Ziele, als den Schutz der Menschenrechte verfolgen, haben das Potential neuer vielfach Technologien bereist erkannt, und wenden diese Erkenntnisse an. Es lässt sich zeigen, dass zahlreiche Staaten bereits eigene Versuche unternehmen, mittels Informationsmanipulation oder Zensur die öffentliche Meinung teils subtil, teils offensichtlich zu beeinflussen, - oder der Bevölkerung den Zugriff auf digitale Kommunikationsmöglichkeiten insgesamt, oder teilweise zu verweigern. So werden die Möglichkeiten eventueller Opposition eingeschränkt. Hierdurch droht nicht nur ein Rückfall auf [den] Zustand, der mit dem, vor der Digitalisierung vergl[i]chen werden kann, sondern die Deutungshoheit des Staates nimmt durch die potentielle Omnipräsenz von Propaganda rapide zu.
>
> Es müssen aber noch mehr Veränderungen der sozialen Interaktion und Kommunikation berücksichtigt werden. Neben der direkten Einflussnahme auf den politischen Diskurs („Information war") drohen viele weitere, beispielsweise durch sogenannte „Chilling Effects", die sich aus den gestiegenen

---

21 Bericht des Amtes des Hohen Kommissars der Vereinten Nationen für Menschenrechte, A/HRC/27/37, 30. Juni 2014, *Das Recht auf Privatheit im digitalen Zeitalter.*

22 Karst, *Menschenrechte im digitalen Zeitalter*, der Freitag, 25. Februar 2015.

23 Damen/Köhler/Woodard, *The Human Right of Privacy in the Digital Age*, Staat, Recht und Politik – Forschungs- und Diskussionspapiere, Bd. 3 (2017), S. 1.

> Überwachungsmöglichkeiten und seinen psychologischen Folgen ergeben. Die Digitalisierung macht Interaktionen nämlich auch deutlich anfälliger für Überwachung.
>
> Da bereits aufgrund der technischen Notwendigkeit digitale Kommunikation mindestens vorübergehend irgendwo gespeichert werden muss, können diese Daten einfach analysiert und bewertet werden. Die Grenzkosten solcher Datensammlungen sind gering, und werden immer noch geringer. Die Daten, die die Staatssicherheit der DDR in ihrer gesamten Geschichte gesammelt hat, sind nichts im Vergleich zu dem, was heutige Dienste in wenigen Jahren sammeln können, und mit ihnen die Möglichkeiten, die sich aus solchen Sammlungen ergeben.
>
> Wenn wir also über die Bedeutung des Internets für die Situation der Menschenrechte sprechen, müssen wir beide Seiten beachten.
>
> Chancen und Risiken sind im digitalen Raum eng miteinander verbunden. [24]

Zusammenfassend wird überwiegend der Schluss gezogen, dass zur Eindämmung der genannten Risiken **aktive politische Maßnahmen** vonnöten sind, die mit der rasanten Entwicklung der Digitalisierung Schritt halten müssen.

> Verschiedene Interessen und technische Vorteile ergeben neben zahlreichen neuen Werkzeugen für ihren Schutz, auch eine immer größere Bedrohung für die Menschenrechte. Diese Entwicklung geht rasant voran, und wird sich in den nächsten Jahren und Jahrzehnten noch beschleunigen. Es gibt also viel zu tun, und nicht in allen Dingen sind Einzelstaaten von internationalen Regelungen abhängig.
>
> Leider haben die meisten nationalen Regierungen das Problem und seine Tragweite schlicht nicht erkannt, oder wollen es aus politischen oder wirtschaftlichen Gründen nicht erkennen.[25]

4. Konkrete Transformationsprozesse im digitalen Zeitalter

4.1. Strukturelle Transformationen

Strukturell lassen sich zwei zentrale Tendenzen feststellen, die sich aus der Digitalisierung für den Menschenrechtsschutz ergeben:

---

24 Karst, *Menschenrechte im digitalen Zeitalter*, der Freitag, 25. Februar 2015.

25 Ebd.

4.1.1. Verschiebung Akteure

Erstens verschieben sich die **Akteure auf der menschenrechtlichen Bühne**. Menschenrechtsverletzungen gingen bisher schwerpunktmäßig von staatlichen Stellen aus. Mit der Digitalisierung sind insbesondere **privatrechtliche Unternehmen als machtvolle Akteure** hinzugetreten, die neuerdings über Informationen in nie dagewesenem Umfang verfügen und gleichzeitig häufig marktbeherrschende Stellungen innehaben:

> Während bisher im Wesentlichen nur Staaten in der Lage waren, beispielsweise das Recht auf Privatsphäre zu verletzen, ist dies heute auch anderen Akteuren möglich. Dabei sind hiervon nicht nur autoritäre Regime, sondern auch ordinär liberale Demokratien mit vielen bürgerlichen Freiheiten betroffen.
>
> Wir müssen also eine neue Rollenverteilung und ein neues Kräfteverhältnis berücksichtigen, welches momentan in der Lage ist, das Primat der Politik auf gefährliche Weise zu unterminiert. Das kann uns aus dem Grund nicht egal sein, weil unternehmerische und staatliche Interessen weit auseinander gehen – und nun auch Konzerne wie Facebook oder Google in der Lage sind, faktische Zensur zu betreiben. Während ein Staat aber gewöhnlich Inhalte der Öffentlichkeit vorenthalten möchte um eine politische Stabilitäten nicht zu gefährden, tun Konzerne dies augenscheinlich aus ökonomischen Interessen. Es ist oft schwierig zu sagen, wo angemessenes Verhalten zur Wahrung des Geschäftsbetriebes vorlieg[t], und wo politische Einflussnahme beginnt. Dabei sind Plattformen wie Youtube oder soziale Netze wie Facebook nicht nur in der Lage bestimmte missliebige Inhalte gezielt zu entfernen, - zum Beispiel weil sie Aufenthaltszeiten auf den Seiten reduzieren könnten, oder negative Assoziationen wecken, - sondern auch durch die bewusste in Umlauf Bringung von Informationen und Ansichten, wirken Konzerne anders als bisher als politische Akteure. So stellt Google für Palästina eine eigene Startseite zur Verfügung – ein „Privileg“, dass gewöhnlich nur international anerkannte Staaten genießen.
>
> Unter Beachtung der Größe solcher Dienste wie Facebook oder Google muss man die politische Dimension ins Auge fassen. Hier entscheidet ein kleiner nicht undurchdringbarer Personenkreis maßgeblich darüber, was kommuniziert wird oder werden darf, und was nicht.
>
> Auch führen gerade die Datensammlungen der großen Konzerne, die sich durch das Verkaufen von Informationen über ihrer Nutzer finanzieren, zu einem weiteren Angriff auf die Privatsphäre, der über die weiter oben beschriebenen Automatismen hinaus geht. Denn je mehr Daten solche Unternehmen über die Menschen sammeln, desto größere Profiterwartungen lassen sich realisieren. Es war bereits eine Grundannahme des „Web 2.0“, dass mehr Daten immer besser sind.
>
> Beachtenswert ist auch, dass Konzerne heute Dinge umsetzen können, über die politisch möglicherweise noch verhandelt wird, - deren gesellschaftliche Debatte noch keine kollektiv verbindliche Entscheidung ergeben hat. So besteht in Deutschland keine Einigung über die Einführung einer Vorratsdatenspeicherung - 22 von 31 in Deutschland tätigen Telekommunikationsunternehmen speichern solche Daten allerdings bereits unabhängig von einer gesetzlichen Verpflichtung. Sollten diese privaten Eingriffe als Menschenrechtsverletzungen interpretiert werden, bleibt die Frage offen an wen die entsprechenden Beschwerden zu richten sind.
>
> Wie mit dieser neuen Situation umgegangen werden muss ist noch unklar, stellt sich schließlich die Frage nach dem Verhältnis von Politik und Wirtschaft bei der Kontrolle des Internets. Auch

> wenn die USA bereits 2005 von ihrem Anspruch zurück getreten sind, die Struktur des Netzes im Wesentlichen alleine zu kontrollieren und man sich auf einen „Multi-Stakeholder"-Ansatz geeinigt hat, sind die Erfolge von Institutionen wie dem seit 2005/2006 tagenden Internet Gouvernance Forum mässig. Immer noch ist vielfach ungeklärt, wer beispielsweise verantwortlich sein könnte, wenn ein Konzern aus einem Staat A, auf seinen Servern in einem anderen Staat B Daten liegen hat, die eine Menschenrechtsverletzung einem Dritten Staat C bedeuten. So könnte dies beispielsweise bei Bilder des US-Amerikanischen Konzerns Facebook der Fall sein, die auf Servern in Irland liegen und die Würde eines Menschen in Marokko verletzen.[26]

Dieser Problemkomplex stellt das Völkerrecht vor die grundlegende und schon seit längerem intensiv diskutierte Frage, **inwiefern völkerrechtliche und insbesondere menschenrechtliche Standards auch privatrechtliche Unternehmen binden** können. Die Beantwortung dieser Frage wird im Kontext der Digitalisierung eine Schlüsselrolle dabei spielen, die Menschenrechte gegen Bedrohungen wirksam in Stellung zu bringen.

> [Der Wandel der Menschenrechte bezieht sich vor allem auf die Frage], wer Träger der Menschenrechte ist und wen die Menschenrechte auf welche Weise verpflichten, [die] ebenfalls von zeitgeschichtlichen Normierungen und Interpretationen bestimmt wird. [Hierbei gibt es gegenwärtig insbesondere solche] Entwicklungen, die Menschenrechte nicht mehr nur auf das Verhältnis Individuum – Staat zu beschränken, welches die bestehenden Menschenrechtsabkommen noch kennzeichnet. So werden teilweise auch Kollektive, wie etwa indigene Gemeinschaften, zu Trägern von Menschenrechten erhoben und über den Staat hinaus auch internationale Organisationen sowie private Akteure – allen voran Wirtschaftsunternehmen – auf die Respektierung der Menschenrechte zu verpflichten versucht.[27]

Diese Ansätze zur Einbeziehung privatrechtlicher Unternehmen in menschenrechtliche Verpflichtungen werden **wie folgt bewertet**:

> Viel diskutiert wird – angesichts der fortschreitenden wirtschaftlichen Globalisierung – die Frage der menschenrechtlichen Verpflichtung privater Wirtschaftsunternehmen, die nicht nur die Rechte auf Arbeit und gerechte Arbeitsbedingungen, sondern die gesamte Palette der Menschenrechte im Positiven wie im Negativen stark beeinflussen können. Zwar unterliegen transnationale und nationale Unternehmen prinzipiell der Regulierung durch jenen Staat, in dem sie ihre Geschäfte tätigen, und haben sich eigentlich an nationale Gesetze und Bestimmungen zu halten, die menschenrechtswidrige Geschäftspraktiken verbieten oder sanktionieren sollten. Doch in vielen – gerade schwachen, korrupten oder auch nur um Standortvorteile wetteifernden – Staaten fehlen oder versagen entsprechende Gesetze, oder sie werden schlichtweg ignoriert und unterlaufen. Mitunter nutznießen die Unternehmen auch von staatlichen Menschenrechtsverletzungen.
>
> Solche Praktiken haben immer wieder Forderungen und Bemühungen Auftrieb gegeben, private Unternehmen stärker menschenrechtlich in die Pflicht zu nehmen. Dies kann auf unterschiedliche Weise erfolgen: a) durch den Auf- und Ausbau staatlicher Regulierungen und Kapazitäten, damit

---

26 Ebd.

27 Krennerich, *Menschenrechte - ein allgemeiner Einstieg*, Handbuch der Menschenrechtsarbeit 2014/2015 (Friedrich-Ebert-Stiftung), S. 7, 24 f.

die Staaten ihrer völkerrechtlich verankerten Pflicht nachkommen (können), in ihrem eigenen Hoheitsgebiet die Menschen vor Menschenrechtsverletzungen durch nationale und transnationale Unternehmen zu schützen; b) durch die Entwicklung und Anwendung von nationalen Gesetzen, die es ermöglichen, transnationale Aktivitäten von Unternehmen in ihren „Heimatstaaten“ zu regulieren und zu sanktionieren, wenn sie in anderen Ländern die Menschenrechte verletzen; c) durch die Erarbeitung und Verabschiedung internationaler Abkommen, welche die Unternehmen menschenrechtlich binden; d) durch die freiwillige, menschenrechtliche Selbstverpflichtung der Unternehmen. Neben mittlerweile einer Vielzahl freiwilliger Verhaltenskodizes sehr unterschiedlicher Qualität liegen bereits seit 1976 OECD-Leitsätze für multinationale Unternehmen vor, die Empfehlungen der teilnehmenden Regierungen an im Land ansässige oder tätige multinationale Unternehmen für verantwortungsvolles unternehmerisches Handeln enthalten. In die Neufassung der Leitsätze 2011 wurde eigens ein Kapitel zu Menschenrechten aufgenommen.

Die staatlichen Schutzpflichten und die Stärkung der menschenrechtlichen Verantwortung der Unternehmen sind zentrale Bestandteile der 2011 verabschiedeten VN-Prinzipien zu Wirtschaft und Menschenrechte, welche die diesbezügliche Diskussion in den vergangenen Jahren über Wirtschaft und Menschenrechte prägten. Sie umfassen drei Dimensionen: a) die staatliche Schutzpflicht, der zufolge die Staaten die Menschen vor Eingriffen in ihre Menschenrechte durch Dritte – hier private Unternehmen – schützen müssen (state duty to protect). Soweit es sich hierbei um Schutzpflichten gegenüber im eigenen Land tätigen Unternehmen handelt, sind diese bereits im bestehenden Menschenrechtsregime fest verankert. Verbindliche extraterritoriale Schutzpflichten in Bezug auf Auslandsaktivitäten der im eigenen Land ansässigen Unternehmen sind hingegen erst im Entstehen; b) die eigenständige (völkerrechtlich unverbindliche) Verantwortung privater Unternehmen, die Menschenrechte zu achten und menschenrechtliche Sorgfalt walten zu lassen (corporate responsibility to protect); c) den Zugang zu Rechtsmitteln und Wiedergutmachung, der im Rahmen der staatlichen Schutzpflichten staatlicherseits gewährt werden muss und im Rahmen der privatwirtschaftlichen Verantwortung seitens der Unternehmen gewährt werden soll (access to remedy).

