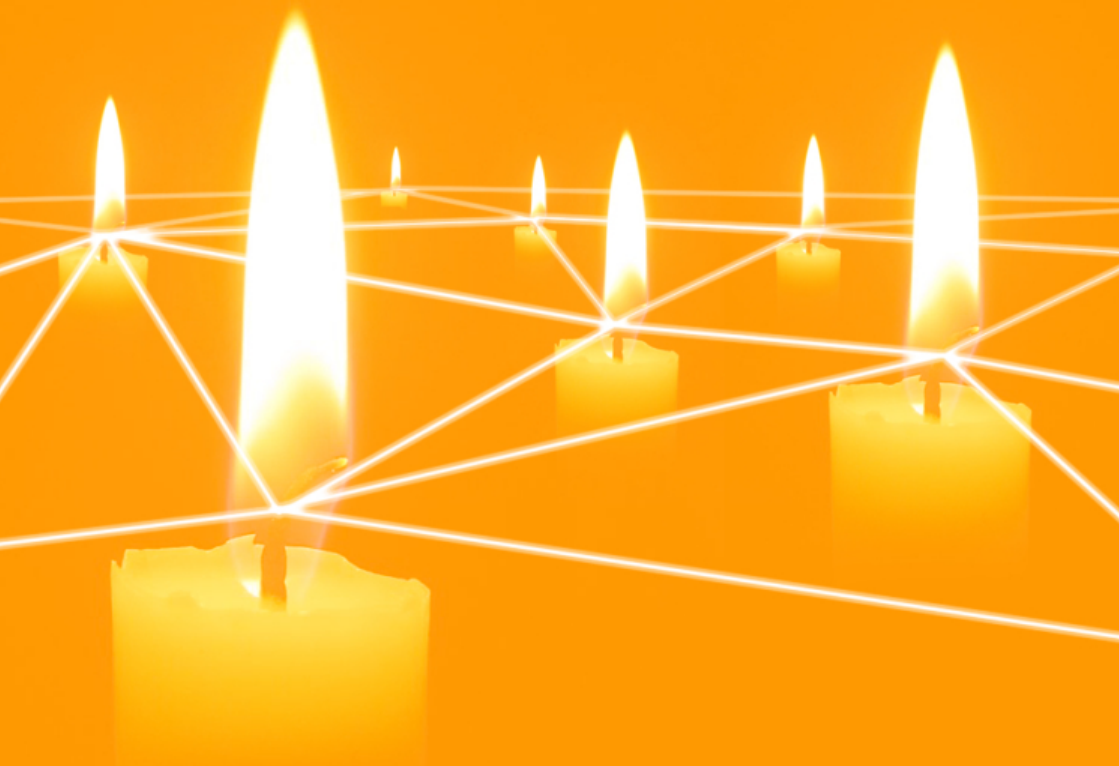
MENSCHENRECHTE IM DIGITALEN ZEITALTER

AMNESTY INTERNATIONAL



In dieser Broschüre befinden sich Diskussionsbeiträge einiger Mitglieder der Themenkoordinationsgruppe Menschenrechte im Digitalen Zeitalter von Amnesty International Deutschland. Sie sind von den Autoren erstellt, um zur Positionierung von Amnesty International beizutragen, und geben nicht notwendigerweise die Meinung der Gesamtorganisation wieder.

V.i.S.d.P.: Sebastian Schweda
Titelbild: ©Amnesty International,
Hintergrundbild Rückseite: ©Cory Doctorow, CC-BY-SA
2. Auflage, März 2014

INHALT

MENSCHENRECHTE IM DIGITALEN ZEITALTER

WARUM AMNESTY INTERNATIONAL SICH MIT DIGITALEN INFORMATIONS- UND KOMMUNIKATIONSTECHNOLOGIEN BESCHÄFTIGT

„Technologie ist weder grundsätzlich gut noch schlecht für die Menschenrechte. Sie ist ein Werkzeug, das beide Seiten benutzen, sowohl diejenigen, die Ungerechtigkeiten überall auf der Welt anprangern wollen, als auch diejenigen, die den Zugang zu Informationen kontrollieren und kritische Stimmen unterdrücken wollen."

Salil Shetty, Generalsekretär Amnesty International,
im Amnesty Report 2011

Für den Schutz der Menschenrechte haben digitale Technologien erhebliche Chancen eröffnet: Der „Arabische Frühling" wäre in dieser Dynamik kaum denkbar gewesen ohne die Nutzung moderner Informations- und Kommunikationsmittel. Die Inhalte vertraulicher Dokumente, mit denen Menschenrechtsverletzungen von Staaten erstmals belegt werden konnten und von denen die von Chelsea Manning und Edward Snowden geleakten nur die aufsehenerregendsten waren, hätten ohne die Möglichkeiten zur weltumspannenden Kommunikation im Internet – sei es über Whistleblower-Plattformen oder durch investigativ-journalistische Berichterstattung – nicht dieselbe Aufmerksamkeit und Verbreitung gefunden. Zahlreiche Projekte vernetzen Menschenrechtsaktivisten mittlerweile über Blogs, soziale Netzwerke, SMS-Dienste oder Smartphone-Apps. Sie ermöglichen es ihnen, sich über ihre Arbeit auszutauschen und sich vor Übergriffen wirksamer zu schützen. Auch Amnesty unterstützt einige davon (etwa das 2012 vorgestellte Pilotprojekt „Panic Button").

Gleichzeitig verwenden aber auch Regierungen diese Technologien, um Menschen zu überwachen, ausfindig zu machen, zu verhaften oder sogar zu töten. In vielen Fällen geht es dabei um Personen, die lediglich von ihren Menschenrechten Gebrauch gemacht haben. Staaten nutzen – in unterschiedlicher Intensität und mit unterschiedlicher Zielsetzung – ihre Möglichkeiten, um ihnen nicht genehme Meinungen oder Aktivitäten zu unterdrücken. Sie lassen Kommunikationsvorgänge ohne konkreten Anlass überwachen und untergraben damit die Anonymität der Kommunikation und die Privatsphäre der Menschen – wie die Mitgliedstaaten der EU, die die (mitt-

lerweile vom Europäischen Gerichtshof für ungültig erklärte) Richtlinie zur Vorratsdatenspeicherung umgesetzt haben. Sie sperren bestimmte Dienste und Inhalte im Internet und dringen in private E-Mail-Konten ein – wie der Iran, der einst ein nationales, nach außen abgeschottetes „Halal"-Internet mit Identifikationspflicht anstrebte. Sie zensieren Meinungsäußerungen anhand von gigantischen Wortfiltern – wie China, dessen „Great Firewall" ein Musterbeispiel für staatliche Versuche zur Lenkung der öffentlichen Meinung ist. Die Regierungen einiger Länder – etwa Ägyptens oder Syriens – haben gar die Abschaltung von Kommunikationsnetzen angeordnet in Zeiten, in denen sie ihren Machterhalt durch die öffentlichen Proteste gefährdet sahen.

Die Enthüllungen über die Spähaktivitäten von NSA, GCHQ und anderen westlichen Geheimdiensten schließlich sprengen alle bisher öffentlich bekannt gewordenen Dimensionen weltweiter Kommunikationsüberwachungsmaßnahmen. Sie stellen eine massive Verletzung des Rechts auf Privatleben nahezu jedes Menschen dar und haben zu einer intensiven internationalen Debatte über den Schutz dieses Menschenrechts im digitalen Zeitalter geführt. Gleichzeitig sehen sich Whistleblower, die vertrauliche Dokumente veröffentlichen, aus denen sich Menschenrechtsverletzungen ergeben, strenger Verfolgung durch staatliche Behörden ausgesetzt. Am 21. August 2013 wurde Chelsea Manning von einem US-Miltärgericht zu einer Freiheitsstrafe von 35 Jahren verurteilt. Auch auf Edward Snowden und die Menschen, die ihm bei der Veröffentlichung seiner Dokumente halfen, wurde hoher politischer Druck ausgeübt.

Unterdessen wurden durch Aussagen wie die des ehemaligen US-Drohnenpiloten Brendon Bryant frühere Recherchen bestätigt, dass auch extralegale Hinrichtungen durch Drohnen in Ländern wie Pakistan, Somalia oder dem Jemen mit Hilfe der Echtzeitanalyse von Daten aus den NSA-Überwachungsprogrammen durchgeführt werden – trotz der bekannten Trefferungenauigkeit dieser Daten. Zunehmend verfestigt sich der Eindruck, dass es nicht nur Staaten mit seit langem bekannter extensiver Überwachungs-, Filter- und Zensurtradition wie Russland, China, Iran oder Saudi-Arabien sind, die den Menschenrechten im digitalen Raum nur geringen Wert beimessen.

Die Staaten müssen die Menschenrechte aber nicht nur selbst achten (sog. Abwehrdimension der Menschenrechte), sondern sie auch vor Verletzungen durch andere Staaten oder Private, die in ihrem Einflussbereich operieren, schützen (Schutzpflichtdimension). Der NSA-Untersuchungsausschuss des deutschen Bundestages soll deshalb unter anderem auch die Rolle von Bundesregierung und deutschen Nachrichtendiensten bei den weltweiten Massenüberwachungsprogrammen der „Five Eyes"-Staaten klären. Dabei wird auch der Frage nachzugehen sein, welche Schutzpflichten Deutschland gegenüber den Menschen in seinem eigenen Einflussbereich hat und ob diese in der Vergangenheit ausreichend erfüllt wurden.

Aus dem Bereich der nichtstaatlichen Akteure ist das US-Unternehmen Yahoo! in unrühmlicher Erinnerung geblieben: Der Internetkonzern unterstützte 2005 die chinesischen Behörden durch die Weitergabe von E-Mail-Nutzerda-

ten des Journalisten Shi Tao, die zu seiner Identifizierung und Verurteilung zu einer zehnjährigen Haftstrafe wegen des Versands einer E-Mail führten. Unter anderem durch die Aufdeckung des geheimen Programms PRISM wurde 2013 schließlich bekannt, dass neben Yahoo! auch andere große Internetunternehmen wie Google, Facebook, Apple oder Microsoft an der massenhaften Weitergabe von Nutzerdaten an den US-amerikanischen Geheimdienst NSA beteiligt sind. Unternehmen wie die deutsche Gamma International GmbH oder die italienische Hacking Team S.r.l. wiederum lieferten Überwachungs- oder Filtersoftware an repressive Regime wie Bahrain.