Völkerrechtlich verbindliche und sanktionsbewehrte Instrumente zur internationalen Regulierung von Unternehmen im Bereich der Menschenrechte bestehen bislang nicht. Entsprechende Versuche – etwa in Form des 2003 vorgelegten Entwurfes für „VN-Normen zur Verantwortung transnationaler und anderer Unternehmen in Bezug auf die Menschenrechte“ – scheiterten regelmäßig am Widerstand der Staaten und der Unternehmen. Gegen den Widerstand u.a. der USA und der EU-Staaten verabschiedete der VN-Menschenrechtsrat jedoch im Juni 2014 eine Resolution zur Einsetzung einer offenen Arbeitsgruppe mit dem Ziel, ein entsprechendes Abkommen auszuarbeiten.[28]

4.1.2. Verschiebung von Verantwortlichkeiten

Aus diesem Zusammenwirken vieler auch neuer Akteure und Interessen resultieren zweitens insbesondere auch **unklarere Verantwortlichkeiten** für den Schutz der Menschenrechte im digitalen Bereich.

28 Ebd., S. 20 f.

> Die polyzentrische und heterarchische Struktur des Internets lässt die Interessen von Staaten, Konzernen und Zivilgesellschaft aufeinander treffen. Viele nationale und internationale Gremien setzten sich daher heute nicht mehr nur aus Staaten zusammen, sondern konsultieren auch Konzerne oder Nichtregierungsorganisationen – verbunden mit der einhergehenden fragwürdigen Legitimation. Multinationale Abkommen, „Marktmechanismen" und Grauzonen bilden ein Geflecht, [das] die Suche nach Verantwortlichen für den Schutz und die Durchsetzung von Menschenrechten vor neue Herausforderungen stellt. Es mag momentan schwierig sein, sich eine andere Lösung vorzustellen, - die aktuelle dürfte aus demokratische[r] und rechtsstaatlicher Sicht allerdings nicht zufrieden stellen.[29]

Ursache für die Verschiebung von Verantwortlichkeiten ist insbesondere das **Zusammentreffen verschiedener auch kontrastierender Interessen** der involvierten Akteure, die einer geordneten Koordinierung bedürfen.

> The inhabitants of today's dizzyingly complex digital ecosystem can be boiled down to three primary stakeholder groups: "legislators, private (mostly corporate) actors, and citizens" (UN 2016a, A/HRC/31/64, 29). This "triangle of actors" tries to "shape cyberspace using their possibilities in an uncoordinated manner" (ibid.). If progress is to be made improving digital security and privacy each of these three levels of actors must further develop and coordinate clear commitments and advocacy mechanisms around the improvement of digital privacy. [30]

4.2. Durch die Digitalisierung konkret berührte Rechtspositionen

Die Transformationen des digitalen Zeitalters haben eine enorme menschenrechtliche Reichweite. Das ergibt sich daraus, dass nahezu sämtliche Lebensbereiche heute durch die Digitalisierung durchdrungen sind und dementsprechend potentiell auch durch diese gefährdet sein können.

4.2.1. Insbesondere Privatsphäre, Meinungsfreiheit, Informationsfreiheit

Zu den besonders stark betroffenen Rechten zählt zuvorderst das **Recht auf Privatsphäre**, dem schon weit vor der Benutzung digitaler Medien großes Gewicht beigemessen wurde,[31] das mit dem digitalen Zeitalter aber eine nie dagewesene neue Relevanz erhalten hat und daher einen beispiellosen Umbruch erfahren hat. Diese Transformationen werden separat dargestellt (s.u. 4.3).

---

29 Karst, *Menschenrechte im digitalen Zeitalter*, der Freitag, 25. Februar 2015.

30 Damen/Köhler/Woodard, *The Human Right of Privacy in the Digital Age*, Staat, Recht und Politik – Forschungs- und Diskussionspapiere, Bd. 3 (2017), S. 8 f.

31 Zu denken ist dabei etwa an die großen öffentlichen Debatten um die Volkszählung von 1983, die auch Gegenstand des Urteils des Bundesverfassungsgerichts vom 15. Dezember 2018 (Az. 1 BvR 209, 269, 362, 420, 440, 484/83) war.

Besonders berührt sind im Zuge revolutionierter Kommunikationsmechanismen außerdem die **Meinungs- und Informationsfreiheit.**

> Es ist nur logisch, dass wenn wir große Teile unseres „ganz normalen Lebens“ mit der Unterstützung technischer Systeme durchführen, auch alle Rechte betroffen sind, die uns in diesem Leben zustehen.
>
> Das Recht auf Privatsphäre wird zwar in Verbindung mit Mail- oder Chatnachrichten regelmäßig genannt und sein Schutz berechtigterweise gefordert, - die Tragweite der gesamten Entwicklung wird aber noch nicht ausreichend wahrgenommen. Wenn wir Demonstrationen oder andere Versammlungen zum Beispiel über soziale Netzwerke organisieren, dann wird ein Netzzugang und seine Qualität auch für die **Versammlungsfreiheit** relevant (Art. 20 AEMR). Wenn ein Großteil unseres weltweiten Wissens und unseres Informations- und Diskussionsaustausches im Computer zu finden sind, dann kann das **Recht auf Bildung** nicht mehr nur noch über Schulen, Zeitungen und Bibliotheken verteidigt werden (Art. 26 AEMR). Dass es ein **eigenständiges Recht auf Teilhabe am kulturellen und technischen Fortschritt** gibt (Art. 27 AEMR), kommt dieser eigentlich logischen Gedankenfolge noch unterstützend hinzu.
>
> All diese Rechte sind **Voraussetzungen um sein Recht auf Meinungsfreiheit** (Art 19 AEMR) wahrnehmen zu können. Und der Schutz all dieser Rechte kann wiederum nur dann gewahrt werden, wenn es möglich ist, sich „frei und ungehindert aus allen verfügbaren Quellen **zu unterrichten**“, sowie seine Meinung „in Schrift Ton und Bild ungehindert zu verbreiten“.[32]

Offensichtliche Gefährdungen des Rechts auf Meinungs- und Informationsfreiheit gehen insbesondere von **Zensurmaßnahmen** aus, die vor allem in autoritären Staaten ein nach wie vor verbreitetes Instrumentarium zur Steuerung der politischen Meinungsbildung darstellen.

> Online-Plattformen und Blogs werden zunehmend zur Mobilisierung bei Protesten genutzt, etwa im „Arabischen Frühling“. Viele Regierungen weltweit beschneiden deshalb die neuen Ausdrucks- und Informationsmöglichkeiten oder nutzen sie für repressive Zwecke. Die Bedrohung der Meinungsfreiheit durch Zensur zeigt sich zum Beispiel an der Blockade von Twitter und YouTube durch die türkische Regierung oder an der umfangreichen Kontrolle des Internets in der Volksrepublik China. Und während der Maidan-Proteste in Kiew im Jahr 2014 erhielten Besitzer von Mobiltelefonen, die in der Nähe der Kundgebungen geortet wurden, eine einschüchternde SMS, in der es hieß: „Sehr geehrter Empfänger, Sie wurden als Teilnehmer einer Massenunruhe registriert“. [33]

Aber auch in unerwarteteren Kontexten bestehen im digitalen Raum erhebliche Bedrohungen dieser Freiheiten, jüngst etwa im Zusammenhang mit der **Bekämpfung sog. „Hate-Speech“ und „Fake-News“**. Der deutsche Gesetzgeber hat zum 1. Oktober 2017 das Netzwerkdurchsetzungsgesetz (**NetzDG)** in Kraft gesetzt, das soziale Netzwerke, also privatwirtschaftliche Unternehmen, dazu verpflichtet, bestimmte Inhalte zu löschen. Problematisch ist hierbei, dass einerseits die Beurteilung der Rechtswidrigkeit von Beiträgen alleine in die Hand der Unternehmen gelegt wird

32 Karst, *Menschenrechte im digitalen Zeitalter*, der Freitag, 25. Februar 2015.

33 Amnesty International, *Menschenrechte im digitalen Zeitalter*, 4. Juni 2015.

und diese sich gleichzeitig einem enormen Zeitdruck bei der Löschung gegenübersehen, weswegen sich praktisch erhebliche Löschwellen auch nicht offensichtlich rechtswidriger Beiträge durch die Netzwerke zeigen.

> Das Gesetz birgt Gefahren für die Meinungsfreiheit, indem es die Entscheidung darüber, welche Meinungsäußerungen zulässig sind, **in die Hände martkdominanter sozialer Netzwerke legt**. […]
>
> Potentiell grundrechtsschädigend ist, dass die Plattformbetreiber ab 1. Januar 2018 „offensichtlich rechtswidrige Inhalte" innerhalb von 24 Stunden löschen oder sperren müssen. Andernfalls drohen Bußgelder in der Höhe von bis zu 50 Millionen Euro. Bei nicht ganz klaren Fällen bleiben den Plattformbetreibern sieben Tage Zeit, eine Entscheidung zu treffen. Das NetzDG listet dabei 21 Straftatbestände auf, die unter das Gesetz fallen. Vielen von ihnen haben mit dem, was man gemeinhin unter Hasskriminalität versteht, nicht viel zu tun, z.B. Verunglimpfung des Staates nach §90a Strafgesetzbuch. […] Ein weiteres Problem sind die **kurzen Fristen und die möglichen Bußgelder**. Dies könnte dazu führen, dass die Plattformbetreiber aufgrund der juristischen Unsicherheiten vorsorglich sehr viele Beiträge löschen, selbst wenn diese rechtmäßig sind (sog. **Overblocking**).
>
> Gleichzeitig gibt das Gesetz denjenigen, deren Inhalte zu Unrecht gelöscht werden, **keine wirksamen Instrumente** an die Hand, um sich zu wehren. Bis heute gibt es für Personen, die von Löschungen betroffen sind, keinerlei Transparenz, keine Konsistenz von Löschentscheidungen und kaum Möglichkeiten, den Rechtsweg einzuschlagen. Das Problem verschärft sich – mit oder ohne NetzDG -, je marktdurchdringender, dominanter und wichtiger für die Öffentlichkeit die Plattformen sind. […]
>
> Im Gesetzgebungsprozess zum NetzDG brachte sich im April eine „**Allianz für die Meinungsfreiheit**" in Stellung – ein ungewöhnlich breites Bündnis aus Industrieverbänden, Journalistenvereinigungen, Bürgerrechtsorganisationen und netzpolitischen Initiativen. […] Wegen des breiten Widerstands wurde das Gesetz zumindest in Teilen entschärft. So wurden beispielsweise die ursprünglich geplanten Inhalte- und Uploadfilter wieder gestrichen. […]
>
> Doch die Grundprobleme des Overblockings durch die Plattformen lösen auch diese eher kosmetischen Korrekturen nicht. Deswegen bleibt das Gesetz auch in der aktuellen Version gefährlich für die Meinungsfreiheit. Diese Befürchtungen wurden zusätzlich genährt, nachdem sich ein Gesetzentwurf zur Kontrolle von Internetinhalten in Russland positiv auf das NetzDG bezog. […]
>
> Das NetzDG könnte sich als schwerwiegender Eingriff in das Grundrecht auf Meinungsfreiheit entpuppen, denn die Plattformen werden mit dem Gesetz zum Richter und Henker zugleich. Die Alternative zum NetzDG liegt auf der Hand: **Entscheidungen über Einschränkungen der Meinungsfreiheit müssen Gerichte treffen**. Sie brauchen dafür die nötige finanzielle und personelle Ausstattung, damit sie schnell reagieren können.[34]

34 Reuter, *das Netzwerkdurchsetzungsgesetz – eine Gefahr für die Meinungsfreiheit*, Grundrechtereport 2018, S. 85.

4.2.2. Recht auf gleichberechtigten Zugang zu digitalen Ressourcen?

Vereinzelt wird darüber hinaus gefordert, dass neben diesen allgemein geltenden Rechten, die im Digitalzeitalter eine besondere Relevanz erhalten, auch der **Zugang zu den digitalen Ressourcen an sich** als Menschenrecht anerkannt wird – konkret das Recht auf Teilhabe an technischem Fortschritt und auf einen diskriminierungsfreien Zugang.

> Wenn man diesen Gedanken konsequent zu Ende denkt, dann müsste man sich sogar nicht nur für einen Schutz dieser Rechte „im Netz" einsetzen, sondern mit zunehmendem Maß der Digitalisierung ein Recht auf diskriminierungsfreien Internetzugang anerkennen.[35]

An dieser Frage, inwiefern der Menschenrechtsschutz im Digitalzeitalter neben den anerkannten grundlegenden Rechten auch das **Recht auf Teilhabe und einen diskriminierungsfreien Zugang** zu den digitalen Ressourcen an sich erfassen soll, zeigen sich jedoch **unterschiedliche Strömungen**. Das Internet wird einerseits als elementarer Raum gesehen, der für die individuelle Entfaltung und kulturelle Teilhabe heute unverzichtbar ist, so dass ein allgemeiner Zugang frei von Diskriminierungen menschenrechtlich zu gewährleisten ist. Bedenken bestehen hierbei allerdings mit Blick auf das Gewicht der sonstigen Menschenrechte und der global nach wie vor existierenden Menschenrechtsverletzungen. **Es wird befürchtet, dass eine derartige Ausweitung des Menschenrechtsschutzes das Gewicht der Menschenrechte langfristig schwächt, indem der Fokus von den elementarsten Rechten weggelenkt wird.**

> Das größte Gegenargument in dieser Debatte ist die Befürchtung, durch ein solches Recht, die Menschenrechte „aufzuweichen" und somit ihrer bedingungslosen Notwendigkeit zu berauben. Dieser Standpunkt mag zum aktuellen Zeitpunkt nicht völlig unbegründet sein, je wichtiger allerdings das Internet für unser Zusammenleben wird, als desto wichtiger muss auch ein diskriminierungsfreies Zugangsrecht bewertet werden.[36]

Die Befürchtung einer Entwertung der Menschenrechte insgesamt lässt sich mit Verweis darauf entschärfen, dass schon heute das „**Recht auf Teilhabe am kulturellen Leben und an den Errungenschaften des wissenschaftlichen Fortschritts**" sowie die „Freiheit des Kulturlebens" durch den Internationalen Pakt über wirtschaftliche, soziale und kulturelle Rechte und die Allgemeine Erklärung der Menschenrechte geschützt wird. Betrachtet man den Zugriff auf digitale Ressourcen, insbesondere das Internet, als elementaren Bestandteil des kulturellen Lebens und des technischen und wirtschaftlichen Fortschritts, muss man konsequenterweise auch den diskriminierungsfreien Zugang zu diesen Ressourcen als menschenrechtlich geschützt bewerten.