An diesen Beispielen werden die ambivalenten Folgen der Digitalisierung für die Menschenrechte sichtbar: Während moderne Informations- und Kommunikationstechnologien dem Einzelnen neue Chancen zur Wahrnehmung seiner Rechte eröffnen, geben sie Regierungen auch neue Instrumente an die Hand, diese Aktivitäten wirksam zu unterbinden, zu behindern oder zu kontrollieren. Die gegenwärtigen Entwicklungen zeigen, dass exzessive staatliche Eingriffe in diesem Umfeld die Menschenrechte – allen voran der Rechte auf freie Meinungsäußerung, auf freien Informationszugang und auf den Schutz des Privatlebens – zunehmend gefährden. Regierungen überall auf der Welt scheinen gegenwärtig darauf hinzuwirken, die Erleichterungen, die moderne Informations- und Kommunikationstechnologien für die Wahrnehmung der Menschenrechte gebracht haben, unter dem Vorwand entgegenstehender Interessen wie der nationalen Sicherheit zu einem erheblichen Teil wieder zu beseitigen oder deutlich einzuschränken.

Um die Auswirkungen der immer schneller ablaufenden technologischen Prozesse auf die Verwirklichung der Menschenrechte aufmerksam im Blick zu behalten und eine strategische Positionierung von Amnesty International vorzubereiten, hat die deutsche Sektion seit 2012 Kapazitäten zu diesem Themenbereich aufgebaut. Seit 2014 besteht mit der Themenkoordinationsgruppe Menschenrechte im digitalen Zeitalter ein ehrenamtliches Expertengremium, das die aktuellen Entwicklungen im Umfeld digitaler Informations- und Kommunikationstechnologien kontinuierlich beobachtet, aus menschenrechtlicher Sicht einordnet und innerhalb der Sektion als „Kompetenzzentrum“ für Menschenrechte in der digitalen Gesellschaft zur Verfügung steht. Die Koordinationsgruppe beteiligt sich an den strategischen Entwicklungen in der internationalen Bewegung, bereitet Kampagnen und Aktionen vor und schult die Mitgliedschaft durch interne Trainings- und Fortbildungsseminare. Nach außen vertreten wir unsere Forderungen auf öffentlichen Veranstaltungen sowie durch gezielte Lobby- und Pressearbeit. Zudem erstellen wir Materialien und bieten Unterrichtsheiten für die themenbezogene Menschenrechtsbildung an. Schließlich stehen wir als Ansprechpartner für Opfer von Menschenrechtsverletzungen im Umfeld digitaler Technologien zur Verfügung.

Sebastian Schweda
Sprecher der Themenkoordinationsgruppe
Menschenrechte im Digitalen Zeitalter (TheKo Digital)
schweda@amnesty-digital.de
PGP: 492F CF12 B7DD B3D3 C603 A0C9 7514 DA29 CBAE F03C

DATENSCHUTZ UND ANONYMITÄT IM DIGITALEN

WAS HABEN DATENSCHUTZ UND ANONYMITÄT MIT FREIHEIT UND MENSCHENRECHTEN ZU TUN?

EINLEITUNG

Wer sich mit Menschenrechten in der digitalen Welt beschäftigt, sollte immer auch die wahrscheinliche zukünftige Entwicklung der Informationsverarbeitung im Blick behalten. Speziell in diesem Bereich können bereits jetzt perspektivisch großflächige und schwere menschenrechtliche Probleme ausgemacht werden, auch wenn sich diese bislang eher auf das Privatleben und die Meinungsfreiheit des Einzelnen beziehen. Dass der Einfluss der Digitalisierung jedoch noch viel tiefer geht, soll der folgende Text beleuchten.

DIGITALE ASKESE?

Angenommen, eine fiktive Person möchte sich nicht den Problemen der digitalen Welt aussetzen und verzichtet gänzlich auf die Nutzung des Internets und von Computern allgemein. Auch wenn es mühevoll ist, schreibt sie Briefe, telefoniert traditionell, lässt den Steuerberater die Einkommenssteuererklärung machen, bestellt postalisch aus Katalogen und nutzt nur Überweisungsträger für Bankgeschäfte.

Dennoch fallen sehr viele digitale personenbezogene Daten an, vor allem weil fast alle mittleren und größeren Organisationen (Firmen/staatliche Stellen etc.) mittlerweile digitale Datenverarbeitung betreiben und auch mit anderen Organisationen zunehmend digital Daten über das Internet austauschen.

So liegen die Steuerdaten digital vor und werden auch digital übermittelt. Meldeämter und Versandhäuser verarbeiten die Adressdaten in digitaler Form; das Telekommmunikationsverhalten – und somit ein aussagekräftiger Ausschnitt der Interaktion mit dem sozialen Umfeld – wird mindestens beim Telefonanbieter in digitaler Form aufgezeichnet; Briefempfänger und -absender werden für die Auslieferung digital erfasst und auch gespeichert. Das Gesicht der Person ist auf digitalen Gruppenfotos von Freunden und in unzähligen Videoüberwachungssystemen der Stadt, das Kennzeichen ihres Kraftfahrzeugs in den Systemen der Mautbetreiber, ihre Bonitätsdaten mindestens bei den Banken, meist aber auch bei Scoringagenturen wie der SCHUFA und ein Teil ihres Einkaufsverhaltens liegt bei ihrem Kreditkartenanbieter.

KEIN ENTKOMMEN

All dies geschieht völlig unabhängig davon, ob sich der einzelne Mensch für die persönliche Internetnutzung entscheidet – und damit vielleicht die Verarbeitung der dabei anfallenden Nutzungs- und Kommunikationsdaten akzeptiert. Die Erstellung detaillierter Personenprofile und Handlungsprognosen ist – auch außerhalb dieses begrenzt vom Betroffenen steuerbaren Bereichs – schon lange keine Zukunftsmusik mehr. Unter dem nebulösen Schlagwort „Big Data“ beginnen öffentliche wie private Stellen großflächig, diese Daten zu nutzen. Die negativen Folgen für Journalisten- und Informantenschutz, das Berufsgeheimnis von Anwälten, Ärzten und Hilfestellen allgemein sind bekannt, doch mit diesen Daten sind eben auch politische Gesinnung, sexuelle Präferenzen, allgemeiner Lebensstil, sozialer Umgang, Bildungsgrad, Vernetzung und potenzielle Straffälligkeit des Individuums berechenbar – zumindest vermeintlich. Kreditvergabebedingungen, Versicherungsbeiträge und Einreiseverbote sind direkte Folgen, generell beeinflussbares Verhalten jedoch dieindirekteKonsequenz. Die personalisierte Obama-Kampagne der letzten Wahlen in den USA einerseits, personalisierte Werbung und sonstige individualisierte Angebote andererseits verdeutlichen dies. Derartige Entwicklungen betreffen also den Kern der individuell-persönlichen Handlungs- und Entscheidungsfreiheit, von denen die Rechte auf Privatleben und Meinungsfreiheit nur ein Teil sind.

DATENSCHUTZ UND DIE SUMME DER TEILE

Die Menschenrechtsrelevanz jedes einzelnen der oben beschriebenen Datenverarbeitungsvorgänge mag diskutabel erscheinen und im konkreten Fall gering sein. Zusammengenommen, ergibt sich aus der Vielzahl der Vorgänge – basierend auf den digitalen Verarbeitungsmöglichkeiten – ein fundamentaler qualitativer Unterschied zu herkömmlichen nicht automatisierten Datenverarbeitungen: Digitale Datenbestände können verlustlos kopiert, aber auch beliebig verkettet, neu kombiniert und korreliert werden und erzeugen im Zusammenhang immenses Zusatzwissen über die einzelne Person, Personengruppen und ganze Gesellschaften. Dabei ist diese Zusammenführung auch heute schon gang und gäbe: Die legale Datenweitergabe durch Meldeämter und andere, kommerzielle Datenhändler, Unternehmensübernahmen, Kooperationen, Outsourcing und Insolvenzen haben eine kontinuierliche und massibe Verschiebung von Datenbeständen zur Folge. An dieser Stelle setzt der Datenschutz an, denn in einer digitalen Welt fallen derartige Daten oft zuhauf an, doch die Gesellschaft muss dafür sorgen, dass z. B. so wenig wie möglich erhoben, die vorhandenen nicht verkettet und alles nach Zweckerfüllung auch wieder gelöscht wird, weil sonst der gläserne – und somit manipulierbare – Mensch entsteht.

DIE DIGITALE WURZEL

Die oben skizzierten Konsequenzen basieren darauf, dass digitale Systeme stets ihre eigenen Arbeitsschritte protokollieren. Das hat teilweise technische, aber auch rechtliche, organisatorische oder immer ofter kommerzielle Gründe. Werden keine anderweitigen Vorkehrungen getroffen, schlägt diese „Spurenerzeugung“ nach oben durch bis zu den mittels digitaler Systeme vollzogenen, menschlichen Handlungen. Um diese

Eigenschaft zu verdeutlichen, kann man sich als analoges Gegenbeispiel den Kauf eines Brotes mit Bargeld beim Bäcker vorstellen. Weder weiß das Personal, wer man ist, noch bleiben dauerhafte personenbezogene Spuren des Kaufes zurück. In der digitalen Welt – das bezieht sich auch auf Käufe mit z. B. Kreditkarten – werden üblicherweise alle bekannten Eigenschaften des Käufers gesammelt und mit vorhandenen Daten in Zusammenhang gebracht. Daraus werden Profile generiert und verwendet oder verkauft. Gleiches gilt für jegliche digitale Interaktionen im kommerziellen Bereich, sei es in sozialen Netzwerken, Kurznachrichtendiensten oder „kostenlosen" Emaildiensten, denn die Überwachung der Nutzer ist das Hauptgeschäftsmodell des Internets und die Digitalisierung aller Lebensbereiche macht das erst effektiv möglich.