> Artikel 15 Internationalen Pakt über wirtschaftliche, soziale und kulturelle Rechte der VN:[37]
> (1) Die Vertragsstaaten erkennen das Recht eines jeden an,
> a) am kulturellen Leben teilzunehmen

---

35 Karst, *Menschenrechte im digitalen Zeitalter*, der Freitag, 25. Februar 2015.

36 Ebd.

37 Internationaler Pakt über wirtschaftliche, soziale und kulturelle Rechte, UN-Doc A/RES/2200 A (XXI), 19. Dezember 1966.

b) an den Errungenschaften des wissenschaftlichen Fortschritts und seiner Anwendung teilzuhaben […]

Artikel 27 AEMR (Freiheit des Kulturlebens):[38]
Jeder Mensch hat das Recht, am kulturellen Leben der Gemeinschaft frei teilzunehmen, sich der Künste zu erfreuen und am wissenschaftlichen Fortschritt und dessen Wohltaten teilzuhaben. […]

Praktisch wird dieses Recht eines gleichberechtigten Zugangs derzeit insbesondere durch Tendenzen gefährdet, die auf eine **Einschränkung der Netzneutralität** abzielen.

Der Begriff Netzneutralität meint, **dass sämtliche Datenströme im Internet gleich behandelt und gleich schnell transportiert werden** - unabhängig davon, woher sie stammen, welcher Art die Daten sind und welchen Inhalt sie haben. Provider sollen demnach die Daten unterschiedslos - ob z.B. Videos, Patientendaten, E-Mail-Verkehr oder Spiele - durch ihre Netze leiten.

Befürworter der Netzneutralität sehen darin einen Grundsatz, der **das Internet als demokratisches Netz** erst ausmacht. Sie gilt ihnen als Garant für Wettbewerb und Innovationen wie auch für demokratische Strukturen. Sie warnen vor steigenden Kosten und der Benachteiligung bestimmter Inhalte. Finanzstarke Firmen könnten sich schnellen Datenverkehr kaufen und damit kleinere Konkurrenten aus dem Markt drängen. Schnelle Verbindungen gäbe es nur noch für Wohlhabende und langsame Leitungen für den Rest.

Kritiker der Netzneutralität argumentieren hingegen, sie stehe **Interessen von Unternehmen** im Weg, die den **Ausbau ihrer Netze refinanzieren** müssen. Der Datenverkehr wachse immens. Das mache es erforderlich, bestimmte Daten etwa wie bei Telefonaten oder Videostreaming vorrangig zu behandeln.[39]

In den Vereinigten Staaten von Amerika ist der **Grundsatz der Netzneutralität seit Ende 2017 eingeschränkt** und auch in der Europäischen Union wird dieses Thema viel diskutiert.

Die US-Telekommunikationsaufsicht FCC hatte sich […] gestern mit knapper Mehrheit hinter den Entwurf ihres von US-Präsident Donald Trump ernannten Chefs gestellt. **Demnach sollen Netzanbieter künftig bestimmte Angebote im Internet bevorzugen dürfen**. Nach der alten Regelung war es den Netzbetreibern nicht erlaubt, bestimmten Datenverkehr zu blockieren oder zu verlangsamen und anderen Inhalten Vorrang zu geben. Dieses Verbot fällt in den USA nun weg - vorausgesetzt es gibt nicht noch erfolgreiche Klagen vor Gericht dagegen.

Und welche Folgen hat die US-Entscheidung nun in Europa? Hier werde man das „indirekt zu spüren bekommen“ - so die Einschätzung von Klaus Müller, dem Vorstand des Verbraucherzentrale

38 Allgemeine Erklärung der Menschenrechte, A/RES/217, UN-Doc. 217/A-(III), 10. Dezember 1948.

39 Tagesschau.de, *Ende der Netzneutralität auch in Europa?,* 15. Dezember 2017, verfügbar unter https://www.tagesschau.de/wirtschaft/netzneutralitaet-115.html.

> Bundesverbands. Die Marktmacht großer Internetanbieter werde wachsen. Damit werde die Auswahl auch für Kunden in Europa schrumpfen. [40]
>
> Wie sich […] gezeigt hat, reizen europäische Netzbetreiber jedes Schlupfloch bis zum Äußersten aus. So erlauben die EU-Regeln unter Auflagen etwa Zero-Rating-Angebote, mit denen die Betreiber das Internet in unterschiedliche Kategorien einteilen und dadurch ein Zwei-Klassen-Netz schaffen.
>
> Teilnehmende Dienste können sich über eine bessere Behandlung freuen und gewinnen so an Attraktivität bei interessierten Nutzern. Anbieter, die sich die Teilnahme nicht leisten können oder wollen, schauen hingegen durch die Finger und müssen damit rechnen, langfristig auf dem Abschiebegleis zu landen. Kein Wunder, dass IT-Experten und Verbraucherschützer gegen die Praxis der Telekom Deutschland und Vodafone Sturm laufen, weil sie das offene Internet und damit die Meinungsfreiheit sowie Angebotsvielfalt im Netz bedroht.
>
> Doch selbst wenn Regulierer gegen offensichtliche Verstöße der Netzbetreiber vorgehen, gibt sich die Branche unbeeindruckt und setzt lieber auf langwierige Gerichtsverfahren, anstatt die gesetzlichen Vorgaben umzusetzen. „Unser größtes Problem in Europa ist die Rechtsdurchsetzung", sagt Lohninger. Obwohl die Bundesnetzagentur etwa das StreamOn-Produkt der Telekom Deutschland bereits für europarechtswidrig befunden habe, werde die gerichtliche Prüfung wohl noch Jahre dauern. „Am Ende steht vermutlich eine winzige Strafe einer sehr lukrativen und jahrelangen Rechtsverletzung gegenüber", sagt Lohninger. „Davon werden andere Telekomkonzerne lernen."[41]

4.2.3. Darüber hinausgehende Bedeutung für die Gestaltung des Gemeinwesens

Gleichzeitig ist hierbei auch folgende übergeordnete Dimension des Menschenrechtsschutzes zu beachten: Zwar sind Träger der Menschenrechte zunächst die einzelnen Menschen als autonome Individuen. Die Rechte haben gleichzeitig aber auch eine erhebliche **Bedeutung für die Ausgestaltung des Gemeinwesens** als Ganzes – im Kontext der Digitalisierung konkret eine offene und inklusive Teilhabe an digitalen Ressourcen.

> Auch individuelle Menschenrechte weisen […] **gemeinschaftliche und gesellschaftliche Bezüge** auf. Die Umsetzung sowohl der bürgerlichen und politischen als auch der wirtschaftlichen, sozialen und kulturellen Rechte ist ohne das soziale Miteinander, ohne die Einbettung in das Gemeinwesen kaum denkbar. Die individuelle Autonomie bedarf daher immer auch der sozialen Teilhabe, Solidarität und Inklusion. Demgemäß schützen die Menschenrechte gerade auch gegen soziale Ausgrenzungen.
>
> Zugleich wirken die Menschenrechte, obwohl sie vornehmlich als Individualrechte ausgestaltet sind, auf eine **freiheitliche und gleichberechtigte Ausgestaltung des Gemeinwesens als Ganzes** hin.

---

40 Ebd.

41 Rudl, *Netzneutralität: USA verabschieden sich vom offenen Internet*, Netzpolitik.org, 11. Juni 2018, verfügbar unter https://netzpolitik.org/2018/netzneutralitaet-usa-verabschieden-sich-vom-offenen-internet/.

> Indem die Menschen nämlich ihre Menschenrechte nutzen, jene ihrer Mitmenschen achten und der Staat die entsprechende Freiräume achtet, schützt oder erst schafft, verändert sich auch das Gemeinwesen, in dem – im Idealfall – sozial und politisch autonome Menschen im Verbund mit anderen leben, sich zusammenschließen und handeln. Der Schutz der Individualrechte weist also weit über den einzelnen Menschen hinaus. [42]

4.3. Kernproblematik: Das Recht auf Privatsphäre

Durch die Digitalisierung und die damit einhergehende automatisierte Datenverarbeitung ist vor allem das **Recht auf Privatsphäre** tangiert.

> The right to privacy in the digital age is threatened aggressively by data automation.[43]

4.3.1. Bedeutung und Schutz

Das Recht auf Privatsphäre wird völkerrechtlich vielfältig geschützt, etwa durch die Allgemeine Erklärung der Menschenrechte der Vereinten Nationen, den Internationalen Pakt über bürgerliche und politische Rechte, die Amerikanische und die Europäische Menschenrechtskonvention, ebenso durch nationales und europäisches Recht, beispielsweise in Form der EU-Datenschutz-Grundverordnung.[44]

> Art. 12 der AEMR (weitgehend wortgleich auch Art. 17 Internationaler Pakt über bürgerliche und politische Rechte):
> Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, sein Heim oder seinen Briefwechsel noch Angriffen auf seine Ehre und seinen Beruf ausgesetzt werden. Jeder Mensch hat Anspruch auf rechtlichen Schutz gegen derartige Eingriffe oder Anschläge.
>
> Art. 8 EMRK:
> (1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.
> (2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur

---

42 Krennerich, *Menschenrechte - ein allgemeiner Einstieg*, Handbuch der Menschenrechtsarbeit 2014/2015 (Friedrich-Ebert-Stiftung), S. 7, 14.

43 International Federation of Library Associations and Institutions, *The right to privacy in the digital age*, S. 1, verfügbar unter https://www.ifla.org/files/assets/faife/ochr_privacy_ifla.pdf.

44 Vgl. Damen/Köhler/Woodard, *The Human Right of Privacy in the Digital Age*, Staat, Recht und Politik – Forschungs- und Diskussionspapiere, Bd. 3 (2017), S. 2 f.

> Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.

Auch darüber hinaus ist das Recht auf Privatheit im Völkerrecht anerkannt:

> 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. [45]

Eine einheitliche **Definition des Konzepts der Privatsphäre existiert nicht**, überwiegend wird jedoch ein weites Verständnis des Begriffs zugrunde gelegt. Im allgemeinen menschenrechtlichen Diskurs hält das institutionell unabhängige, mit Wissenschaftlern besetzte sog. *Committee on Privacy in the Information Age* sämtliche Informationen über eine Person für erfasst;

> [The term privacy] includes reference to the types of information available about an individual, whether they are primary or derived from analysis. These types of information include behavioral, financial, medical, biometric, consumer, and biographical.[46]

Im Rahmen der jeweiligen völker- und menschenrechtlichen Übereinkommen kommt es auf die Auslegung an, die die zuständigen Gerichte für die jeweiligen Begriffe entwickelt haben. Eine ausdifferenzierte Rechtsprechung besteht etwa zu **Art. 8 EMRK**, der nach dem Europäischer Gerichtshof für Menschenrechte (EGMR) **die Privatsphäre im Sinne des gesamten Privatlebens** in noch umfassenderem Maße schützt;

> Der Begriff des „Privatlebens" ist – so der EGMR – umfassend und einer abschließenden Definition nicht zugänglich. Darunter fällt zunächst die körperliche und psychische Integrität einer Person. Der EGMR hat entschieden, dass nicht jede Handlung oder Maßnahme, die sich nachteilig auf die geistige oder körperliche Integrität auswirkt, einen Eingriff in das Recht auf Achtung des Privatlebens darstellt. […] Des Weiteren können Aspekte der körperlichen und sozialen Identität einer Person unter den Begriff „Privatleben" fallen. Teilbereiche hiervon, wie etwa die geschlechtliche Identität, der Name und die sexuelle Ausrichtung sowie das Sexualleben, gehören zu der von Art. 8 Abs. 1 geschützten Privatsphäre. Auch die ethnische Herkunft eines Menschen – wie die Zugehörigkeit zur Volksgruppe der Roma – ist ein wichtiger Bestandteil des Privatlebens (EGMR BeckRS 2013, 00833 Rn. 58 – Aksu). [47]

---

45 Bericht des Amtes des Hohen Kommissars der Vereinten Nationen für Menschenrechte, A/HRC/27/37, 30. Juni 2014, *Das Recht auf Privatheit im digitalen Zeitalter*, S. 5.

46 Zitiert nach Damen/Köhler/Woodard, *The Human Right of Privacy in the Digital Age*, Staat, Recht und Politik – Forschungs- und Diskussionspapiere, Bd. 3 (2017), S. 2.

47 Hofmann, *Beck'scher Online-Kommentar Ausländerrecht*, Art. 8 EMRK, Rn. 20.

Das Recht des Datenschutzes wird in der Regel als eine von mehreren Ausprägungen des Schutzes des Privatlebens aus Art. 8 EMRK verstanden:

> Das aus dem Privatleben folgende **Recht, sich selbst zu verwirklichen**, **kann durch die Erhebung, Speicherung und Verwendung von Daten des Einzelnen erheblich gestört werden**. Deshalb ist das Recht auf informationelle Selbstbestimmung, das schon die Europäische Kommission anerkannte (EKMR DR 30, 239), Teil des Privatlebens iSv Art. 8 (EGMR Urt. v. 26.3.1987 – 9248/81 – Leander ./. Schweden; Urt. v. 16.2.2000 – 27798/95 – Amann ./. Schweiz). Dabei ist es unerheblich, ob sich die erhobenen Daten auf das öffentliche oder auf das private Leben des Betroffenen beziehen (EGMR Urt. v. 25.3.1998 – 23224/94 – Kopp; EGMR Urt. v. 4.5.2000 – 28341/95 – Rotaru ./. Rumänien).[48]

Im Rahmen der AEMR besteht keine verbindliche Auslegung, der Begriff des Privatlebens wird aber auch hier überwiegend weit verstanden und enthält als eine Ausprägung anerkanntermaßen auch den Schutz intimer und aus der Kommunikation stammender Informationen.