GESELLSCHAFTLICHE EFFEKTE UND MENSCHENRECHTE

Da mehr und mehr Handlungen, Wahrnehmungen und Interaktionen digital veräußert vorliegen, kann darauf auch von dritten Einfluss genommen werden. Sowohl individuell also auch systematisch – von staatlicher Seite als auch von privaten Unternehmen. Je mehr Behörden, Organisationen oder Firmen über einen Menschen wissen und je mehr sie Zugriff auf das digitale Umfeld haben oder es sogar kontrollieren, umso mehr Macht erlangen sie über den Menschen. Die Einflussmöglichkeiten reichen dabei von der Präsentation personalisierter Werbung bis hin zu Manipulationen von Wahrnehmung und Handlung der Betroffenen. So hat der Betreiber eines großen sozialen Netzwerks damit experimentiert, inwieweit sich das Verhalten der Nutzer ändert, wenn speziell ausgewählte Nachrichten von Freunden vermehrt präsentiert oder vorenthalten werden; das alles fand ohne vorherige Einwilligung der Nutzer statt, aber ganz im Sinne des Unternehmens, denn wer froh ist konsumiert mehr. Und auch staatliche Akteure bedienen sich dieses Datenpools und vergrößern ihn auch aktiv z. B. durchgesetzliche „Vorratsdatenspeicherungen" oder sonstige anlasslose Überwachungbestrebungen aller Art (von Fluggast- über Videoüberwachungs- bis hin zu Telekommunikationsdaten).

Zusätzlich kommen die gesellschaftlichen Effekte vernetzter Systeme zum Tragen. Die Wahl des Kommunikationsanbieters oder des Speicherortes der digitalen Habseligkeiten betrifft immer auch andere Menschen, sogar ganz wesentlich. Betroffen sind meist so viele Menschen – z. B. alle Kommunikationspartner, dass es schwerfällt, überhaupt noch individuelle Freiheits- und Entscheidungsräume zu definieren, in denen der Einzelne tatsächlich datenseitig selbstbestimmt agieren kann. Immer mehr strukturiert die kommerziell getriebenen Spielart der Digitalisierung alle Lebensbereiche – von der individuell angepassten und dauerhaft auf Einhaltung überwachten Auto- und Krankenversicherung bis hin zu datenbasiertenAnalysen ganzer Nutzergruppen. Einer im Vorhinein stattfindenden Be- und Auswertung errechneter Handlungsprognosen wird somit Vorschub geleistet. Die präventiven Verhaltensänderungen derartig überwachter Menschen zeichnen sich schon jetzt ab, sei es am Telefon, auf der Straße oder insgesamt im privaten und politischen Handeln; die vernetzte Gesellschaft muss folglich unbedingt menschenrechtsorientiert gestaltet werden, um elementare

Freiheitsrechte zu erhalten.

Diese Konsequenzen der massenhaften Anhäufung riesiger Datenmengen über Menschen und ganze Gesellschaften müssen dringend thematisiert sowie die Ursachen freigelegt und entsprechend bearbeitet werden. Der Handel mit personenbezogenen Daten und generell Geschäftsmodelle, die auf der kommerziellen Verwertung solcher Daten basieren, müssen vor dem Hintergrund der schleichenden, gesamtgesellschaftlichen Verdatung grundlegend auf ihre systematische Menschenrechtsrelevanz hin analysiert und kritisch hinterfragt werden. Datenschutz und insbesondere Anonymität werden dabei eine ganz wesentliche Rolle spielen müssen; Datenschutz als Wirkbegrenzung vorhandener Daten und der Spezialfall Anonymität als vorgeschaltete Nichterzeugung personenbezogener Daten.

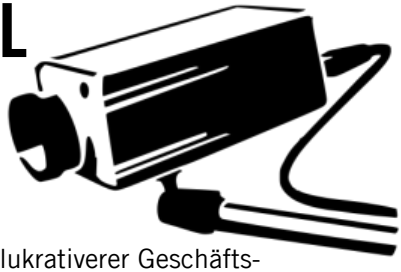
ZUM ABSCHLUSS NACH VORN GEDACHT

Akute Probleme wie die globale Überwachung durch Geheimdienste sind natürlich prioritär anzugehen. Die oben beschriebenen Entwicklungen – von denen der Überwachungsskandal nur eine bestimmte Erscheinungsform darstellt – müssen darüber hinaus aber auch langfristig im Auge behalten werden. Die „Freiheit des Menschen“ wird nochmals diskutiert werden müssen, wenn immer mehr Menschen mit vernetzten Kamerabrillen/-kontaktlinsen à la Google Glass umherlaufen, „smarte“ Fernseher die Zimmergespräche übermitteln oder jegliche Videoüberwachung mit Gesichtserkennung ausgestattet wird – wie schon 2006/2007 im Mainzer Hauptbahnhof vom Bundeskriminalamt getestet – oder wenn das eigene Auto stehenbleibt, weil die entsprechende Funktion neuerdings nicht nur – wie in den AGBs eingewilligt – von der eigenen Werkstatt, sondern auch von staatlichen Behörden oder Versicherungen verwendet wird.

Amnesty International muss die Entwicklungen im Bereich der Digitalisierung im gesellschaftlich-politischen Gesamtkontext betrachten, um den Bedrohungen für die Menschenrechte im digitalen Zeitalter fundiert entgegentreten und eine positive Entwicklung dieser Welt mitgestalten zu können.

Rainer Rehak
rainer.rehak@amnesty-digital.de
PGP: 0D66 63E5 70A3 964A EE60 D927 4427 CFE5 8C19 AE19

ÜBERWACHUNG DIGITAL



EIN (KURZER) ÜBERBLICK

DATENERHEBUNG

Aufgrund des Aufkommens immer mehr und immer lukrativerer Geschäftsmodelle, die auf der Verwertung und dem Verkauf von Daten basieren, wird zunehmend jeder Klick im Internet, jeder Webseitenaufruf maschinell weiterverarbeitet oder sogar gespeichert. Dies geht so weit, dass mittlerweile in einige Online-Formularfelder eingegebene, aber nicht explizit „verschickte" Texte gespeichert werden. Diese Daten werden meist nicht nur von den Webseitenbetreibern verarbeitet und weitergereicht, sondern oft von sozialen Medien oder sogenannten Data Brokern zusammengeführt. So werden durch die sogenannten „Social Media Buttons" oder „Analytic"-Dienste IP-Adresse und oftmals weitere Informationen über den/die Nutzer/in oft schon beim alleinigen Aufruf der Webseite übertragen. Ein möglicher Vergleich hierfür wäre, dass bei einem Stadtrundgang alle „Blicke" registriert und weitergeleitet werden, d. h. welches Produkt man sich in einem Geschäft genauer anschaut, welchen Kaffee man trinkt oder wann man sich im Café auf den Abort begibt. Wenn diese Daten, die bei einigen Unternehmen auch Nutzerprofile in sozialen Medien beinhalten, nun zusammengeführt werden, so kann ein Profil über Nutzer/innen angelegt werden, das laut Aussage der meisten Firmen von diesen selbst für Werbung genutzt wird.

In diese Profile fließen häufig nicht nur Webseitenaufrufe oder Informationen aus sozialen Medien ein, sondern auch im Alltag erhobene Daten, zum Beispiel über Smartphones. Durch die ständige Internetanbindung des Telefons und seine immer ausgefeilteren Funktionen lassen sich Standort, Akkuladung, gespeicherte Kontaktdaten oder Kurznachrichtentexte ohne weiteres erheben, wenn dem genutzten Programm die Rechte eingeräumt werden. Allerdings bieten als weiterführendes Beispiel auch Firmen die Identifikation von Kunden, die per Karte zahlen, an, wenn sie an der Kasse nach ihrer Postleitzahl gefragt werden. Außerdem gibt es Bestrebungen, Ladenkäufe mit Onlineprofilen zu verknüpfen[1], unabhängig von der Nutzung einer Kundenkarte. Durch das immer stärker aufkommende „Internet der Dinge" wird der Trend zu einem vollständigen Profil bestärkt, und auch Personen, die nicht „im Internet" aktiv sind, können sich diesem nicht entziehen.

Wie die Daten verarbeitet und gespeichert werden, was rechtlich möglich oder nicht möglich ist, wird in einem anderen Beitrag genauer besprochen.

GEHEIMDIENSTLICHE UND POLIZEILICHE ÜBERWACHUNG

Daten und gebildete Profile werden von Unternehmen nicht nur zur eigenen Werbung verwendet, sondern auch als Verkaufsgegenstand wahrgenommen. Dies beginnt beim einfachen Adresshandel für Kundengewinnung[2] und er-

streckt sich bis zum Anbieten von Dienstleistungen für Militär und Geheimdienste[3]. Hier wird ersichtlich, dass der private Sektor, sobald er hinreichend unreguliert ist, sogar teilweise unverdeckt als Datenerhebungsdienstleister und Analyst für staatliche Stellen fungieren kann. Diese Feststellung ist nicht auf Autokratien beschränkt. Es ergibt sich aus dem Fundus der Snowden-Enthüllungen, dass private Unternehmen verdeckt zu Kooperationen gezwungen werden[4] und Geheimdienste Daten tauschen oder weiterleiten[5]. Zusätzlich zu den Möglichkeiten, die private Unternehmen zur Datenerhebung haben, hat sich gezeigt, dass staatliche Stellen weitere Zugriffsmöglichkeiten haben.

Neben der bewussten Weitergabe von Daten durch private Unternehmen ist öffentlich geworden, dass der amerikanische Geheimdienst NSA in die Datenzentren von Google und Yahoo! eingedrungen ist. Über sogenannte Apps hat(te) die NSA Zugriff auf Adressbücher, Ort und Anrufhistorie vieler Smartphones[6]. In einem Snowden-Dokument ist die Rede von der Erhebung von ungefähr 250 Millionen Adressbüchern pro Jahr. Außerdem verfügt die NSA über die Möglichkeit, infrastrukturbedingt erhobene Daten wie SMS[7] oder Standorte von Mobiltelefonen[8] zu erhalten und auszuwerten. Auch der Zugriff auf Kommunikationsinfrastruktur wird sich aktiv und teilweise ohne Einwilligung der entsprechenden Firma verschafft[9]. Zusammenfassend kann gesagt werden, dass eine umfassende, flächendeckende Datensammlung entstanden ist.

Neben den von Edward Snowden enthüllten Überwachungsaktivitäten der Staatenallianz „Five Eyes“ (USA, Großbritannien, Neuseeland, Kanada, Australien) wird von weiteren Ländern die Aktivität von Internetteilnehmer/innen überwacht, jedoch meist lokal. Dies umfasst allein schon aufgrund der technischen Notwendigkeit[10] alle Länder, in denen bestimmte Dienste gesperrt werden oder auf Inhalten basierende Zensur stattfindet. Beispiele hierfür sind China, Bahrain, Äthiopien oder Iran. Zum Beispiel forderte 2012 die chinesische Regierung in China ansässige Firmen auf, technische Vorkehrungen für das Blockieren bestimmter Inhalte zu treffen. Zudem wurde öffentlichkeitswirksam ein Klarnamenzwang für das Internet bzw. für den Internetzugang gefordert. Außerdem wird der Internetverkehr auf kritische Stichworte untersucht.

DATENNUTZUNG

Diese Datensammlungen gehen weit über das hinaus, was aktuell wissenschaftlich untersucht wird. Verschiedene Studien haben gezeigt, dass es allein aufgrund der von verschiedenen Politiker/innen als harmlos dargestellten Metadaten möglich war, Personen vergleichsweise gut im sogenannten „Big Five“-Charaktermodell einzuordnen[11,12]. Im Zuge dessen, dass alleine Metadatenanalyse eine vergleichsweise hohe Genauigkeit aufweiste, erscheint eine präzise Charakteranalyse durch Anreicherung mit den anderen, weit umfassenderen Datensätzen möglich. Wo früher die Observierung von Personen sich aus Kostengründen auf Verdächtige beschränkt hat, bietet die Digitalisierung die Möglichkeit einer flächendeckenden Überwachung von Unschuldigen und Unverdächtigen, die dann aufgrund von unbekannten Al-


Hauptquartier der NSA in Fort Meade, Maryland. Foto: Trevor Paglen, CC0

gorithmen seitens Geheimdiensten oder der Polizei als „Verdächtige“ ausgemacht werden.

Die oben beschriebenen Methoden zur Überwachung ermöglichen Menschenrechtsverletzungen gefolgt auf z.B. die Aufklärung der sexuellen Identität, der Religionszugehörigkeit, der politischen Ansichten und anderer Eigenschaften.

Zusätzlich ermöglichen statistische Methoden die Ergänzung durch wahrscheinliche Eigenschaften jeder einzelnen Person. Solche „wahrscheinlichen“ Informationen können in einem autoritären Präventionsstaat genutzt werden, um aktuelle und zukünftige vermeintliche Oppositionelle oder Menschenrechtsverteidiger/innen zu identifizieren und einzuschüchtern, „verschwinden zu lassen“ oder Zensurmaßnahmen vorzubereiten.

AUCH IM DISZIPLINARSTAAT

Aber selbst in einem „idealen“ menschenrechtsschützenden Staat wiegt das Risiko für das Recht auf Privatsphäre nicht geringer als in einem unterdrückenden Regime. Aufgrund sogenannter „chilling effects“ kann anlasslose Überwachung zu einer Transformation hin zu einer Kontrollgesellschaft führen: Allein die Möglichkeit, dass jemand überwacht wird, reicht aus, um das Verhalten zu beeinflussen[13].

Denn selbst wenn in einem Staat nur „gerechte“ Gesetze herrschen, ein ewiges Rückwirkungsverbot durchgesetzt ist und Informationen ausschließlich zur Durchsetzung der Gesetze genutzt werden, ist anlasslose Überwachung problematisch: Der Algorithmus zur Erkennung von Verdächtigen kann nicht öffentlich sein, weil Straftäter/innen ihr Verhalten entsprechend anpassen könnten. Damit wäre niemandem klar, welche legale Handlung ihn oder sie auffällig werden lassen könnte, und wahrscheinlich würde sich ein Großteil der Bevölkerung an einen vermuteten Erkennungsalgorithmus anpassen. Das kann dazu führen, dass Personen auf die Einforderung von Menschenrechten, wie zum Beispiel Versammlungs- oder Meinungsfreiheit, verzichten. Zweitens erfolgt Überwachung durch eine Mischung aus Mensch und Maschine. Es gibt ein erhebliches Missbrauchspotential bei Überwachung, wie zum Beispiel die Diskreditierung persönlicher oder politischer Gegner/innen oder das Gegenteil. In Geheimdienstkreisen gibt es zum Beispiel den Begriff „LoveInt“ für das Ausspähen von gewünschten Partner/innen. Missbrauch kann auch im „idealen“ Staat passieren. Eigentlich reicht sogar die Möglichkeit des Missbrauchs schon aus, um Verhalten zu beeinflussen. Dadurch, dass nicht klar ist, was bei politischer Teilhabe gegen ein/e Kandidat/in verwendet werden kann oder wessen Existenz oder sogar Leben durch Erkenntnisse über sexuelle Identität, politische Gesinnung, Sexualpartner/innen, deliktuales Verhal-

ten, o.ä. gefährdet ist, erzeugt Überwachung eine Selbstzensur, die sogar das Einfordern der eigenen Menschenrechte betrifft.

Selbst bei gewissenhaften Überwacher/innen ist ein technisches System anfällig und die Snowden-Affäre an sich zeigt, dass auch Geheimdienste die Verteilung von Daten nicht kontrolliert können. Dass personenbezogene Daten nicht veröffentlicht wurden, ist lediglich dem Verantwortungsbewusstsein von Snowden und den Medienvertreter/innen zu verdanken. Somit ist anlasslose Überwachung auch in einem „idealen" Staat abzulehnen.

ZUSAMMENFASSUNG

Zusammenfassend verletzen die Praktiken der u.a. die in diesem Artikel genannten Akteure das Recht auf Privatsphäre/Privatleben. Dieses Recht ist unter anderem in der Allgemeinen Erklärung der Menschenrechte (Art. 12), dem UN-Zivilpakt (Art. 17) sowie in der Europäischen Menschenrechtskonvention (Art. 8) verankert. Darüber hinaus gefährden die Praktiken die Wahrnehmung vieler anderer Menschenrechte und deren Verteidigung.

Steffen Härting
steffen.haerting@amnesty-digital.de
PGP: 79D6 94B3 03F8 1302 106A BF5D BA05 470F 2E7C A960

[1] „Through the acquisition of LiveRamp, Acxiom will expand its capability to bridge the gap between offline data and the rapidly growing universe of online marketing applications", http://www.acxiom.com/acxiom-liveramp/, 14.12.2014.
[2] Z.B. bietet AZ Direct Adressen von „Die Zeit"-Abonnent/innen an. http://www.az-direct.com/site/blaetterkatalog/listinfos/index.html, Seite 50, 14.12.2014
[3] Recorded Future, https://www.recordedfuture.com/defense-intelligence/, 14.12.2014.
[4] Snowden-Dokumente: Squeaky Dolphin, XKeyScore, GoogleCookies.
[5] Snowden-Dokumente: Eikonal.
[6] Snowden-Dokumente: per Apps wie z. B. Angrybird.
[7] Snowden-Dokumente: Dishfire: angeblich ca. 200 Mio. SMS pro Tag, aber auch Finanztransaktionen.
[8] Snowden-Dokumente: ca 5 Mio Datensätze pro Tag.
[9] Snowden-Dokumente: Deutsche Telekom (Eikonal), Stellar.
[10] Stichwort „Deep Packet Inspection".
[11] Chittaranjan et al. (2011) sprechen von einer Genauigkeit von 76% innerhalb der untersuchten Gruppe.
[12] De Montjoye et al. (2012); Youyoua, Kosinskib, Stillwella (2015).
[13] Stichwort: Hawthorne-Effekt.
PEN America - Studie (2013) Titel: "chilling effects"
Bude (2014)

GIBT ES EIN RECHT AUF DISKRIMINIERUNGSFREIEN INTERNETZUGANG?

In dieser Broschüre werden verschiedene Aspekte aufgegriffen, wie das Internet unser Leben und die Situation der Menschenrechte verändert. Wenn man sich die Tragweite der Digitalisierung anschaut, dann wird schnell klar, dass diese nahezu alle Lebensbereiche umfasst. Da man sich schwerlich der elektronischen Datensammlung und -verarbeitung durch Staaten und Konzerne entziehen kann, wird somit ersichtlich, dass wir den Schutzraum verschiedener Menschenrechte neu definieren müssen.

Wir haben jedoch noch ein weiteres Problem zu diskutieren. Je mehr unsere Kultur, unsere Politik und unsere Wissenschaft auf die Unterstützung von elektronischen Werkzeugen zurückgreift, desto wichtiger muss ein Zugang zu diesen Bereichen gewertet werden. Somit zwingt sich die Frage auf, ob aus der Digitalisierung ein Recht auf diskriminierungsfreien Zugang zum Internet abzuleiten ist.

Als Grundlage für unsere Überlegungen kommen verschiedene Menschenrechte in Betracht. Auch wenn man zuerst an die Meinungs- oder Pressefreiheit (Art. 19 der Allgemeinen Erklärung der Menschenrechte, AEMR) denken würde, so geht es heute oftmals um den grund- sätzlichen Zugang zu kulturellen oder Bildungsangeboten. Das Recht, sich gleichberechtigt an den Künsten zu erfreuen oder am wissenschaftlichen Fortschritt und seinen Errungenschaften teilzuhaben (Art. 26 und 27 AEMR), kann zunehmend nur noch dann gewährleistet werden, wenn ein Zugang zum Internet besteht. Je größer der Anteil unseres Wissens ist, der nur noch „digital“ verfügbar ist, desto schwerer wiegt ein Ausschluss aus diesem Medium.

Aus der Perspektive einer Menschenrechtsorganisation wie Amnesty International ist ein Zugangsrecht zum Internet von besonderer Bedeutung. Welche Chancen sich aus der Verbreitung von Laptops und Smartphones für die Öffentlichkeitsarbeit oder die Dokumentation von Verbrechen und Unterdrückung ergeben, haben bisher vor allem Staaten entdeckt. Nicht überraschend hat die Türkei während der Proteste im Gezi-Park Twitter sperren lassen oder der Iran den Zugriff auf Facebook geblockt. Statt mit einem großen Polizeiaufgebot hat China vor allem mit entsprechender Internetzensur dem 25. Jahrestag von Tian'anmen gedacht.

Die Informations- und Ausdrucksfähigkeit einer Gesellschaft unterscheidet sich enorm, je nachdem ob ihr Zugang zum Internet frei wie in Island oder Deutschland oder eingeschränkt wie in China oder auch den USA und Groß-

britannien ist. Diese Ansicht teilen vor allem Menschen in Staaten, deren Zugang immer wieder eingeschränkt wird – denn hier sind die Unterschiede oftmals spürbar. Nach einer Ipsos-Studie aus dem Jahr 2014 unterstützen durchschnittlich 83% der Befragten in Staaten wie Tunesien, Ägypten, der Türkei oder Pakistan die Forderung nach Anerkennung eines Menschenrechts auf Internetzugang. Und das, obwohl die Internetabdeckung in diesen Staaten deutlich geringer ist als beispielsweise in Europa.