> Zum Privatleben gehört nach heutiger Auffassung in erster Linie die Identität (u.a. Name, Kleidung, Haartracht, Gefühle und Gedanken), die Integrität (was etwa eine medizinische Behandlung gegen den Willen der Betroffenen ausschliesst), die Intimität (wie etwa die Geheimhaltung privater Eigenschaften und Handlungen, der Schutz des eigenen Bildes vor Veröffentlichung oder der Schutz vor Weitergabe personenbezogener Daten), die Kommunikation (z.B. die Aufnahme und Entwicklung von Beziehungen zu anderen Leuten) und die Sexualität (allerdings darf hier der Staat zum Schutze bestimmter Personengruppen, etwa von Kindern, Einschränkungen wie z.B. ein Mindestalter vorschreiben).[49]

4.3.2. Privatsphäre als Grundlage für Freiheit und Autonomie

Wie bereits angeklungen, wird die Privatsphäre nicht nur um ihrer selbst Willen geschützt, sondern dient insbesondere als **Grundlage zur Ausübung zahlreicher anderer Menschenrechte**:

> Das Recht auf Privatsphäre ist eine wichtige Grundlage für zahlreiche andere Menschenrechte wie Meinungs- und Informationsfreiheit, das Recht auf friedliche Versammlung und das Recht auf Freiheit von Diskriminierung. Wer Angst hat, dabei überwacht zu werden, sagt weniger frei seine Meinung und traut sich seltener, im Internet zu Protest aufzurufen oder sich über sensible Themen zu informieren. [50]

Auch der Hochkommissar für Menschenrechte der Vereinten Nationen hat dies ausdrücklich anerkannt;

---

48 Gersdorf, *Beck'scher Online-Kommentar Informations- und Medienrecht*, Art. 8 EMRK, Rn. 29.

49 Informationsplattform HumanRights.ch, *Erläuterungen zur AEMR*, Art. 12 AEMR.

50 Amnesty International, *Menschenrechte im digitalen Zeitalter*, 4. Juni 2015.

> [Es] 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 – 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. [51]

Auch in der Literatur wird die Privatsphäre als Grundlage individueller Autonomie betrachtet:

> Privacy is the “right to be free from unwarranted intrusion and to keep certain matters from public view” (Law 2015). As such, “privacy is an important element in the autonomy of the individual. Much of what makes us human comes from our interactions with others within a private sphere where we assume no one is observing. Privacy thus relates to what we say, what we do, and perhaps even what we feel” (MacMenemy 2016).
>
> **A private space enhances autonomy**. If we feel we may not be completely autonomous in our thoughts and actions, we may hold back crucial elements of ourselves. Privacy, therefore, “protects our subjectivity from the pervasive efforts of commercial and government actors to render individual and communities fixed, transparent and predictable. Privacy is an indispensable feature of a democracy where an individual maintains his identity while contributing to their civic duty” (Cohen 2016).
>
> […] ‘[E]xcessive data collection and use threatens individual users’ privacy and has other social and legal consequences. When Internet users are aware of large-scale data collection and surveillance, they may self-censor their behaviour due to the fear of unexpected consequences. Excessive data collection can then have a chilling effect on society, narrowing an individual’s right to freedom of speech and freedom of expression because of this perceived threat. Limiting freedom of speech and expression has the potential to compromise democracy and greatly limit civil engagement by making us “predictable” in our actions and thoughts (Cohen, 2016). [52]

---

51 Bericht des Amtes des Hohen Kommissars der Vereinten Nationen für Menschenrechte, A/HRC/27/37, 30. Juni 2014, *Das Recht auf Privatheit im digitalen Zeitalter*, S. 5 f.

52 International Federation of Library Associations and Institutions, *The right to privacy in the digital age*, S. 1.

4.3.3. Gefährdung durch neue Möglichkeiten automatisierter Datenverarbeitung

Dieses Recht wird vor dem Hintergrund neuer **Möglichkeiten der automatisierten Datensammlung und -auswertung** verbreitet als stark gefährdet betrachtet – neben staatlichen neuerdings insbesondere auch durch privatwirtschaftliche Akteure (vgl. dazu zu auch oben 4.1.1):

> **The right to privacy in the digital age is threatened aggressively by data automation**. In 1985 Spiros Simitis, Germany's leading privacy scholar recognized the risks data automation would cause to privacy, individuals and the democratic process. "Privacy is not an end in itself, Simitis suggested, but an important tool to achieve a self-critical democracy where citizens are not unwitting suppliers of information to an all-seeing, and all-optimizing technocrats" (Morozov 2013). If privacy is at risk or threatened, we might miss the chance for personal assessment of the political process, one based on critical evaluation and self-reflection of our choices and preferences.
>
> Data collection, through hacking or simple data harvesting, allows governments and commercial entities to amass huge banks of information about common citizens and their online behaviour. Privacy incursions occur frequently, affecting our search and digital behaviour patterns. These incursions are not only about a person or in this case a user – they can also affect a group, a family, a community.
>
> Automated data gathering is **carried out by government and private actors**. Government surveillance includes communications interception, bulk data collection and processing, targeted intrusions in ICT systems and issues relating to cross-border surveillance and access to personal data.
>
> As one of the many **examples of governmental privacy infringement**, the Pegasus software allowed the Mexican Government to spy on human rights defenders, journalists and anti-corruption activists. In this specific case of government sponsored cyberattacks, the WhatsApp feed of the son of a prominent lawyer and civil right journalist was the target of intrusion and privacy infringement (New York Times 2017).
>
> **Businesses can also contribute to surveillance activities** based on data automation and collection and so encroach on our privacy. The latest scandal involves Facebook users and Cambridge Analytica researchers mishandling the data of over 40 million users. The dubious data gathering tactic included the use of Facebook Graphs API (application program interface) "that makes possible all the interconnectivity and the data delivery Facebook boasts when claiming that the platform was building a web where the default option is sharing" (Albright 2018). What is worrisome is that FB claims that its interface is based on the pretence that users are in control of what it is shared. In actuality, Facebook users have next to no control what is covertly shared about them – meaning the information and metadata others can extract. Whether the threat comes from governments or private entities, these occurrences pose a significant question as to the right to live without arbitrary attacks on privacy (Article 12 of the Universal Declaration on Human Rights) and how our right to safeguard privacy can be defended. [53]

53 Ebd.

In diesem Kontext wird allerdings auch der Umstand aufgegriffen, dass **Internetnutzer Daten in großem Umfang auch freiwillig preisgeben**, etwa in sozialen Netzwerken. Diesbezügliche Bedenken werden jedoch mit Hinweis darauf entkräftet, dass den Nutzern die Reichweite und die genauen Umstände dieser Preisgabe in der Regel nicht vollständig bewusst sein dürften und sie daher ungeachtet dessen schutzwürdig seien.

> Einige vertreten die Auffassung, dass die Weitergabe und der Austausch personenbezogener Informationen auf elektronischem Weg Teil eines bewusst eingegangenen Kompromisses 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. […]“[54]

4.3.4. Staatliche Eingriffe in die Privatsphäre zugunsten der nationalen Sicherheit

Grundlage von Einschränkungen der Privatsphäre **durch staatliche Organe** sind häufig **sicherheitspolitische Argumente**. Diese Tendenz hat sich mit steigender Präsenz terroristischer Gefahren verstärkt und setzt die individuellen Freiheitsrechte, insbesondere die Privatsphäre, stark unter Druck.

> While data protection legislation has the potential to cut back on speculative data collection by companies, data privacy laws are not well placed to protect individuals' rights vis-a-vis automated technologies and privacy can all too often be undermined by laws elsewhere.
>
> Currently, as a response to terrorist attacks in Europe**, increased surveillance powers have been implemented at the national level, with much data shared across borders**. Security has too often been cited as a reason for limiting use of encryption technologies, or for creating “back-doors”, which are likely both to facilitate incursions on privacy by both government and other actors.
>
> There are already **voices against blanket surveillance**. The Council of Europe has called on Member States to refrain from indiscriminate mass digital surveillance. In 2016 the European Court of Human Rights (ECtHR) “delivered a judgement on secret surveillance in the case Szabo and Vissy vs. Hungary. The court found that Hungary’s 2011 legislation on secret surveillance violated article 8 of the ECHR because it failed to safeguard against abuse” (Fundamental Right Report 2017).
>
> Referring to the “Court of Justice of the European Union’s (CJEU) judgment in Digital Rights Ireland v. Minister of Communications & Others, the ECtHR stated that, where national rules enable large-scale or strategic interception and where this interference may result in particularly invasive inter-

54 Bericht des Amtes des Hohen Kommissars der Vereinten Nationen für Menschenrechte, A/HRC/27/37, 30. Juni 2014, *Das Recht auf Privatheit im digitalen Zeitalter*, S. 6 f.

> ferences with private life", the "guarantees required by the extant Convention case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices" (Fundamental Right Report 2017).
>
> Regarding current legislation, even under the **General Data Protection Regulation**, governments still have ample scope to claim that national security – for right or for wrong – justifies attacks on privacy. This is not to say that steps to ensure that firms and others will have to be clearer about what information they are gathering, and how it will be used, are not welcome, alongside the possibility for citizens to ask to see what data is held, and for it to be deleted. [55]

Insbesondere durch Menschenrechtsorganisationen wird hierzu teilweise die Extremposition vertreten, Überwachungsmaßnahmen hätten **keinerlei nachgewiesenen Nutzen für die öffentliche Sicherheit**:

> Eingriffe in Menschenrechte werden häufig mit dem Verweis auf die „nationale Sicherheit" gerechtfertigt. Doch es gibt bislang keine Beweise dafür, dass anlasslose Überwachungsmaßnahmen zusätzliche Sicherheit schaffen. Im Gegenteil:
>
> Eine von Präsident Obama eingesetzte unabhängige Untersuchungskommission (PCLOB) kam im Januar 2015 zu dem Ergebnis, dass die Vorratsdatenspeicherung der NSA illegal sei und eine „ernsthafte Bedrohung" für die Bürgerrechte und die Demokratie darstelle. Im Kampf gegen den Terrorismus habe sie sich als nutzlos erwiesen: „Es gibt keinen einzigen Fall, in dem das Programm zur Aufdeckung eines zuvor unbekannten Terrorplans oder zur Verhinderung von terroristischen Angriffen beigetragen hätte", heißt es im Abschlussbricht der Kommission. [56]

Überwiegend ist anerkannt, dass Überwachungsmaßnahmen durch Sicherheitsinteressen grundsätzlich durchaus **gerechtfertigt werden können**. Als Maßstab wird hierbei formuliert, dass erstens **prozedurale Mechanismen** zur Sicherung der Grund- und Menschenrechte vorgesehen werden müssen und zweitens Überwachungsmaßnahmen, die **anlasslos** ohne den Verdacht krimineller Aktivitäten erfolgen, grundsätzlich **menschenrechtswidrig** sind.

> Within international political discourse, mass data surveillance and storage are legitimized by the "War on Terror" (Cohen/Fisher 2016). Indeed, in some cases of national security and criminal activities, **surveillance can be justified**. However, fully developed **mechanisms for civil society to be protected from such are lacking**. If there are **no reasonable grounds for suspicion** such as terrorist or criminal activities, indiscriminate mass surveillance of all individuals and states is a violation of human rights.[57]

Nach einer Vielzahl von Stimmen fehlen dementsprechende **rechtliche Rahmenbedingungen oder sind jedenfalls überwiegend unzureichend**.

---

55 International Federation of Library Associations and Institutions, *The right to privacy in the digital age*, S. 2 f.

56 Amnesty International, *Menschenrechte im digitalen Zeitalter*, 4. Juni 2015.

57 Damen/Köhler/Woodard, *The Human Right of Privacy in the Digital Age*, Staat, Recht und Politik – Forschungs- und Diskussionspapiere, Bd. 3 (2017), S. 3.

> The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, states that national laws that regulate the involvement of states in communication surveillances often do not exist, or are inadequate (UN 2013, A/HRC/23/40, 3). […]
>
> Compounded with the slippery consensus around legal definitions for culturally sensitive terms, like privacy, technology is quickly growing and therefore international law-making becomes very difficult. The nature of the Internet is borderless and different stakeholders have contradicting interests. Also, legislative processes are relatively slow and lawmakers often lack a technological understanding (Bernal 2014, 82). Still these difficulties do not excuse foregoing the urgent need for more thorough regulations of privacy. Sisk argues, that there is a need for more, and stronger, privacy rights in our digital age (Sisk 2016, 101).[58]

Der „Grundrechtereport“ aus dem Jahr 2018 bestätigt jedenfalls für die Bundesrepublik Deutschland, dass der **Schwerpunkt menschenrechtsrelevanter Aktivitäten durch den Staat** heute auf dem Gebiet der Überwachungsmaßnahmen im Namen der nationalen Sicherheit liegt. Als problematische Beispielmaßnahmen werden in diesem Zusammenhang konkret das Pilotprojekt zur Gesichtserkennung am Bahnhof Berlin Südkreuz, die Schaffung einer biometrischen Verbunddatei der Sicherheitsbehörden, die Vorratsdatenspeicherung, die Quellen-Telekommunikationsüberwachung und Online-Durchsuchung zur Strafverfolgung, der Austausch von Fluggastdaten und das sog. Offline-Tracking (also die Beobachtung im analogen Alltag) genannt.[59]

> [**Zur Gesichtserkennung**:] Wenn ein unbefangenes Verhalten an öffentlichen Plätzen nicht mehr möglich ist, weil befürchtet werden muss, dass man (falsch) identifiziert wird, nimmt ein Gefühl des Überwachtwerdens und sozialer Kontrolle zu. Nonkonformes Verhalten und politische Freiheit werden beeinträchtigt. […] Erschwerend kommt hinzu, dass die Intensität des Eingriffs bei einer (drohenden) Gesichtserfassung viel höher sein wird als bei der Erfassung von Kfz-Kennzeichen. Gesichter haben nicht nur ein höheres Identifikationspotential, sondern sind auch ein urpersönliches Merkmal des Menschen: Die Persönlichkeitsrelevanz des Eingriffs ist ungleich höher. Wird die Technik tatsächlich flächendeckend eingesetzt, wird es vielleicht im Zuge weiterer technischer Entwicklung und Gesetzesneuerungen und –verschärfungen möglich sein, Bewegungsprofile von Menschen zu erstellen, im Extremfall sogar Persönlichkeitsprofile. […]
>
> Die intransparente Sorglosigkeit der Regierung sollte Grund zur Skepsis sein. Dieser Test steht in einer Reihe mit dem Erlass des Neuen Pass- und Personalausweisgesetzes, des Gesetzes zur Überwachung von Messenger-Diensten und des Gesetzes zur Überwachung der Videoüberwachung. Ziel ist die Ausweitung der staatlichen Kontrolle durch Zugriff auf persönliche Daten in immer mehr Lebensbereichen, alles unter dem Label „Sicherheit“. […] zuletzt sei noch erwähnt, dass vom Minister und anderen Verantwortlichen unerwähnt bleibt, dass abschreckende Effekte, abgesehen von Delikten gerichtet gegen Eigentum, durch den Einsatz von Videoüberwachung bisher nicht nachgewiesen werden konnten.[60]

---

58 Ebd., S. 3 f.

59 Heidelberg u.a., *Grundrechtereport 2018 – zur Lage der Menschen- und Bürgerrechte in Deutschland*.

60 Ruhwedel, *Pilotprojekt zur Gesichtserkennung*, Grundrechtereport 2018, S. 26.

> [**Zum sog. Offline-Tracking**:] [… N]icht nur Polizeibehörden haben ein Interesse an der sog. intelligenten Videoüberwachung, auch die kommerzielle Videoüberwachung entwickelt sich weiter. Bekannt wurde dies, als die Supermarktkette REAL sowie die Deutsche Post einräumen mussten, beim Einsatz ihrer Software neuartige Software einzusetzen. Diese vermag in Sekundenbruchteilen Alter, Geschlecht und Stimmungen von Menschen einzuschätzen. […] Kommerzielles Tracking im Alter erfolgt auch mittels Smartphones, die eine Mehrzahl der BürgerInnen ständig bei sich tragen. […] Mit diesem sozialen und technischen Wandel hin zu einer allgegenwärtigen, sensorgestützten Erfassung unserer Alltagswelten verschieben sich aber bislang sicher geglaubte Zugänglichkeitsgrenzen und Freiräume. Für die BürgerInnen wächst das Risiko, die bisherige relative Anonymität des Alltags zu verlieren. Es entsteht absehbar eine Beobachtungslandschaft, in der immer mehr Akteure das individuelle Verhalten in öffentlichen und öffentlich zugänglichen Räumen erfassen. [61]

Als besonderes Problemfeld werden im Kontext von Sicherheitsstrategien insbesondere **transnationale Datenströme** benannt, die mit der Globalisierung notwendig einhergehen, für die rechtliche Rahmenbedingungen aber noch weitgehend fehlten. Beispielhaft wird das für unwirksam erklärte Safe-Harbour-Abkommen zwischen der EU und den USA genannt, das an den unterschiedlichen Datenschutzstandards der beiden Rechtsräume scheiterte.