Es hat natürlich nicht jeder Staat die Möglichkeit, seiner Bevölkerung flächendeckenden Zugang zum Internet zu gewährleisten. Es fordert auch niemand, den Ausbau von Mobilfunknetzen auf Kosten zum Beispiel einer Versorgung mit Grundnahrungsmitteln voranzutreiben. Je mehr aber ein Staat seine Verwaltung, Bildung und Kultur digitalisiert, und je mehr der politische und gesellschaftliche Diskurs online stattfindet, desto eher müssen sich Staaten dieser Aufgabe stellen. Die möglichen Ersparnisse, die durch digitale Datenverarbeitung gemacht werden können, dürfen nicht auf Kosten von denjenigen Bevölkerungsteilen erfolgen, die nicht über die finanziellen Mittel verfügen, von alleine an dieser Entwicklung Teil zu haben. Vielmehr sollten die Chancen erkannt werden, die der Zugang zum Internet bei der Unterstützung von Eigeninitiative und der Linderung von Not bieten kann. Dass es momentan aber hauptsächlich gewinnorientierte Privatunternehmen sind, die sich der Versorgung von beispielsweise mittelafrikanischen Gebieten, die bisher nicht über Netzabdeckung verfügen, verschrieben haben, kann dabei langfristig große Risiken mit sich bringen und muss daher staatlich kontrolliert werden.

Ein Problem, das durch einen profitorientierten Ausbau des Internets entstehen kann, ist eine Gefährdung der sogenannten Netzneutralität. Hierbei geht es darum, ob alle Dienste und Daten im Internet gleichberechtigt behandelt werden. Von manchen Unternehmen wird gefordert, dass die Geschwindigkeit und die Priorität, mit der Daten im Netz weitergeleitet werden, ab einem gewissen Transfervolumen davon abhängen sollen, was die Anbieter oder Nutzer von Services zu zahlen bereit sind. Das kann negative Auswirkungen auf die Reichweite vor allem von kleinen Nichtregierungsorganisationen haben – und stellt in gleichem Maße eine Diskriminierung von bestimmten Benutzer- und Anbietergruppen dar.

Auch die Bestrebungen, den Zugang zum Internet für bestimmte Nutzer zu sperren, wenn diese Urheberrechtsverstöße begangen haben („Three Strikes“), muss unter menschenrechtspolitischen Gesichtspunkten äußerst kritisch betrachtet werden. Unabhängig von der strafrechtlichen Bedeutung dürfen die Folgen von Urheberrechtskonflikten nicht in Diskriminierung und Zugangsbeschränkungen enden.

Wie an so vielen anderen Punkten, wenn es um den Menschenrechtsschutz in digitalen Sphären geht, wird auch hier ersichtlich, dass Staaten nicht mehr als alleinige Ansprechpartner ausreichen. Dieser Punkt wird unter dem Schlagwort Internet Governance an anderer Stelle in dieser Broschüre ausführlich behandelt.

Ein Recht auf diskriminierungsfreien Internetzugang ergibt sich nicht wörtlich aus der AEMR, zumindest aber aus den veränderten Voraussetzungen, die sich für den Schutz vieler anderer Rechte durch die Digitalisierung ergeben. Hier geht es also nicht darum, ein Menschenrecht auf eine bestimmte Technologie zu konstruieren. Technologie kann nur bei der Verwirklichung von Rechten helfen und ist keineswegs ein Recht an sich. Mit der Bedeutung, die das Internet aber bereits erreicht hat und noch erreichen wird, ist anzunehmen, dass die in der AEMR verbürgten Rechte kaum noch ohne ein Zugangsrecht gewährt werden können.

Die Situation und Bedeutung dieses Rechtes muss wohl in Abhängigkeit der Situation eines Landes im Einzelfall bewertet werden – so wie auch das Recht auf Bildung oder Sozialfürsorge bei Arbeitslosigkeit an den Möglichkeiten eines jeweiligen Staates gemessen wird. Es mag daher in den industrialisierten Ländern eine diskussionsfähige Forderung sein, Provider dazu verpflichten zu wollen, jedem Haushalt eine Mindestmenge an Datenvolumen zur Verfügung zu stellen – an anderen Orten auf der Erde wäre solch eine Idee noch zu weit gegriffen.

Wer die Diskussion um ein mögliches Zugangsrecht zum Internet noch ablehnt, der wird dennoch langfristig nicht um sie herum kommen. Denn eine Nichtbeachtung der digitalen Sphäre ignoriert nicht nur die möglichen Gefahren, die sich für die Menschenrechte ergeben können, sondern verschwendet auch das menschenrechtliche Potenzial, das sich aus der Digitalisierung ergeben kann. Wir sind dabei, eine Bibliothek zu bauen, und wir müssen Sorge tragen, dass es nicht vom Geldbeutel oder den politischen Interessen weniger abhängt, wer diese Bibliothek betreten darf, denn das wäre ein Verstoß gegen die Gleichheit und das Diskriminierungsverbot. Wer also ein Recht auf Internetzugang heute noch verneinen mag, wird diese Position vermutlich in Zukunft immer häufiger auf den Prüfstand stellen müssen.

Das Internet kann mit seinen Kanälen und seiner Geschwindigkeit ein Katalysator für den Menschenrechtsschutz sein, und schon aus diesem Grund muss es im Interesse einer Menschenrechtsorganisation liegen, sich für einen freien und ungehinderten Zugang einzusetzen.

Ein Recht auf Internetzugang muss nicht unbedingt neu geschaffen werden, sondern leitet sich aus den verschiedenen Rechten der AEMR ab. Dieses im Rahmen eines Internationalen Paktes noch einmal deutlich zu bekräftigen, kann aber nicht schaden und könnte nach der hier vertretenen Ansicht eines der ersten Ziele von Amnesty International sein.

Mike Karst
karst@amnesty-digital.de
PGP: EE3E 936E 755E AC36 7715 2205 992C C947 E948 47E2

WHISTLEBLOWER UND DIE DIGITALE WELT

Bei Whistleblowern handelt es sich um Menschen, die Missstände aufdecken. In der Regel sind es Insider, die geheime oder interne Dokumente veröffentlichen, mit denen Straftaten wie Korruption oder Insiderhandel, Datenmissbrauch oder Menschenrechtsverletzungen belegt werden.

Whistleblower übernehmen damit eine wichtige gesellschaftliche Funktion: Es ist im Interesse aller Menschen, diese Missstände aufzudecken und dadurch die Verantwortlichen zum Handeln zu bewegen und die Missstände abzustellen. Meist versuchen die Informanten zuvor vergeblich, die Probleme intern zu melden oder stoßen bei Vorgesetzten mit ihrem Anliegen auf taube Ohren. Der Weg an die Öffentlichkeit ist dann die letzte und einzige Möglichkeit, dass Missstände aufgedeckt und abgestellt werden.

Wenn beispielsweise ein Mitarbeiter eines Entsorgungsunternehmens erfährt, dass seine Firma Giftmüll illegal entsorgt, sollte er die zuständigen Behörden und die Öffentlichkeit informieren. Wenn ein Beamter erfährt, dass Politiker an betrügerischen Geschäften beteiligt sind, sollte auch dies bekannt werden. Wir brauchen diese mutigen Menschen, damit die Gesellschaft von den Missständen erfährt und die Probleme gelöst werden.

Zuletzt haben die Fälle von Bradley Manning (2010) und von Edward Snowden (2013) das Thema Whistleblowing in den Fokus der Öffentlichkeit gerückt.

Bradley Manning hat über die Plattform Wikileaks Dokumente über den Irak-Krieg zugänglich gemacht. Darunter war ein Video über Angriffe aus einem US-Kampfhubschrauber auf irakische Zivilisten, bei denen elf Menschen, darunter zwei Reuters-Reporter, getötet wurden. Diese Dokumente zeichneten ein anderes Bild vom Irak-Krieg als das, welches das US-Verteidigungsministerium gerne der Weltöffentlichkeit präsentieren wollte. Nach seiner Enttarnung wurde Bradley Manning von einem US-Militärgericht unter anderem wegen Geheimnisverrats, Spionage, Computerbetrugs und Diebstahls zu 35 Jahren Haft verurteilt.

Edward Snowden hat aufgedeckt, in welchem Ausmaß der amerikanische Auslandsgeheimdienst NSA (National Security Agency) elektronische Kommunikation im In- und Ausland überwacht. Eine solche exzessive Überwachung stellt eine Menschenrechtsverletzung dar. Snowden lebt zur Zeit in Russland, wo ihm zeitlich begrenztes Asyl gewährt wurde. Er wird von den USA per Haftbefehl gesucht. Ihm drohen für diese Informationsweitergabe lange Haftstrafen und verschärfte Haftbedingungen.

Diese beiden Fälle machen deutlich, wie Whistleblowing mit den Menschenrechten in Zusammenhang steht. Whistleblowing ist vom Menschenrecht der Meinungsfreiheit gedeckt (Art. 19 der Allgemeinen Erklärung der Menschenrechte, Art. 19 des Internationalen Paktes über bürgerliche und politische Rechte, Art. 10 der Europäischen Menschenrechtskonvention). Es dient der allgemeinen Informationsfreiheit aller Menschen, die ohne das Whistleblowing nicht von den Missständen erfahren würden. Wenn Whistleblower Informationen über Menschenrechtsverletzungen aufdecken, verdienen sie besonderen Schutz.

Daher wird schon lange ein Whistleblower-Gesetz gefordert, das es weltweit längst gibt, aber in Deutschland bislang nicht umgesetzt wurde. Dabei soll es besonders darum gehen, dem Whistleblower weniger Risiko und mehr Berechenbarkeit für die Informationsweitergabe zu geben, indem zum Beispiel dem Arbeitgeber Rachemaßnahmen untersagt werden und der Schutz vor staatlicher Verfolgung festgeschrieben wird.