> [D]ifferences in national legal frameworks and their enforcement mechanisms raise worldwide disputes about internationally feasible regulation.
>
> Emphasizing the differences in national frameworks, in the 2015 **Maximilian Schrems v. Data Protection Commissioner decision of the European Court of Justice** a relevant example is provided: Personal data was transferred from a European Facebook account to the United States of America. As US-rights of data protection differ from European rights and do, according to the Data Protection Commissioner of the EU Court of Justice, "not offer sufficient protection against surveillance by public authorities" (Schrems 2015, 1) the US Safe Harbour Decision was declared invalid (ibid.). The decision reverses the so called **"Safe Harbor" agreement** between [the] US and EU in 2000 which effectively smoothed over differences in the legal standards around privacy in the two respective unions. Though this agreement and its 2002 reaffirmation by the EU Commission previously sufficed as a resolution of inadequacies and contradictions, in the post-Snowd[e]n environment a reversion to the adherence [to] the supranational Charter of Fundamental Rights of the European Union, and its rigid protection of individual privacy, highlights idiosyncrasies in the collision of multilayered legislation. [62]

Als Maßstab gerade für derartige transnationale Sachverhalte wird ein **Rückgriff auf menschenrechtliche Bindungen** angemahnt, wobei gleichzeitig auf fehlende effektive Durchsetzungsmechanismen verwiesen wird.

---

61 Leopold, *Offline-Tracking – Einem wütenden Mann Mitte 30 rasch eine Flasche Whiskey empfehlen*, Grundrechtereport 2018, S. 30.

62 Damen/Köhler/Woodard, *The Human Right of Privacy in the Digital Age*, Staat, Recht und Politik – Forschungs- und Diskussionspapiere, Bd. 3 (2017), S. 3 f.

> Reinforcing the international perspective on this issue, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson, concurs with the High Commissioner for Human Rights that where States penetrate infrastructure located outside their territorial jurisdiction, **they remain bound by their obligations under the Universal Declaration of Human Rights** (UN 2014e, A/69/397). A multilevel legal framework reinforces the respective obligations; however it does not begin to resolve the issue of the **lack of necessary multilateral enforcement mechanisms**. [63]

Konkreter Maßstab ist nach dem Hochkommissar der Vereinten Nationen für Menschenrechte in diesem Zusammenhang die **Notwendigkeit und Verhältnismäßigkeit** der Maßnahme:

> 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. [64]

4.3.5. Die Entwicklung des Menschenrechtsschutzes und -diskurses auf diesem Gebiet

Der Menschenrechtsdiskurs zum Recht auf Privatsphäre **hat sich in den letzten Jahren stark weiterentwickelt**, wobei insbesondere die Enthüllungen Edward Snowdens zu den Überwachungstätigkeiten der US-amerikanischen und britischen Geheimdienste im Jahr 2013 eine entscheidende Zäsur bildeten. [65]

---

63 Ebd., S. 4.

64 Bericht des Amtes des Hohen Kommissars der Vereinten Nationen für Menschenrechte, A/HRC/27/37, 30. Juni 2014, *Das Recht auf Privatheit im digitalen Zeitalter*, S. 9.

65 Damen/Köhler/Woodard, *The Human Right of Privacy in the Digital Age*, Staat, Recht und Politik – Forschungs- und Diskussionspapiere, Bd. 3 (2017), S. 4.

4.3.5.1. Snowden-Enthüllungen als Wendepunkt des Diskurses

Es fällt auf, dass sich die menschenrechtlichen Maßnahmen bis zu diesem Zeitpunkt vor allem auf die **Rechte gegenüber autoritären Regimen** konzentrierten:

> Before 2013, resolutions from the UN-General Assembly were primarily concerned with bolstering privacy rights under oppressive regimes as a mechanism for protecting the freedom to speech, opinion and expression in a democratic society. For example the Resolution 7/36 from the Human Rights Council (UN 2008, R/7/36), a mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (March 2008) or Resolution L13 , the Promotion, Protection and Enjoyment of Human Rights on the Internet (UN 2012, A/HRC/20/L.13).[66]

Ein erster Einschnitt des menschenrechtlichen Diskurses ergab sich anschließend, als die menschenrechtlichen **Implikationen des amerikanischen „War on Terror“** sichtbar wurden:

> Whether by discerning eletronic from traditional communication, or by bringing all forms of communications under privacy protection national and international law failed under legislation enacted by the USA Patriot-Act of 2001. As stated by the US Department of Justice, the Patriot Act's effect on the pre-existing ECPA results in the "[...] easing [of] restrictions on law enforcement access to stored communications in some cases" (ibid.). Twelve years later, the international human rights community found itself confronting the uncomfortable fact that the Patriot Act disabled privacy protections on a sweeping global scale. [67]

Spätestens **seit den Snowden-Enthüllungen im Jahr 2013**, durch die bekannt geworden ist, dass Staaten flächendeckend und massenhaft überwachen, ist der **Schutz vor anlasslosen staatlichen Überwachungsmaßnahmen** in das primäre Interesse des Menschenrechtsschutzes gerückt.

> The new facts the human rights community had to negotiate after Snowden's revelations was not that the US and UK intelligence agencies (NSA and GCHQ) were intercepting and monitoring electronic communications of targeted sources in the "war on terror". Rather the NSA and GCHQ, with use of an agency developed program PRISM, were **indiscriminately monitoring the communications of US and UK citizens, as well as foreign nationals**. Dating back to 1988, the United Nations Human Rights Committee (HRC) has been calling attention to **the important distinction between targeted and indiscriminate data collection** in the General Comments made on CCPR Article 17 (Right to Privacy).
>
> "[...] 'arbitrary interference' can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances." (UN 1988, HRI/GEN/1/Rev.9 (Vol. I), 1)

66 Ebd.

67 Ebd., S. 5.

> Proponents of increased surveillance will point to the events of 9/11, the decentralization of power within terrorist networks, and the ever evolving nature of digital communications as "particular circumstances" which necessitate the blanket collection of digital communications and data to prevent further terror attacks. However, in direct response to the Snowdon revelations the Special Rapporteur Emmerson reiterated demands that, "relevant States are in a position to justify as proportionate the systematic interference with the Internet privacy rights of a potentially unlimited number of innocent people located in any part of the world" (UN 2014e, A/69/397, 20).
>
> **The overwhelming majority of voices from the human rights community and civil society on the new threats to personal privacy**, namely that the intelligence communities' indiscriminate interception and storage of bulk user data, **goes to the very heart of the social contract in modern democracies.**
>
> "Bulk access technology is indiscriminately corrosive of online privacy and impinges on the very essence of the right guaranteed by article 17 [Right to Privacy]. In the absence of a formal derogation from States' obligations under the Covenant, these programmes pose a direct and ongoing challenge to an established norm of international law." (UN 2014e, A/69/397, 21)
>
> In its comment on CCPR Article 17, the Human Rights Committee also emphasises the importance of guaranteeing integrity and confidentiality of correspondence "de jure and de facto" (UN 1988, HRI/GEN/1/Rev.9 (Vol. I), 2). [68]

Das daraus folgende geschärfte Bewusstsein hat sich in einigen handfesten Maßnahmen auf dem Gebiet des Menschenrechtsschutzes niedergeschlagen: Die **Generalversammlung und der Menschenrechtsrat der Vereinten Nationen** haben in **mehreren Resolutionen seit 2013** die besondere Bedeutung der Privatsphäre im digitalen Zeitalter betont und Vorkehrungen für deren Schutz getroffen.

4.3.5.2. VN-Resolution 68/167 (2013)

Ausgangspunkt dieser Entwicklung war die **Resolution 68/167 der VN-Generalversammlung vom 18. Dezember 2013**.[69] Darin wird zunächst die Reichweite des technischen Wandels, die Wichtigkeit des Privatsphäreschutzes und die von staatlicher Überwachung ausgehenden Gefahren aufgezeigt:

> Noting that the **rapid pace of technological development** enables individuals all over the world to use new information and communication technologies and at the same time enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which **may violate or abuse human rights**, in particular the right to privacy, as set out in

68 Ebd.

69 VN-Generalversammlung, Resolution A/RES/68/167, *The right to privacy in the digital age*, 18. Dezember 2013, verfügbar unter http://undocs.org/A/RES/68/167.

article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, and is therefore an issue of increasing concern,

Reaffirming the human right to privacy, according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference, and recognizing that the exercise of the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference, and is one of the foundations of a democratic society,

Stressing the **importance of the full respect for the freedom to seek, receive and impart information**, including the fundamental importance of access to information and democratic participation,

Emphasizing that **unlawful or arbitrary surveillance and/or interception of communications**, as well as unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the rights to privacy and to freedom of expression and may contradict the tenets of a democratic society,

Noting that while concerns about **public security may justify** the gathering and protection of certain sensitive information, States must ensure full compliance with their obligations under international human rights law,

Deeply **concerned at the negative impact** that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights … [70]

Auf Grundlage dessen stellt die Generalversammlung **konkrete Forderung an die Staaten** zum Schutz der Menschenrechte im digitalen Zeitalter:

4. Calls upon all States:

(a) To **respect and protect** the right to privacy, including in the context of digital communication;

(b) To **take measures** to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law;

(c) To **review their procedures, practices and legislation** regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

70 Ebd.

> (d) To **establish or maintain existing independent, effective domestic oversight mechanisms** capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data … [71]

Schließlich forderte die Generalversammlung den **Hochkommissar für Menschenrechte** auf, **Report über die Menschenrechtssituation** im Hinblick auf Massenüberwachungen zu erbringen.

> 5. Requests the United Nations **High Commissioner for Human Rights to submit a report** on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale, to the Human Rights Council at its twenty-seventh session and to the General Assembly at its sixty-ninth session, with views and recommendations, to be considered by Member States

Die **Maßnahmen der Resolution** werden unterschiedlich bewertet. Einerseits wird argumentiert, dass die prominente Anerkennung der Menschenrechte auch im digitalen Raum einen **wichtigen Schritt** darstellt.

> Diplomaten sehen die aktuelle Fassung als wichtigen Schritt bei der Ausweitung der Menschenrechte im digitalen Zeitalter: Erstmals in der Geschichte der UNO wird der Schutz der Privatsphäre, wie er zum Beispiel im Brief- und Post- (Kommunikations-)geheimnis festgeschrieben ist, auch fürs Internet explizit verankert. Die NSA, das GCHQ und andere Geheimdienste greifen in großem Umfang internationale Kommunikation ab, spionieren Unternehmen sowie staatliche Stellen aus und verpflichten Dienstleister im Geheimen zur Kooperation. Einzelheiten dieses teilweise totalitär angelegten Überwachungssystems enthüllen die geheimen Dokumente, die der Whistleblower und ehemalige NSA-Analyst Edward Snowden an sich gebracht und an Medien weitergegeben hat.
>
> Die Resolution kam insbesondere auf Betreiben von Deutschland und Brasilien zustande, beides Länder, deren politische Führungen gezielt von den USA ausspioniert wurden. Die Arbeit daran hatte bereits begonnen, bevor die Bespitzelung von Bundeskanzlerin Merkel bekannt geworden war. Die ergänzt und erweitert den Pakt für zivile und politische Rechte. Die vorangegangenen Wochen hätten, so Stimmen aus deutschen Regierungskreisen, gezeigt, dass „gegen diese Regeln insbesondere im digitalen Raum systematisch verstoßen wird". Deutschlands damaliger Uno-Botschafter Peter Wittig meinte nach der Abstimmung: „Es geht um neue Herausforderungen für die Menschenrechte. Wir müssen uns fragen, ob alles, was technisch möglich ist, auch erlaubt sein darf." Die Resolution sei ein wichtiges Zeichen. „Wir zeigen die Bereitschaft und Fähigkeit der UNO, Herausforderungen für die Menschenrechte anzugehen und auf die Sorgen der Menschen zu reagieren."[72]

71 Ebd.

72 Weichert, *UNO-Resolution „zum Schutz der Privatheit im digitalen Zeitalter"*, Datenschutz und Datensicherheit – DuD Bd. 38 (6/2014), S. 402.

Andererseits wird **kritisiert**, dass die Erklärung letztendlich weniger drastisch formuliert wurde, insbesondere indem sie weder die Vereinigten Staaten noch die NSA explizit nennt und Raum für eine Bewertung lässt, wann Überwachungsmaßnahmen Menschenrechte verletzen.