Der Europäische Gerichtshof für Menschenrechte hat für den Schutz von Whistleblowern Kriterien aufgestellt, nach denen sich die Schutzwürdigkeit der Informationsweitergabe bestimmt. Danach kommt es maßgeblich an auf
- das öffentliche Interesse an der aufgedeckten Information,
- die Authentizität der aufgedeckten Information,
- mögliche Alternativen zur Veröffentlichung der Information (z.B. vorherige interne Beschwerde beim Arbeitgeber),
- den Schaden, der für den Arbeitgeber oder den Staat entsteht und in welchem Verhältnis dieser zum öffentlichen Interesse steht,
- die Schwere der Sanktion, die der Whistleblower zu befürchten hat.

Amnesty International fordert den Schutz der Whistleblower vor exzessiven Sanktionen. Whistleblower, die im Interesse der Öffentlichkeit Missstände oder sogar schwere Menschenrechtsverletzungen aufdecken, handeln im Rahmen ihrer Meinungsfreiheit.

Das öffentliche Interesse, in dem Whistleblower aktiv werden, muss im strafrechtlichen, arbeitsrechtlichen oder in sonstigen Verfahren berücksichtigt werden. Bei der Zumessung der Sanktionen muss auch eine Rolle spielen, ob der Staat durch die Enthüllungen tatsächlich Schaden genommen hat.

Christopher Schmidt

MEINUNGSFREIHEIT 404

DER DIGITALE ASPEKT

Eine immer größere Menge an Informationen, die durch das Internet zugänglich gemacht wird, beinhaltet aktuell nicht nur Einkaufsportale. Man findet dort „wilde“ Zeitungen, politische Foren und Informationsportale, gefüllt mit Informationen über die Studentenproteste in China oder über den „Tank Man“ auf dem Tian'anmen-Platz. Aber auch Dinge wie Anleitungen für anonymen Internetzugang oder Berichte über Geheimdienstüberwachung.

Darüber hinaus erlaubt das Internet eine Vernetzung, durch die Informationen blitzschnell verbreitet werden können. Beweise für Menschenrechtsverletzungen oder Korruption können "freigelassen" werden und lassen sich von Machthaber/innen nicht einfach wieder entfernen. Im Internet kann jede Person prinzipiell jeder Person Informationen schicken. Wenn etwas öffentlich verbreitet wird, dann ist die Kontrolle über diese Information meistens nicht einmal mehr dem/der Urheber/in gegeben. Wenn sich etwas blitzschnell verbreitet, dann wird dieses Phänomen im Werbeumfeld „virales Marketing“ genannt. Für Menschenrechtaktivist/innen, Oppositionelle und Journalist/innen kann das Internet „virale Aufklärung“ bieten.

Jedoch wird in verschiedenen Ländern die Verbreitung oder Beschaffung bestimmter Informationen geahndet oder es findet Zensur durch Filterung statt.

Bekannte Methoden sind die Einschüchterung von Autor/innen, stichwortbezogene Filterung von Webseiten und die Erstellung von „schwarzen Listen“. Im Extremfall wird sogar ein nationales Netz aufgebaut und alle anderen Informationskanäle verboten.

FILTERUNG VON INHALTEN

Das bekannteste Beispiel für Filterung von Stichworten ist die „Great Firewall of China“. Sie blockiert bestimmte Begriffe wie „Demokratie“, „Platz des himmlischen Friedens“, „Menschenrechte“ oder „Arabischer Frühling“. Vereinfacht gesagt, ist es möglich, dass Daten, die nach China „hineingeschickt“ werden, untersucht und gefiltert werden. China verwendet außerdem Technologien, die verdächtige Teile der Adresse einer Webseite identifizieren, und sogenannte „schwarze Listen“. An dieser vergleichsweise hoch ausgereiften Technologie haben auch andere Länder Interesse gezeigt. So haben China und Iran angekündigt, dass für den Aufbau eines „Halal-Internet“ im Iran die technische Unterstützung durch China erfolgen kann.

Weniger ausgefeilt, aber umso effektiver, ist die Kontrolle von Informationen in Nordkorea. Eigentlich kann in Nordkorea eher von einem Intranet gesprochen werden. Die Bevölkerung hat bis auf wenige Ausnahmen keine Möglichkeit, Zugang zum Internet zu erhalten. Inhalte werden sozusagen vom Internet erst in das Intranet kopiert. Hier kann man das Ausmaß der Zensur besser anhand der zugänglichen Webseiten als anhand der gesperrten

Webseiten abschätzen. Andere Informationskanäle, wie internationale Telefongespräche, sind gesperrt.

EINSCHÜCHTERUNG MÖGLICHER VERÖFFENTLICHER/INNEN
In großen Teilen der Welt werden Betreiber unerwünschter Webseiten und Blogs eingeschüchtert und verhaftet. Amnesty International berichtete im Zuge der „Jasminrevolution" in China über Verhaftung von über 100 Aktivist/innen, von denen viele auf Twitter und in Blogging-Netzwerken aktiv waren. In den Vereinigten Arabischen Emiraten gab es den sogenannten „UAE 94"-Prozess, bei dem sich unter den Angeklagten viele Blogger und Internetaktivist/innen befanden. Amnesty International stellte fest, dass das Verfahren in grober Weise unfair war und berichtete darüber, dass der Sohn des Angeklagten Abdulrahman al-Hadidi aufgrund von Tweets über den Prozess verurteilt wurde. In den Tweets fragte er nur, warum das Gericht Foltervorwürfen durch einige Angeklagte nicht nachgehen würde und warum den Angeklagten kein Zugang zu ihren Rechtsbeiständen gewährt würde. In Saudi-Arabien wurde Raif Badawi, ein Blogger und Betreiber einer Webseite zum politischen Austausch, zu 1000 Peitschenhieben, einer Geldstrafe und Gefängnis verurteilt. Mit der Einschüchterung von (Internet-)Aktivist/innen sind die eben beschriebenen Länder nicht alleine. Russland, Kuba, Iran, Bahrain, Weißrussland oder Vietnam ergänzen diese Liste nicht exklusiv.

In den USA findet Einschüchterung von Whistleblower/innen, die Menschenrechtsverletzungen durch Militär und Geheimdienste aufdecken könnten, durch rigide Gesetzgebung statt. Informationen über Menschenrechtsverletzungen durch den Staat sind zwar als geheim eingestuft, allerdings von so großem öffentlichem Interesse, dass Whistleblower/innen nicht angeklagt werden dürfen. Die Gesetzgebung muss Whistleblower/innen schützen. Beispiele sind Edward Snowden und Chelsea Manning, zu denen in dieser Broschüre unter dem Punkt „Whistleblower" mehr Informationen gefunden werden können.

SCHWARZE LISTEN
Darüber hinaus gibt es eine große Anzahl von Ländern, in denen Webseiten auf eine „Sperrliste" gesetzt werden.

So gibt in Australien eine „schwarze Liste" von Webseiten, die zu einem großen Teil in Zusammenhang mit Straftaten stehen. Diese Listen werden nicht veröffentlicht, um nicht als „Landkarte" zu dienen. Das allerdings birgt die Gefahr, dass unliebsame Webseiten gesperrt werden. Dass das auch geschieht, zeigen Beispiele, bei denen harmlose, politische Webseiten in solche Listen aufgenommen wurden.

Liegt es vielleicht in der Natur von Zensur, dass sie zwangsläufig früher oder später zur Durchsetzung politischer Interessen missbraucht wird?

In der Tat zeigen Beispiele wie Russland oder Iran, dass zu Beginn der Internetsperren die Kriterien für die Aufnahme in schwarze Listen meistens gesellschaftlich akzeptiert sind. In Russland ging es zunächst um den Schutz

von Kindern und Jugendlichen. Die Kriterienliste wurde seitdem erweitert und Formulierungen wie „extremistische Ideen“ bieten Spielraum für Interpretation. Russland ist auch ein Beispiel für die Sperrung von Webseiten, die nicht den Kriterien entsprechen, wie die von rublacklist.net veröffentlichte Liste von Webseiten, die wegen übereinstimmender IP-Adresse mit anderen Webseiten versehentlich blockiert wurden, zeigt.

Die Einrichtung von „schwarzen Listen“, die auch zunehmend in Europa diskutiert wird und teilweise umgesetzt ist, bietet eine schlüsselfertige Zensurinfrastruktur, deren Kriterien bei vorhandenem Willen zum Missbrauch lediglich angepasst werden müssen.

Außerdem muss man sich fragen, ob die Einrichtung von Filtern für den Jugendschutz oder den Schutz der Demokratie überhaupt notwendig ist: Die regelmäßige Abschaltung von Webseiten, die für Betrug im Bereich Onlinebanking effektiv und schnell durchgeführt wird, zeigt, dass ein Abschalten von Webseiten mit Bezug zu schweren illegalen Aktivitäten ohne Filterung möglich ist.

KOMMUNIKATION MITTELS INTERNET

Da das Internet neue, schnellere und günstigere Vernetzungsmöglichkeiten bietet, werden über die Zensur von Inhalten hinaus in einigen Ländern, insbesondere bei Protesten, soziale Medien gesperrt. So wurden Smartphones intensiv während der Taksim-Proteste in der Türkei genutzt, um Beweise zu sichern und Aufmerksamkeit zu erzeugen. Als Reaktion wurde ein Gesetz beschlossen, das die Sperrung von Webseiten ohne Richtervorbehalt ermöglicht und von Amnesty International scharf kritisiert wird. Des Weiteren drohte der Präsident der Türkei im Zuge eines Korruptionsskandales 2014 mit der Sperrung sozialer Netzwerke, die in der Türkei zunehmend regelmäßig durchgeführt wird. Die Türkei ist nur ein Beispiel dafür, dass in vielen Ländern die Kommunikationsinfrastruktur bei Protesten ausgeschaltet oder beeinträchtigt wird.

ZUSAMMENFASSUNG

Zusammenfassend kann man im Bereich Internetzensur und Einschränkung von Meinungsfreiheit im Internet von einem fast weltweiten Phänomen reden. In Ländern, in denen eine politisch motivierte Zensur durchgeführt wird, wird diese in den meisten Fällen lediglich durch die technischen Möglichkeiten der Länder beschränkt. Wenn die technischen Möglichkeiten oder der politische Spielraum so eingeschränkt sind, dass eine mögliche Umgehung der Zensurmaßnahmen befürchtet wird, wird auf Einschüchterung der Informationsverteiler/innen oder die Einschränkung des Zugangs zum Internet zurückgegriffen. Da die technische Aufrüstung allerdings aktiv von Ländern unterstützt wird, die ebenfalls zensieren und über das notwendige Wissen verfügen, ist hier eine Verschlimmerung zu befürchten. In vielen Ländern, in denen keine Blockade von Webseiten stattfindet, wird regelmäßig ein Diskurs über die Einführung von Filtern entfacht.