> Zuvor war die Resolution auf Drängen der USA **deutlich entschärft** worden. Die Vereinigten Staaten (USA) hatten in einem eigentlich geheimen Schreiben an Alliierte kritisiert, dass der erste Entwurf andeute, Staaten seien durch Menschenrechte verpflichtet, die Privatsphäre von Ausländern im Ausland zu achten. Die USA konnten sich mit ihrer Forderung teilweise durchsetzen, den Text zu ändern. In der abschließenden Fassung zeigt sich der Staatenbund lediglich „tief besorgt" über grenzüberschreitende Abhöraktionen und deren Folgen für die Menschenrechte. Das Papier nennt weder die USA noch die NSA namentlich. Die Überwachung des Internetverkehrs wird nicht in jedem Fall als Menschenrechtsverletzung betrachtet. [73]

Schließlich wird auch die **praktische Wirkung** differenziert bewertet; der Resolution kommt zwar keine unmittelbare völkerrechtliche Bindungswirkung zu, ihr wird jedoch ein umso höherer **symbolischer und politischer Wert** beigemessen.

> Im Gegensatz zu einer Resolution des UN-Sicherheitsrats ist eine Resolution wie diese zum „Recht auf Privatheit im digitalen Zeitalter" der UN-Generalversammlung **nicht völkerrechtlich bindend**. Mit der geballten Macht der Zustimmung aller UN-Mitgliedsstaaten im Rücken kann sie aber eine nicht zu unterschätzende **symbolische Wirkung** entfalten. Dies ist auch der Grund, warum die USA hinter den Kulissen so entschieden daran gearbeitet haben, den Text zu stutzen und den Inhalt abzuschwächen. Mit der Resolution kommt das Thema Online-Privatsphäre zum ersten Mal seit langem auf die Agenda der UNO. Die Resolution traf auf eine **breite Unterstützung**. Selbst Staaten, die mit ihrer Praxis der Anlass für das Papier waren, stimmten zu. Dazu gehören die USA, die wegen der Ausspähung fremder Bürger kritisiert worden waren, aber auch Länder wie Russland und Nordkorea, die wegen der Überwachung der eigenen Bürger in der Kritik stehen. [74]

4.3.5.3. Erster Jahresbericht des Hochkommissars für Menschenrechte (2014)

In dem Jahresbericht vom 30. Juni 2014 (A/HRC/27/37) **benennt der Hochkommissar für Menschenrechte** die menschenrechtliche **Eingriffsqualität** staatlicher Massenüberwachung und ihre **Grenzen**.[75] Der Bericht wird als maßstabsetzend betrachtet und geht konkret auf folgende Fragen ein:

> Die Enthüllungen über digitale Massenüberwachung werfen […] 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**

73 Ebd.

74 Ebd.

75 Bericht des Amtes des Hohen Kommissars der Vereinten Nationen für Menschenrechte, A/HRC/27/37, 30. Juni 2014, *Das Recht auf Privatheit im digitalen Zeitalter*.

> **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.
>
> 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. [76]

In dem Bericht wird der **Begriff des „Eingriffs" in die Privatsphäre** ausdrücklich als besonders weit formuliert. Insbesondere die Freiwilligkeit der Preisgabe der Daten sei unschädlich (s. dazu oben 4.3.3) und auch die Erhebung von Metadaten sei erfasst. **Schon die Existenz eines Programms zur Massenüberwachung stellt demnach einen Eingriff in die Privatsphäre dar**:

> 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". […]
>
> 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." Die Erkenntnis dieser Entwicklung hat zu Initiativen geführt, die die bestehenden Politiken und Praktiken reformieren wollen, um einen stärkeren Schutz der Privatsphäre zu gewährleisten.
>
> 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**, der einen abschreckenden Effekt auf andere Rechte, namentlich die der freien Meinungsäußerung und der Vereinigungsfrei-

76 Ebd., S. 6.

> heit, 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. [77]

Der **Maßstab für die menschenrechtliche Zulässigkeit eines Eingriffs** lautet klar:

> Eingriffe in das Recht eines Menschen auf Privatheit sind nach den internationalen Menschenrechtsnormen nur zulässig, wenn sie **weder willkürlich noch rechtswidrig** sind. [78]

Es folgen Ausführungen dazu, wann genau ein Eingriff als willkürlich oder rechtswidrig zu betrachten ist.

> In seiner Allgemeinen Bemerkung Nr. 16 erläuterte der Ausschuss, dass der Begriff „**rechtswidrig**“ bedeutet, 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.“ 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.“ 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”. […]
>
> 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 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. 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

77 Ebd., S. 6 f.

78 Ebd., S. 7.

> 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. [79]

Als elementarer Bestandteil des Menschenrechtsschutzes wird außerdem die Möglichkeit genannt, **effektiven Rechtsschutz** zu erlangen. Grundlegende Voraussetzung dafür ist, dass jede Kommunikationsüberwachung auf einem nationalen Gesetzes beruht, das wiederum mit der Rechtsordnung im Einklang steht und ggf. gerichtlich überprüft werden kann:

> 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**. „Zugänglichkeit" erfordert nicht nur, dass das Gesetz veröffentlicht wurde, sondern dass es so präzise formuliert ist, 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.
>
> Geheime Vorschriften und geheime Auslegungen – selbst geheime gerichtliche Auslegungen – erfüllen daher nicht die Merkmale eines „Gesetzes". 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. […]
>
> 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

79 Ebd., S. 8 f.

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. [80]

Bestandteil eines wirksamen Rechtsschutzes sind schließlich auch **verfahrensmäßige Sicherungen**, insbesondere Kontroll- und Benachrichtigungspflichten:

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

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. [81]

Und schließlich ist insbesondere eine **unabhängige rechtliche Überprüfungsmöglichkeit** für Überwachungsmaßnahmen im Sinne der Menschenrechte zwingend.

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,

80 Ebd., S. 10 f.

81 Ebd., S. 13 f.

> nach den Rechtsvorschriften des Staates zuständige Stelle feststellen lassen kann, und den gerichtlichen Rechtsschutz auszubauen." Außerdem müssen die Staaten dafür Sorge tragen, dass die zuständigen Stellen Beschwerden, denen stattgegeben wurde, Geltung verschaffen. […]
>
> 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. […]
>
> 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". 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. […] Viertens werden dort, wo Menschenrechte in einem Ausmaß verletzt werden, dass der Tatbestand einer groben Verletzung erfüllt ist, nichtgerichtliche Rechtsschutzmaßnahmen nicht mehr ausreichen; in solchen Fällen ist eine strafrechtliche Verfolgung erforderlich. [82]

In diesem Zusammenhang wird außerdem klargestellt, dass die menschenrechtliche Bindung von Staaten über das eigene Hoheitsgebiet hinausreicht, also auch **extraterritorial** anwendbar ist.

> 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. 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, 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

82 Ebd., S. 14 f.

auch strukturelle Anreize für Staaten schaffen, Überwachungsaktivitäten wechselseitig auszulagern.

Daraus folgt, dass **digitale Überwachungsmaßnahmen die Menschenrechtsverpflichtungen eines Staates berühren können, wenn die Überwachung mit der Ausübung staatlicher Gewalt 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. […]

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 oder sehen anderweitig ein geringeres Schutzniveau für Auslands- bzw. externe Kommunikation vor.

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**". [83]

Zuletzt nimmt der Bericht den **Technologiesektor** in den Blick und betont dessen Verantwortung für den Schutz der Menschenrechte.

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 möglich ausgelegt werden, dass von den staatlichen Stellen eine Klarstellung des Umfangs und der Rechtsgrundlage

83 Ebd., S. 12 f.

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. […]

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. [84]

4.3.5.4. Weitere Entwicklung des menschenrechtlichen Schutzes der Privatsphäre

Mit der Resolution von 2013 und dem Bericht des Hochkommissars für Menschenrechte von 2014 hat die Frage des Schutzes der Privatsphäre einen **festen Platz in der menschenrechtlichen Dogmatik erlangt**, an den durch vielfältige regelmäßige Maßnahmen durch die Vereinten Nationen **bis heute angeknüpft wird**.

Mit Resolution 69/166 hat die Generalversammlung den Jahresbericht des Hochkommissars für Menschenrechte zur Kenntnis genommen und das Ergreifen von Maßnahmen angemahnt.[85]

Im April 2015 hat der Menschenrechtsrat durch Resolution 28/16 einen **Sonderberichterstatter der Vereinten Nationen zum Recht auf Privatheit** (eng. „Special Rapporteur on the right to privacy“) eingesetzt,[86] der die Aufgabe hat, der VN-Generalversammlung Berichte und Empfehlungen zum Schutz des Rechts auf Privatsphäre vorzulegen:

---

84 Ebd., S. 12 f.

85 VN-Generalversammlung, Resolution A/RES/69/166, *The right to privacy in the digital age*, 18. Dezember 2014, verfügbar unter http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/166.

86 VN-Menschenrechtsrat, Resolution A/HRC/RES/28/16, *The right to privacy in the digital age*, 1. April 2015, verfügbar unter https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/068/78/PDF/G1506878.pdf?OpenElement.

> In April 2015, the Human Rights Council appointed the first Special Rapporteur on the right to privacy, responsible for the mandate of **reporting violations of this right** and of **rising awareness** towards the importance of its protection, as well as further threats and challenges arising from new technologies (UN 2015, A/HRC/28/L.27, 3f). This Special Rapporteur, Prof. Joseph Cannataci, of Malta, is collecting information related to the issue of privacy in the digital age – including international and national frameworks and the experiences, practices, trends, challenges and developments of different nations. Cannataci reports to the UN General Assembly and proposes recommendations to ensure the "promotion and protection" (ibid., 4) of the right to privacy. [87]

Der Sonderberichterstatter hat einen **Zehn-Punkte-Plan** entworfen, indem neben einer einheitlichen Definition des Rechts auf Privatsphäre und der individuellen Verantwortung der Bürger ebenfalls insbesondere die Verantwortung der Unternehmen besonders betont wird.

> In March 2016, the Special Rapporteur introduced a 10-Point Action Plan for the period of his mandate. It includes the development of a **clear and universal definition for the "right to privacy"**, which all 21st century global citizens should be able to understand and apply to their own lives – on and offline. The Action Plan also calls for the initiation of a general discourse, and the **raising of awareness amongst citizens** around the imperatives of managing their own privacy (UN 2016a, A/HRC/31/64, 18f). Cannataci asserts that citizens should have I formation about the monetization of their data and also learn how to protect themselves and minimize the risk of infringement of privacy. The Special Rapporteur also advocates a structured, comprehensive, effective, transparent and permanent dialogue between stakeholders.
>
> As the **corporate IT sector** gather the majority of personal data, it is especially important to focus on a "dialogue with the corporate world" (ibid., 18). Cannataci, therefore, sues "safeguards and remedies" (ibid.) and aims at **holding the tech community accountable** for the "promote the development of effective technical safeguards including encryption, overlay software and various other technical solutions" (ibid.). The 10-Point Action Plan further promotes the "national and regional development" (ibid.) of **mechanisms to protect privacy** in coordination with representatives of civil society organizations. It also wants to tackle cyber-realities, and – starting with an update of legal instruments – is going to invest in "**development of international law relevant to privacy**" (ibid.). Therefore, a better understanding of the term "right to privacy" (ibid., 18-19) is necessary. [88]

Auch aus der Technologiebranche selbst kommen verstärkt Anregungen zum Schutz der Menschenrechte im Lichte der Digitalisierung, wobei insbesondere das **Anliegen der Cybersicherheit**, also der Schutz von Daten und Informationssystemen, als zusätzliche Dimension eines wirksamen Menschenrechtsschutzes auf die Agenda gesetzt wurde.

> Smith [president and chief legal officer of Microsoft] was calling upon technology companies "to do more to protect and defend" (ibid.) customers worldwide and also upon world governments to protect civilians by implementing international rules. He states, that **civilians should be protected by governments from nation-states' cyberspace attacks** based on a "**Digital Geneva Convention**"

87 Damen/Köhler/Woodard, *The Human Right of Privacy in the Digital Age*, Staat, Recht und Politik – Forschungs- und Diskussionspapiere, Bd. 3 (2017), S. 7.

88 Ebd.

(ibid.), in the same way that civilians have the right to physical protection during times of war by the Fourth Geneva Convention.

Further, Smith stresses, that the **active cooperation of the technology sector is necessary to protect civilians against cyberattacks**. Continuing his metaphor, Smith states that involvement of the technology sector is now as necessary to protect human rights as the 1949 requirement of "active involvement of the Red Cross" (ibid.) to protect civilians from the primary threat to their human rights, as recognized in the Fourth Geneva Convention. The technology sector, for its part, plays an indispensable role as their companies are the first responders to cyberattacks and threats. Therefore, **cybersecurity norms should become global rules of a multilateral agreement** between the worlds governments (ibid.). [89]

In den **Berichten des Sonderberichterstatters** an die Generalversammlung werden seitdem regelmäßig die Problemfelder auf dem Gebiet des Privatsphäreschutzes identifiziert und die Menschenrechtssituation auf diesem Gebiet evaluiert:

In his first report to the General Assembly in August 2016 Prof. Joseph Cannataci identified critical areas in the protection of privacy. Beyond promoting the development of a greater understanding of privacy, the report prioritized awareness around "Thematic Action Streams (TAS) on Big Data and Open Data; Security and Surveillance, Health Data" (UN 2016b, A/71/368, 8) and "Personal data processed by corporations" (ibid.). Different working parties with high expertise shall organize events "to **gather evidence and identify options for strategies which would produce improved safeguards and remedies for privacy in a given sector of activity**" (ibid., 2).

In his report to the Human Rights Council in March 2017, Cannataci stated that **measures of current national legislation to regulate government surveillance are extremely intrusive, inefficient, and non-proportional**. Drafted laws have been "rushed through the legislative process" (UN 2017, A/HRC/34/60, 7) in order to legitimize practices of surveillance. Governments thereby make use of the fear of terrorism and manipulate policy-makers to adopt "unduly disproportionate privacy-intrusive laws" (ibid., 15). This sentiment is echoed throughout the many investigations into government surveillance by the UN and the many civil society actors specially engaged around this issue, which characterizes the moral collision course set by intelligence community special interests and regulators defending individual sovereignty. [90]

Zuletzt hat der **Menschenrechtsrat mit Resolution 34/7 vom 7. April 2017** den Menschenrechtsdiskurs auf diesem Gebiet fortgeführt und die dargelegten Grundsätze zunächst erneut bestätigt, um anschließend eine Reihe weiterer Problemfelder aufzuzeigen; neben dem Schutz von Metadaten insbesondere die Gefahr von Diskriminierungen auf Grundlage automatisierter Datenverarbeitung.

Noting that the rapid pace of technological development enables individuals all over the world to use information and communications technology and at the same time enhances the capacity of Governments, business enterprises and individuals to **undertake surveillance, interception and**

89 Ebd., S. 6 f.

90 Ebd., S. 8.

> **data collection, which may violate or abuse human rights**, in particular the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, and is therefore an issue of increasing concern,
>
> Noting also that, while **metadata** may provide benefits, certain types of metadata, when aggregated, can reveal personal information that can be no less sensitive than the actual content of communications and can give an insight into an individual's behaviour, social relationships, private preferences and identity,
>
> Noting with concern that **automatic processing of personal data for individual profiling may lead to discrimination** or decisions that otherwise have the potential to affect the enjoyment of human rights, including economic, social and cultural rights, and recognizing the need to further discuss and analyse these practices on the basis of international human rights law[91]

Im Übrigen werden durch diese Resolution primär die **Erwartungen an die Staaten und Unternehmen bekräftigt**, den Privatsphäreschutz voranzutreiben und wirksame Maßnahmen zu treffen, die in der Presse wie folgt zusammengefasst werden:

> Kaum bemerkt von der Öffentlichkeit, hat sich die Vollversammlung der Vereinten Nationen im November vergangenen Jahres nun schon zum dritten Mal nach 2013 und 2014 einstimmig auf eine Grundsatzerklärung zum "Schutz der Privatheit im digitalen Zeitalter" verständigt. […]
>
> In ihrer Resolution konstatieren die Staaten der Vereinten Nationen die Entwicklung eines weltweiten Überwachungssystems. Sie stellen fest, dass durch die neuen Technologien die Fähigkeiten von Regierungen, Firmen und Einzelpersonen gesteigert werden, Überwachungen und Datensammlungen in die Wege zu leiten, die Menschenrechtsverletzungen – insbesondere des Rechts auf Privatheit – zur Folge haben. Sie fordern, dass niemand eigenmächtiger und ungesetzlicher Einmischung in seine Privatheit, Familie, Wohnung oder Kommunikation unterworfen werden darf.
>
> Das Recht auf Privatheit wird als bedeutsam angesehen für die Ausübung von Meinungsfreiheit, Versammlungsfreiheit und Vereinigungsfreiheit. Der Schutz der Privatheit ist schon angelegt in der Allgemeinen Erklärung der Menschenrechte von 1948 und später als bindendes Völkerrecht im sogenannten Zivilpakt von 1966.
>
> Die Verletzungen, die dieses Menschenrecht heute erfährt, werden in der Grundsatzerklärung kritisiert – ebenso angeprangert wird die Verfolgung derjenigen, die diese Freiheiten zu schützen suchen. Der Freiheit, Informationen zu suchen, zu empfangen und zu übermitteln, soll „voller Respekt" entgegengebracht werden. Der freie Zugang zu Informationen und zu demokratischer Partizipation muss gewährleistet sein.

---

91 VN-Menschenrechtsrat, Resolution A/HRC/RES/34/7, *The right to privacy in the digital age*, verfügbar unter https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/086/31/PDF/G1708631.pdf?OpenElement.

> Die besonderen Gefahren der anlasslosen Massenüberwachung werden ebenfalls kritisiert. Zur Bekämpfung von Terrorismus wird gefordert, dass sich die Staaten an die Verpflichtungen des Internationalen Rechts, insbesondere an den Schutz der Privatheit und des humanitären Völkerrechts halten.
>
> Es werden also eindeutige Forderungen sowohl an die Staaten wie an die privaten Datenverarbeiter gerichtet. Diese sollen auf gesetzlichem Wege auf den Schutz der Privatheit verpflichtet werden. Unabhängige Mechanismen sollen Transparenz und Schutz gewährleisten, auch Sanktionen werden erwogen. Private Firmen sollen vor dem Ansinnen des Staates geschützt werden, Informationen unter Bruch des Privatheitsschutzes herausgeben zu müssen. Die Europäische Union hat mit der 2018 in Kraft tretenden Datenschutzgrundverordnung in diesem Sinne bereits gehandelt.[92]

Der Menschenrechtsrat ist damit seinem Auftrag nachgekommen, gerade im globalisierten digitalen Raum die Einhaltung der Menschenrechte prominent anzumahnen und den Diskurs auf diesem Gebiet weiter zu fördern – so eine Sichtweise.

> Mit diesem Dokument beschreibt und kritisiert die Vollversammlung, anders als es die eher zurückhaltenden Politiker in unserem Lande tun, die vielfachen Freiheitsverletzungen, die das Internet bewirkt – unabhängig von den großen Chancen, die es eröffnet. Das Internet ist der Treibsatz der Globalisierung. Es ist wirtschaftliche und politische Macht. Das Informationszeitalter hat eine Nachtseite.
>
> National oder in Europa allein sind die Entwicklungen nicht mehr zu fassen. Aus diesem Grunde forderte der Europäische Gerichtshof eine "Konstitutionalisierung internationaler Datenströme", und das ist in erster Linie eine Aufgabe der UN, insbesondere von deren Menschenrechtsrat. [93]

Zur **vereinzelten Kritik an den Schutzmaßnahmen** zum Schutz der Menschenrechte im Digitalzeitalter wird an dieser Stelle entgegnet, dass das Bemühen trotz der vielfältigen Verstöße nicht aufgegeben werden, sondern vielmehr nach gemeinsamen Interessen insbesondere mit der Technologiebranche gesucht werden sollte.

> Nun wird oft eingewandt, dass die Realität an diesen Forderungen vorbeigehe. Ja, das stimmt. Doch alle Erfahrungen zeigen: Solche Menschenrechtsstandards bringen Menschenrechtsverletzer in eine argumentative Defensive. So verhält es sich auch in anderen Fällen: Soll etwa das Folterverbot aufgegeben werden, weil immer noch gefoltert wird?
>
> Schützenhilfe bei dem Bemühen, Privatheitsschutz zu globalisieren, kommt seit Kurzem von ganz unerwarteter Seite: aus dem Silicon Valley. Da lautete seit Jahren die trotzige Parole „privacy is no longer a social norm“. Mittlerweile scheinen Macher im Silicon Valley ihre Kritiker ernst zu nehmen. Sie sehen, dass ihre eigenen Produkte Gefahren für Freiheit und Wohlstand mit sich bringen, und fürchten um ihr Geschäftsmodell.

---

92 Baum, *Vereinte digitale Nationen*, DIE ZEIT 22/2017, verfügbar unter https://www.zeit.de/2017/22/menschenrechte-schutz-der-privatheit-digitalcharta.

93 Ebd.

> Mark Zuckerberg formuliert das so: „Das Wichtigste, was wir in diesen Zeiten bei Facebook tun können, ist, die soziale Infrastruktur zu entwickeln, die den Menschen die Macht gibt, eine globale Gemeinschaft zu bauen, die für uns alle funktioniert.“ Sind das Ansatzpunkte, um weltweit gemeinsam ethische Standards zu entwickeln?
>
> Es sind jedenfalls immer die gemeinsamen Interessen, die zu Übereinkünften führen. So wird Kriminalität im Cyberspace mit der Cybercrime Convention bereits weltweit bekämpft. Eine neue Genfer Konvention gegen Kriegführung durch Cyberangriffe sollte ebenfalls erwogen werden. Vor allem sind Abkommen zur Bändigung des Internets erforderlich. Es gibt dafür Beispiele aus dem Bereich der Abrüstung (beispielsweise Vereinbarungen über Atomwaffen, Chemiewaffen, Landminen), neuerdings auch die wegweisende Pariser Übereinkunft zum Klimaschutz.
>
> Der Primat der Politik muss wiederhergestellt werden, um der schrankenlosen Dynamik der Technologie Grenzen zu setzen.
>
> Und die Zivilgesellschaft sollte angesichts dieser Gefahren aufwachen. [94]

In der Resolution ist außerdem ein **Workshop des Hochkommissars für Menschenrechte** mit dem Zweck der „Identifizierung und Klärung der Prinzipien, Standards und Best Practices bezüglich der Förderung und des Schutzes des Rechts auf Privatsphäre im digitalen Zeitalter“ vorgesehen, der im Februar 2018 stattgefunden und folgende Themen aufgegriffen hat:

> [R]ole of the right to privacy within the human rights framework and for civic space protection, Surveillance and communications interception, Securing and protecting online confidentiality, Processing of personal data by individuals, Governments, business enterprises and private organisations, New and emerging issues, Procedural and institutional safeguards, oversight and remedies[.] [95]

Die Vereinten Nationen haben in diesem Bereich also erhebliches Engagement gezeigt, das **im politischen Raum** überwiegend als bedeutender Maßstab für den Privatsphäreschutz bewertet wird – durch Gerhart Baum, der sich in der Presse dazu besonders ausführlich geäußert hat, etwa mit den Worten:

> Die Vereinten Nationen haben sich also auf den Weg gemacht, eine Art "**Magna Charta des Schutzes der Privatheit im Völkerrecht**" zu entwickeln – ein universell geltendes Menschenrecht. [96]

---

94 Ebd.

95 Concept Note zu dem Workshop verfügbar unter https://www.ohchr.org/Documents/Issues/DigitalAge/ConceptNote.pdf.

96 Baum, *Vereinte digitale Nationen*, DIE ZEIT 22/2017.

5. Ausblick – Maßnahmen zum Schutz von Menschenrechten im digitalen Zeitalter: Forderungen und Initiativen

5.1. Grundlegende Forderungen

Aufgrund der genannten vielfältigen Bedrohungen werden eine Reihe **konkreter Maßnahmen gefordert, durch die Staaten und sonstige Organisationen bedrohlichen Tendenzen entgegenwirken** könnten. Diese beziehen sich ganz überwiegend auf den Schutz der Privatsphäre, nehmen aber auch die anderen gefährdeten Rechte in den Blick. So etwa in der Tagespresse:

> Einzelne Staaten oder Organisationen, die unabhängig von den Bestrebungen zu internationalen Abkommen über Menschenrechtsschutz oder elektronische Waffen eine Verbesserung der Situation der Bevölkerung anstreben, sollten sich […] regional für schrittweise Verbesserungen einsetzen. Solche Verbesserungen könnten die verpflichtende Einführung von Kryptographie oder offener Software sein, ein strenger Datenschutz, und das Verbot des Handels mit personenbezogenen Daten. Dies wären erste Schritte zum besseren Schutz der Privatsphäre. Eine Überarbeitung des Urheberrechts wäre außerdem notwendig um die wachsenden Bedrohungen der Meinungsfreiheit abzuwenden. Eine gesetzliche Verpflichtung zur Netzneutralität und der Aufbau von anonymen Freifunknetzen könnte darüber hinaus einen diskriminierungsfreien Zugang gewährleisten, der alle Menschen gleichermaßen am technologischen Fortschritt und seinen Errungenschaften Teil haben lässt. So würde nicht nur ein Menschenrecht geschützt werden, sondern es kämen gleichzeitig mehr Stimmen und Ansichten zu Gehör, die bisher unbeachtet geblieben sind.[97]

Durch die **Menschenrechtsorganisation Amnesty International** werden folgende konkrete Forderungen genannt:

> Amnesty International fordert Regierungen weltweit auf,
>
> ● alle Programme zur Massenüberwachung unverzüglich zu beenden und sicherzustellen, dass alle Überwachungsmaßnahmen internationale Menschenrechtsstandards einhalten;
>
> ● sicherzustellen, dass Kommunikationsüberwachung nur bei einem konkreten Verdacht und nur mit einer richterlichen Genehmigung stattfindet und dass dabei die Mittel gewählt werden, die so wenig wie möglich in die betroffenen Menschenrechte eingreifen. Die Überwachungsmaßnahme muss gezielt, notwendig und verhältnismäßig sein;
>
> ● sicherzustellen, dass die Meinungs- und Informationsfreiheit online geschützt ist und Menschen auch über das Internet ohne Rücksicht auf Grenzen Informationen und Gedanken suchen, empfangen und verbreiten können. [98]

---

97 Karst, *Menschenrechte im digitalen Zeitalter*, der Freitag, 25. Februar 2015.

98 Amnesty International, *Menschenrechte im digitalen Zeitalter*, 4. Juni 2015.

Gerade zum Schutz der Privatsphäre sind in der Literatur darüber hinaus ausführlichere Konzepte entwickelt worden, die sämtliche beteiligten Akteure einbeziehen und diejenigen Maßnahmen aufschlüsseln, die im Sinne eines effektiven Menschenrechtsschutzes im digitalen Zeitalter erforderlich sind.

> **First off, international governance** needs to play a more effective role in this inherently international issue. The **definition of privacy** (in the digital age) must be universally clarified and become clear for all parties to be able to fight violations towards the right to digital privacy.
>
> An internationally effective legal framework on the right to privacy exists, but there is still much work to be done in order to "be sincere in our efforts to ensure a transparent, free, fair and respectful international intergovernmental mechanism of internet governance and one that also ensures the right to privacy" (Brown 2013). Current **international monitoring systems** need to be reviewed regarding their efficacy and commitment to protections. International bodies, such as the UN, that have garnered hard-won international consensus around the definition of, and commitment to, human rights and the steadfast protection of the values which they uphold have an acute need to develop **stronger implementation mechanisms** in order to hold individual signatory states responsible to their commitments.
>
> This is a monumental task, given that the multitude of vested interests around surveillance and data collection, in both the private sector and nation states, through military and intelligence communities, increase at rates similar to the exponential growth of digital technology's usage. States' legitimations of collecting personal data and communication interception must be scrutinized by independent regulatory bodies to ensure that they are justified under the universally accepted norms and values.
>
> **Secondly**, as stated at the RSA Conference, the **technology sector** plays a key role in fighting violations against **cyber-attacks**. It is the Internet's architect, content manager and the first responders in case of emergency. Also the tech field has the necessary knowledge and capabilities to tackle and prevent digital attacks at all levels with appropriate preventative and responsive protections.
>
> The mandate of a "Digital Geneva Convention" would ideally meet the needs of the quickly developing and ever-growing problem of eroding individual privacy. In this Convention, states are called on for an implementation of rules protecting the rights of civil society in the digital sphere. Consumers, companies and states worldwide have to be protected and the online-space needs to be a secure space. Therefore, IT providers and developers must take responsibility and respond in "new and innovative ways that disrupt attacks" (Smith 2017).
>
> **Thirdly**, there is an urgent need for the **stronger involvement of civil society**. Without the engagement of the citizens, customers, users, and individuals driving the momentum behind digital communications all other efforts to support individual sovereignty through the preservation of digital privacy will be for naught. On the one hand, **citizens must become more aware** of the information that they "voluntarily surrender [...] in return for digital access to goods, services and information" (UN 2014a, A/HRC.27.37, 6) and how easily their personal data through entertainment, social media, commerce, health and financial services can be surveilled by different stakeholders. The "reality of big data is that once data is collected, it can be very difficult to keep anonymous" (ibid.).