Amnesty International hält das Internet für eine Triebkraft für politische Frei-

„Die Zensur ist das lebendige Geständnis der Großen, daß sie nur verdummte Sklaven treten, aber keine freien Völker regieren können."

Charakter „Eberhard Ultra"
in Johann Nestroys Stück „Freiheit in Krähwinkel"

heit und stellt sich gegen den Missbrauch für Repression. Menschen haben das Recht, sich Informationen zu beschaffen, sie zu empfangen und zu verbreiten, sie haben das Recht auf Meinungs- und Informationsfreiheit mit allen Verständigungsmitteln. Diese Verständigungsmittel umfassen auch das Internet.

Steffen Härting
steffen.haerting@amnesty-digital.de
PGP: 79D6 94B3 03F8 1302 106A BF5D BA05 470F 2E7C A960

MENSCHENRECHTE 2.0

DER BEITRAG DER INTERNET GOVERNANCE ZUR MODERNISIERUNG DES MENSCHENRECHTSSCHUTZES IN EINER DIGITAL VERNETZTEN WELT

Die zunehmende Vernetzung über das Internet hat zu einer fortschreitenden Durchdringung unseres Alltags mit digitaler Kommunikationstechnologie geführt. Seit geraumer Zeit schon ist das Phänomen der Medienkonvergenz bekannt, mit dem das (zunächst technische) Zusammenwachsen unterschiedlicher Kommunikations- und Informationsmedien auf demselben Endgerät über dasselbe Netz beschrieben wird. Bald schon könnte dieser Prozess seinen Abschluss finden, wenn das Internet zum einzigen globalen (Massen- und Individual-)Kommunikationsnetz geworden ist, in das sich die bisherigen Mobilfunk- und Telefonfestnetze sowie Rundfunkübertragungsnetze als reine Zugangsinfrastruktur einfügen. Doch es ist nicht nur die Kommunikation zwischen Menschen, die schon heute auf breiter Basis über das Internet erfolgt: Auch Datenbanken (etwa beim Cloud Computing), Maschinen (Internet of Things), ja, ganze Häuser, Städte und Fertigungsstätten (beschrieben mit Begriffen wie Smart Home, Smart Cities oder Industrie 4.0) kommunizieren zunehmend über das Internet miteinander.

Nicht nur wir selbst organisieren uns also immer stärker über das Internet – wir werden auch organisiert durch automatisierte Prozesse, die das Netz als Grundlage verwenden. Mit dem Internet ist eine kollektive Arbeits- und Freizeitinfrastruktur entstanden, die uns in jeder Lebenslage zur Verfügung steht, uns bei unseren Zielen und Aufgaben unterstützen kann und dabei selbst immer intelligenter wird, weil sie im Gegenzug von unseren menschlichen Interessen und Vorgehensweisen lernt.

Die Grenzen zwischen offline und online verschwimmen dadurch zusehends. Eine künstliche Trennung beider Welten beim Menschenrechtsschutz aufrechterhalten zu wollen, würde den tatsächlichen technischen Gegebenheiten nicht gerecht und könnte sogar zu einer willkürlichen Differenzierung menschenrechtlicher Schutzniveaus führen. Statt dessen muss klar sein, dass das Leben in der „virtuellen Welt“ grundsätzlich denselben Regeln zu folgen hat wie das Leben in der „realen Welt“. Wenn wir dabei an unserem freiheitlichen Menschenbild festhalten wollen, müssen die Menschenrechte die Grundlage beider Welten sein.

Im Offline-Bereich ist dies seit der Verabschiedung der Allgemeinen Erklärung der Menschenrechte vom 10. Dezember 1948 klar. Dass dieselben Rechte, die offline gelten, aber auch online zu schützen sind, erkannte die Staatengemeinschaft erst in einer Resolution des Menschenrechtsrates vom Juli 2012[1], offiziell an. Sie bekräftigte dies in einer weiteren Resoluti-

on[2], die angesichts der Enthüllungen Edward Snowdens im Dezember 2013 von der UN-Generalversammlung zum Recht auf Privatheit im digitalen Zeitalter verabschiedet wurde.

Dieses Bekenntnis stellt das Fundament für die Anwendung der Menschenrechte auf das Internet dar. Damit sind aber noch nicht die wesentlichen Folgefragen geklärt: Vor welche spezifischen Herausforderungen stellt das Netz die Menschenrechte? Welche Rechte sind daher dort besonders betroffen? Wer ist legitimiert, diese Rechte für den Kommunikationsraum Internet zu konkretisieren? Und wer ist in einem Netz, das hauptsächlich von privaten Akteuren errichtet, betrieben und verwaltet wird, zu ihrem Schutz berufen – und befähigt?

UM WELCHE RECHTE GEHT ES?

Mit der Aussage, die uns aus der Offline-Welt bekannten Menschenrechte gälten auch im Netz, kann es nicht sein Bewenden haben. Die diesen Rechten zugrundeliegenden Werte gelten zwar nach wie vor, und das ist die wesentliche Botschaft dieser Resolutionen. Wie sie aber geschützt werden sollen in einer Netzwelt, die geprägt ist von den technischen Besonderheiten, die eine digitale Datenverarbeitung mit sich bringt, aber auch von gesellschaftlichen und kulturellen Andersartigkeiten, die auf ihrem globalen Charakter gründen – das ist damit nicht gesagt. Es bedarf daher einer neuen, an die Gegebenheiten in einer Welt der globalen digitalen Kommunikation angepassten Formulierung.

Funktionen des Internets und Bezüge zu den Menschenrechten

- Medium (Massenkommunikation): Meinungsfreiheit, Informationsfreiheit
- Telekommunikationsnetz (Individualkommunikation): Recht auf Privatsphäre
- Bildungsstätte: Recht auf Bildung
- Arbeitsstelle: Recht auf Arbeit
- Datenspeicher: Datenschutz
- Gesundheitsdienst: Recht auf Gesundheit/angemessenen Lebensstandard
- Ort politischer Debatten: Versammlungs- und Vereinigungsfreiheit, Recht auf politische Teilhabe
- Kulturstätte: Recht auf kulturelle Teilhabe, Recht auf Urheberschutz
- Ort des wissenschaftichen Diskurses: Recht auf Teilhabe am wissenschaftlichen Fortschritt
- Ort religiöser und weltanschaulicher Betätigung: Gedanken-, Gewissens- und Religionsfreiheit

Nicht alle Menschenrechte sind von der zunehmenden Vernetzung über das digitale Medium Internet gleichermaßen betroffen. Betrachtet man das Internet funktional, so wird deutlich, dass seine zahlreichen Nutzungsmöglichkeiten untrennbar mit einer Reihe von Menschenrechten verbunden sind, von denen ihre ungehinderte Verwirklichung abhängt (siehe Kasten).

Die Realisierung dieser Rechte ist bislang Aufgabe der Staaten, denn sie waren es, die sich in zahlreichen internationalen Verträgen wie dem Internationalen Pakt über bürgerliche und politische Rechte (UN-Zivilpakt) und dem Internationalen Pakt über wirtschaftliche, soziale und kulturelle Rechte (UN-Sozialpakt) auf die Einhaltung der Menschenrechte verpflichtet haben. Diese Verpflichtung besteht für die Staaten in dreierlei Ausprägung:

- als Achtungspflicht: Der Staat muss eigene Eingriffe in diese Rechte auf das beschränken, was nach den in den Verträgen niedergelegten Grundsätzen, insbesondere dem Verhältnismäßigkeitsprinzip, zulässig ist.
- als Schutzpflicht: Der Staat muss – insbesondere durch Gesetze und eine funktionsfähige Justiz – unrechtmäßige Eingriffe in die Menschenrechte durch Dritte (seien es private Akteure oder ausländische Staaten) unterbinden, indem er sie verbietet und Verstöße gegen diese Verbote effektiv bestraft.
- als Erfüllungspflicht: Der Staat muss mit den ihm zur Verfügung stehenden Möglichkeiten aktiv auf eine Verwirklichung dieser Menschenrechte hinwirken, z. B. durch die Finanzierung oder anderweitige Förderung entsprechender Angebote.

Aus der Bedeutung der Funktionen des Internet für die Durchsetzung der damit zusammenhängenden Menschenrechte lässt sich einerseits ein Recht ableiten, überhaupt Zugang zu diesem öffentlichem Kommunikationsraum zu erhalten. Denn nur so kann die Teilnahme an den durch ihn vermittelten Kommunikations- und Informationsmöglichkeiten und die Partizipation an den öffentlichen Angelegenheiten für den Einzelnen heute noch wirksam sichergestellt werden. Ob dies bedeutet, dass der Staat durch Anreizmodelle dafür sorgen muss, dass der Privatsektor ausreichend in den Netzausbau investiert, oder ob er darüber hinaus sogar kostenlose öffentliche Internetzugänge bereitstellen muss, ist in diesem Zusammenhang zu klären.

Andererseits ist die Frage zu beantworten, wie dieser Kommunikationsraum ausgestaltet werden muss, damit die Wahrnehmung der Menschenrechte in ihm effektiv gewährleistet ist. Dies kann bedeuten, dass der Staat eine Grundversorgung mit Informationen zu gewährleisten hat. Es bedeutet aber auch, dass seine Befugnisse zur Überwachung privater Kommunikation und zur (zweckfremden) Verwendung persönlicher Daten – insbesondere durch den Grundsatz der Verhältnismäßigkeit – beschränkt sind. Aus seiner menschenrechtlichen Schutzpflicht ergibt sich ferner die Aufgabe zu verhindern, dass sich Dritte in unzulässiger Weise Daten über die Menschen unter seiner Herrschaftsgewalt beschaffen.

WER SOLL DIE MENSCHENRECHTE GARANTIEREN?

Waren es bisher ausschließlich die Staaten, die sich als Völkerrechtssubjekte nach dem Völkerrecht auf die Menschenrechte verpflichten konnten, stellt sich angesichts zweier Besonderheiten im Kommunikationsraum Internet die Frage nach dem richtigen Verpflichtetenkreis: Zum einen erscheint der Einfluss des Staates in einem globalen, die Grenzen seines eigenen Hoheitsgebiets weit überschreitenden Kommunikationsnetz sehr beschränkt. Zum anderen ist das Internet selbst kein öffentlicher Raum: Ein Großteil der Infrastruktur und der angebotenen Dienste wird von privater Seite bereitgestellt.