> On the other hand, there should be **more decisive political activism and joint movements by civil actors that put pressure on the public and the private sector**. At no juncture in private commerce, or public policy, development has there ever been movement without clear demand from the consumer base, or body politic, respectively. It is the belief of UN Special Rapporteur Cannataci, and of experts in the field of social development, that when equipped with the relevant information about the collection and use of their personal data, individuals will make informed choices and demand responsive policy making to protect their rights as consumers and citizens. [99]

Insbesondere die **Wichtigkeit einer engagierten Zivilgesellschaft**, die sich Gefährdungen der Privatsphäre entschieden entgegenstellt, wird in diesem Kontext verstärkt betont.

> The growing prominence of the Right to Privacy in the Digital Age over the past years would not have occurred without the presence of a robust and expert civil society constituency.
>
> This engaged constituency strived to achieve consensus on key issues ranging from the disproportionality of mass surveillance to the dangers associated with the bulk retention and acquisition of metadata. Also, the requirement to obtain legal authorization prior to the collection of personal data also remains central to consensus building. Civil society organizations have been highly effective in influencing the evolving discourse on the right to privacy in the digital age. They should continue to have a strong voice in the discussions. […]
>
> In turn, governments need to take a consistent line on privacy. Action to prevent unwarranted and speculative data collection by private companies is welcome but is undone when security becomes an excuse for disproportionate harvesting of information by government agencies. [100]

5.2. Konkrete Initiativen

Als besonders relevant werden in diesem Zusammenhang beispielsweise folgende **konkrete zivilgesellschaftliche Initiativen** genannt:

> For example, some private organizations, civil society organizations, and well as experts from all over the world established the "**13 International Principles on the Application of Human Rights to Communication Surveillance**". With their statement, they are urging governments to conduct communication surveillance that is consistent with human rights. The 13 Principles have been launched at the Human Rights Council in September 2013 (Brown, 2013) which itself is called to "reaffirm its commitment to promoting the right to privacy in light of evolving technologies and establish a framework for national guidelines" (ibid.).

---

99 Damen/Köhler/Woodard, *The Human Right of Privacy in the Digital Age*, Staat, Recht und Politik – Forschungs- und Diskussionspapiere, Bd. 3 (2017), S. 9 f.

100 International Federation of Library Associations and Institutions, *The right to privacy in the digital age*, S. 4.

Since the principles were published, more than 400 organizations, as well as thousands of citizens worldwide have co-signed the statement. The stated principles call for a transparent and continuously updated privacy protection legal basis and stronger regulation of surveillance.

Proper regulation would entail the necessity for states surveillance to be legitimate, adequate and necessary. The burden of proof for these criteria lies with the respective states. The principles also strive for "prior authorization from a competent judicial authority" (EFF 2013) that is "impartial and independent" (ibid.) before communication surveillance can be executed. All topics related to the violation of the human right to privacy should be available for the public and information given should be sufficient, transparent, accessible and accountable.

Individuals are to be more informed about any communication surveillance – except if there is a case of an urgent investigation, that should not be hindered, for example a legitimate threat of violence. In the technological sector, software, hardware and service providers should not collect information for the purpose of state surveillance. Lastly, the principles also call for the punishment of any illegal surveillance, and the development of a legal mechanism for those affected by surveillance (ibid.).

Policy makers, non-governmental organization, companies, as well as activists can make use of the above mentioned principles to create pressure on their governments and strive for a necessary change. The 13 Principles also "provide a benchmark" (EFF 2013) with which to measure the compliance of surveillance practices against the internationally held standard for human rights (ibid.).

Besides the development of the 13 International Principles there are a multitude of other civil society movements related to human rights and internet surveillance. One example is **Best Bits**, which is a network of worldwide civil society organizations that offers a platform for their members' agenda related to internet and state surveillance (Best Bits 2013). Other important statements on the "impact of surveillance on human rights" (Brown 2013) were written by **Amnesty International** and several **South Korean non-governmental organizations**. Such joint statements aim at ensuring "more systematic attention by the UN" (ibid.).

Essentially, the problem of maintaining individual sovereignty though the strengthening of digital security is a multifaceted issue which requires attention from all stakeholders. To be initiated on every level of digital engagement - from the grassroots individual user to the upper echelons of government responsible for overseeing surveillance programs - is a commitment to broadening awareness about the macro and micro management of data, and the strengthening of safeguards for all human rights in the 21st Century. [101]

101 Damen/Köhler/Woodard, *The Human Right of Privacy in the Digital Age*, Staat, Recht und Politik – Forschungs- und Diskussionspapiere, Bd. 3 (2017), S. 10.

In Deutschland ist die zivilgesellschaftlich entwickelte "**Charta der Digitalen Grundrechte der Europäischen Union**"[102] öffentlich besonders prominent in Erscheinung getreten, die eine Regelung der grundlegenden Rechte im digitalen Raum anstrebt und der Europäischen Union und der Öffentlichkeit zur Diskussion vorgelegt wurde.

> Die Initiative entstand 2015 auf Anregung von Giovanni di Lorenzo, Kurator der Stiftung im Rahmen des Bucerius Labs der ZEIT-Stiftung, das sich mit den Folgen und Gestaltungsmöglichkeiten der Digitalisierung beschäftigt. Gemeinsam mit 27 ExpertInnen aus verschiedenen Bereichen der Zivilgesellschaft – darunter Juli Zeh, Heinz Bude, Johnny Haeusler, Wolfgang Hoffmann-Riem, Jeanette Hofmann und Sascha Lobo – wurde eine digitale Grundrechtecharta erarbeitet, die erstmals im Dezember 2016 in überregionalen Medien, im Netz und einem Ausschuss des Europäischen Parlaments vorgestellt wurde.[103]

Die Initiatoren beschreiben ihre Motivation und den **Zweck des Projekts** wie folgt:

> [E]ine solch mächtige Technologie [lässt] ganz neue Möglichkeiten der Eingrenzung, Überwachung, Verfolgung und Kontrolle zu. Wurde Anfang der 2010er der „Arabische Frühling" noch ad hoc als „Facebookrevolution" gefeiert, so folgten nur kurze Zeit später erste Nachrichten, wie sich repressive Regime ihrerseits sozialer Medien bedienten, um Dissidenten aufzuspüren oder ihre Bevölkerung mit sozialen Kreditpunkten als gute oder schlechte Bürger zu bewerten. Spätestens seit den Snowden-Enthüllungen ist also klar, was Kritiker wie der verstorbene FAZ-Herausgeber Frank Schirrmacher schon lange anmahnten: Das Netz hat seine Unschuld verloren und die Gefahr eines „technologischen Totalitarismus" ist real.
>
> Vor diesem Hintergrund ist die Initiative einer digitalen Grundrechtecharta zu verstehen. Ziel des Entwurfs ist es, auf europäischen Werten fußend einen Rahmen von Grundregeln zu formulieren, der Politik, Wirtschaft und Individuen eine Orientierung bieten soll, wie eine offene, liberale und menschenwürdige Gesellschaft im digitalen Zeitalter garantiert werden kann. Es geht den Initiatoren darum, den rasanten Fortschritt zu humanisieren, damit er sein Potenzial zum Wohl der Gesellschaft entfalten kann und bestehende Freiheiten zu verteidigen, die unserem rechtsstaatlichen Verständnis entsprechen. [104]

Der **Inhalt der Charta** wird so zusammengefasst:

> In 23 Artikeln unterbreitet der Charta-Entwurf Vorschläge zur Autonomie und Freiheit des Einzelnen, zum Einsatz und zur maßvollen Entwicklung künstlicher Intelligenz, zu informationeller Selbstbestimmung und Datensicherheit und zum Umgang mit Hetze und Hass im Netz.
>
> Gleich im zweiten Artikel wird unterstrichen, was niemals zur Disposition gestellt werden darf: „Jeder Mensch hat ein Recht auf freie Information und Kommunikation." Artikel 5 verteidigt die

---

102 Verfügbar unter https://digitalcharta.eu/.

103 Internetauftritt der Initiative, verfügbar unter https://www.internet-freiheit.de/grundrechte-im-digitalen-zeitalter-verteidigen/.

104 Ebd.

> Meinungsfreiheit aller Bürger im Netz gegen Zensur. Er macht aber gleichzeitig darauf aufmerksam, dass die Meinungsfreiheit seine Grenzen dort finden muss, wo der Ruf oder die Unversehrtheit anderer Menschen ernsthaft gefährdet werden – etwa durch andauernde Hetze oder Cybermobbing. Weitere Artikel widmen sich der möglichen Einschränkung unserer Freiheit durch (diskriminierende) Auswertung unserer Daten, durch Massenüberwachung, Profiling etc. [105]

Der Entwurf dieser Charta hat seitdem eine öffentliche **Diskussion** darüber entfacht, wie die Menschenrechte auch im digitalen Zeitalter wirksam geschützt werden können, welche Freiheiten und welche Grenzen bestehen sollten;

> Bereits kurz nach der Veröffentlichung hagelte es insbesondere im Netz Kritik am Vorhaben an sich und an einzelnen Formulierungen. Die Kommentarspalten füllten sich ebenso schnell wie die Liste von Menschen, die die Charta mitunterzeichneten. Beides war im Sinne der Initiatoren: Eine kontroverse öffentliche Diskussion über die Charta und ihre inhaltlichen Aussagen sowie eine breite Unterstützung für das Anliegen selbst zu erwirken. In den folgenden Monaten seit der Veröffentlichung im Dezember 2016 wurde viel diskutiert: in klassischen Medien, im Netz, auf Podiumsdiskussionen und auf der re:publica in Berlin.
>
> Besonders heftig kritisiert wurde dabei beispielsweise der erwähnte Artikel 5 zur Meinungsfreiheit. Wenn digitale Hetze und Mobbing im Netz „zu verhindern“ seien (so steht es im zweiten Absatz), dann bedeute das doch eine Art Zensur in sozialen Medien und Blogs, gar eine „Schwarze Liste“ von Begriffen oder Redewendungen, die zur sofortigen Löschung führten. Wer bestimmt diese Liste? Wer würde löschen? Der Staat? Internetkonzerne?
>
> „Die lebhafte Kritik folgt vor allem aus einem Widerspruch, der nicht nur in diesem Artikel sichtbar ist, sondern in der Natur der Sache liegt. Einerseits ist jeder Bürger daran interessiert, die Meinungsfreiheit im Internet bestmöglich zu wahren und zu schützen. Andererseits hat sich gerade in jüngster Zeit die Erkenntnis herausgebildet, dass eben diese Meinungsfreiheit nicht selten missbraucht wird, volksverhetzend, beleidigend, im negativen Sinne mobilisierend,“ schrieb daraufhin die Schriftstellerin und Mitinitiatorin Juli Zeh gegenüber den Kritikern.
>
> Ein zweiter wichtiger Aspekt, den die Charta thematisiert, ist die Machtverschiebung hin zu großen Digitalunternehmen und deren Plattformen. Sie birgt nicht nur Risiken für fairen Wettbewerb, sondern auch für den Schutz von Bürgerrechten. Daher verfolgt die Charta den – sicherlich sehr kontroversen – Ansatz, Grundrechte künftig auch gegenüber privaten Firmen durchzusetzen, wenn sie de facto eine ähnliche gesellschaftliche Funktion ausüben wie staatliche Stellen. Welche Relevanz die Diskussion solcher Ansätze aber hat, zeigt der Fall um den Missbrauch von Facebook-Userdaten, bei dem deutlich wird, dass selbst bestehende Datenschutzgesetze dem Bürger heute keinen effektiven Schutz ihrer Daten und Rechte bieten. [106]

105 Ebd.

106 Ebd.

6. Vertiefende Literatur

- Graf von Westphalen*, Digitale Charta: Erweiterung der europäischen Grundrechte für das digitale Zeitalter*, Betriebs-Berater (Zeitschrift für Recht, Steuern und Wirtschaft), 73 (2018), 899-907

- Gunnarsson (Hrsg.), *Recht auf Privatheit im digitalen Zeitalter* (2017)
  - Rössler, *Wie wir uns regieren. Soziale Dimension des Privaten in der Post-Snowden-Ära*, 9-30
  - Weiß, *Die internationalen Debatten über das Recht auf Privatheit im digitalen Zeitalter: Anmerkungen zu den Grundlagen und Inhalten*, 31-44
  - Schiedmair, *Das Recht auf Privatheit in der deutschen und internationalen Rechtsordnung,* 45-56
  - Daniels, *Über die Grenzen des Rechts auf Privatheit und die Rolle der Literatur*, 57-71

- Bull, *Digitale Grundrechte für Europa: eine rechtspolitische Initiative zur Einhegung des Internets: symbolische Politik oder effektive Rechtsetzung?*, Recht und Politik (Zeitschrift für deutsche und europäische Rechtspolitik), 53 (2017), 9-25

- Zeitschrift für Menschenrechte, Jahrgang 10 (2016), Heft 1, *Menschenrechte digital:*
  - Thiel, *Anonymität und der digitale Strukturwandel der Öffentlichkeit*, 7-23
  - Kettemann, *Menschenrechte im Multistakeholder-Zeitalter: Mehr Demokratie für das Internet*, 24-37
  - Wagner, *Kommunikation konstituiert Gesellschaft: Warum es Zeit ist, den Zugang zum freien Internet als Menschenrecht anzuerkennen,* 38-43
  - Mihr, *Ein Cyber-Gesellschaftsvertrag für die Menschenrechte*, 44-59

- Helbing u.a., *Digitale Demokratie statt Datendiktatur*, Spektrum der Wissenschaft, 1/2016, 51-58

- *Das Digital-Manifest: Expertenkommentare,* Spektrum der Wissenschaft, 3/2016, 18-19

- Schaar*, Globale Überwachung und digitale Souveränität*, Zeitschrift für Außen- und Sicherheitspolitik, 8 (2015), 447-459

***