ENTGRENZUNG UND EXTRATERRITORIALITÄT

Mit der Entwicklung des weltumspannenden Kommunikationsnetzes Internet hat sich der Einflußbereich der gesellschaftlichen Akteure grundlegend erweitert: Unternehmen bieten ihre Dienstleistungen heute global an, Verbraucher kaufen grenzüberschreitend ein. Auch der „globale Bürger“ kann im Internet seine Menschenrechte nun mit nahezu weltweiter Wirkung ausüben. Dagegen bleiben die Einflussmöglichkeiten der Staaten aus rechtlicher Sicht aktuell überwiegend auf das eigene Hoheitsgebiet beschränkt. Ihre tatsächlichen Handlungsmöglichkeiten reichen wegen der Fernwirkung im Netz jedoch oftmals weit über das eigene Territorium hinaus. Die Enthüllungen Edward Snowdens haben gezeigt, dass diese Möglichkeiten durch einige Staaten auch genutzt werden, um die Rechte von Menschen in anderen Staaten zu verletzen, ohne daß die letzteren dies aktuell verhindern könnten. Zwar werden die internationalen Menschenrechtspakte ganz überwiegend so interpretiert, dass Staaten die Menschenrechte nicht nur gegenüber den in ihrer Hoheitsgewalt befindlichen Menschen achten müssen[3]. Insbesondere von den USA wird dieser Grundsatz der extraterritorialen Wirkung von Menschenrechten jedoch nicht anerkannt. Sie fühlen sich zur Achtung der Menschenrechte nur gegenüber ihren eigenen Bürgern sowie Personen auf ihrem Hoheitsgebiet verpflichtet.

DAS INTERNET ALS NICHT-STAATLICHER RAUM

Ihrer ursprünglichen Zielsetzung zufolge sollten die Menschenrechte den Einzelnen vor der staatlichen Übermacht schützen. Im Internet liegt die Macht jedoch in erster Linie in privater Hand. Der Zugang zum Internet erfolgt in den meisten Fällen über private Anbieter. Dienste, Applikationen und Inhalte werden im Netz zu einem großen Teil von Privaten zur Verfügung gestellt, und auch die Verwaltungsstrukturen des Internet (Vergabe von IP-Adressen und Domains, Festlegung technischer Standards) sind überwiegend staatsfern organisiert. Die klassischen Abwehrrechte gegen den Staat nützen dem Einzelnen daher nur wenig, wenn er sich in diesen Strukturen bewegt.

Zwar hat der Staat gegenüber dem Einzelnen auch Schutzpflichten hinsichtlich des Handelns Dritter (s. o.). Das Schutzniveau, das er dabei sicherstellen muss, ist allerdings deutlich geringer als dasjenige, das er bei eigenem Handeln zu wahren hat. Zudem bestehen diese Pflichten nur unter engen Voraussetzungen und belassen dem Staat einen erheblichen Handlungsspielraum. Dies schlägt sich für den Einzelnen in einem gegenüber den Menschenrechten in der Offline-Welt deutlich reduzierten Schutzumfang nieder.

Ein umfassender Menschenrechtsschutz wird im Internet daher nur zu realisieren sein, wenn sich entweder die Staaten in ihrer Gesamtheit ihrer gestiegenen Schutzverantwortung bewusst werden oder die privaten Akteure selbst bereits sind, in rechtlich verbindlicher Form Verantwortung für die Menschenrechte im Netz zu übernehmen.

Dabei kann eine verstärkte Konkretisierung staatlicher Schutzpflichten selbstverständlich nicht bedeuten, dass die Staaten jede Detailfrage im Internet regeln: Privaten Akteuren zu strikte Vorgaben zu machen, würde dem Abwehrgedanken der Menschenrechte zuwiderlaufen und kann die Wahrnehmung von Menschenrechten letztlich sogar beschränken. Gleichzeitig muss aber sichergestellt sein, dass der Menschenrechtsschutz durch die Verlagerung relevanter Tätigkeiten vom öffentlichen in den privat organisierten Raum Internet nicht ausgehöhlt werden kann. Völlig freiwillige und letztlich nicht bindende Selbstregulierungsansätze genügen dem Schutzziel daher ebensowenig, da sie von den beteiligten Unternehmen und Organisationen sanktionslos unterlaufen werden könnten. Erfolgversprechender erscheinen Konzepte einer „regulierten Selbstregulierung“ oder Ko-Regulierung von Staat und Privatsektor, wie sie bereits in vielen europäischen Staaten auf ein anderes Medium, den Rundfunk, Anwendung finden.

DER MULTI-STAKEHOLDER-ANSATZ IN DER INTERNET GOVERNANCE

Als Folge der Weltgipfel zur Informationsgesellschaft (World Summit on the Information Society, WSIS) 2003 in Genf und 2005 in Tunis setzte der UN-Generalsekretär auf Beschluss der Staatengemeinschaft 2006 das Internet Governance Forum (IGF) ein. Das IGF fungiert als Plattform für den vom WSIS beschlossenen „multi-stakeholder policy dialogue“ zu Fragen der Internet Governance und soll alle Interessenvertreter – Staaten, Wirtschaft, Zivilgesellschaft, Wissenschaft und technische Gemeinschaft – auf gleichbe-rechtigter Basis zusammenbringen. Das IGF kann selbst keine völkerrechtlich verbindlichen Beschlüsse fassen, gilt aber als das wichtigste ständige Forum zu diesem Themengebiet. Der WSIS-Prozess soll insgesamt 2015 durch die UN-Generalversammlung überprüft werden.

Innerhalb des IGF gründete sich 2008 die Dynamic Coalition on Internet

Internet Governance

Die vom WSIS 2003 eingesetzte Working Group on Internet Governance erarbeitete die folgende Arbeitsdefinition für den Begriff der Internet Governance:
„Internet Governance ist die Entwicklung und Anwendung durch Regierungen, den Privatsektor und die Zivilgesellschaft, in ihren jeweiligen Rollen, von gemeinsamen Prinzipien, Normen, Regeln, Vorgehensweisen zur Entscheidungsfindung und Programmen, die die Weiterentwicklung und die Nutzung des Internets beeinflussen.“

Rights and Principles (IRP Coalition), ein offenes Netzwerk mit dem Ziel, das Internet mit den Menschenrechten in Einklang zu bringen. Die IRP Coalition veröffentlichte 2011 die erste Fassung der Charter of Human Rights and Principles for the Internet (Internet Rights and Principles Charter, IRPC[4]), einer Art Rahmenwerk für das Internet, das auf den international anerkannten Menschenrechten basiert, diese jedoch für den Internet-Kontext teils konkretisiert, teils fortentwickelt. So finden sich neben internetspezifischen Ausformulierungen klassischer Menschenrechte wie der Meinungs- und Informationsfreiheit, dem Recht auf Privatsphäre und dem Recht auf Arbeit auch bisher nicht explizit als solche anerkannte Menschenrechte wie das Recht auf Internetzugang, das Recht auf digitalen Datenschutz und das Recht auf Verbraucherschutz.

Unter dem Eindruck der Enthüllungen Edward Snowdens über Massenüberwachungsprogramme und massive Eingriffe in die Integrität des Internet durch die Geheimdienste der „Five Eyes"-Staaten (USA, Großbritannien, Kanada, Australien und Neuseeland) fand am 23./24. April 2014 auf Einladung Brasiliens ein „Global Multistakeholder Meeting on the Future of Internet Governance" (Kurzbezeichnung: NETmundial) in São Paulo statt. Auf der Konferenz wurde auch über menschenrechtliche Standards für das Internet debattiert. Das Schlussdokument (NETmundial Multistakeholder Statement[5]) enthält unter anderem Empfehlungen für die Formulierung von Menschenrechten im Internet, die wiederum wesentlich auf der IRPC basieren.

Weder das IGF noch NETmundial treffen völkerrechtlich verbindliche Entscheidungen. Auch regionale Initiativen, die auf den Arbeiten zur IRPC gründen – etwa der Leitfaden für Menschenrechte von Internetnutzern des Europarates[6] oder die Afrikanische Erklärung der Internetrechte und -freiheiten[7] – entfalten keine unmittelbare Rechtswirkung (wenngleich aus ihnen die Rechtsauffassung der beschlussfassenden Staaten ersichtlich wird). Diese Rolle verbleibt nach wie vor bei den dazu legitimierten Akteuren, den Staaten. Als primäre Garanten der Menschenrechte ist es daher auch ihre Aufgabe, die grundlegenden Rahmenbedingungen für das Handeln von Unternehmen, Organisationen und Einzelpersonen im Internet mit letzter Verbindlichkeit zu setzen und zu gewährleisten. In einigen Staaten wurde bereits damit begonnen, die Idee eines rechtlichen Rahmens für die Menschenrechte im Internet auf nationaler Ebene umzusetzen, so etwa in Brasilien mit dem Marco Civil da Internet und in Neuseeland mit dem Vorschlag einer Internet Rights and Freedoms Bill.

EIN INTERNATIONALER RAHMEN FÜR DIE MENSCHENRECHTE IM INTERNET!

Dennoch haftet rein nationalen Initiativen das eingangs geschilderte Problem an, dass der Einfluss staatlicher Hoheitsmacht in vielen Fällen auf das eigene Staatsgebiet beschränkt ist. Ein umfassender und einheitlicher Schutz der Menschenrechte im weltumspannenden Internet lässt sich daher effektiv nur durch einen völkerrechtlichen Vertrag gewährleisten, dessen Norminhalte von einer internationalen (oder durch diesen Vertrag errichteten supranationalen) Institution angewandt werden, der Aufsichtsbefugnisse und im Falle eines

Verstoßes Sanktionsmechanismen zur Verfügung stehen. Entsprechend der herausragenden Rolle transnationaler Internetkonzerne und für das Funktionieren wesentlicher privatrechtlich verfasster Organisationen wie der Internet Corporation for Assigned Names and Numbers (ICANN) oder des Internet Architecture Board (IAB) sollte das internationale Abkommen aber auch diesen Strukturen zum Beitritt offenstehen. Ihre Einbindung würde dem Rechtsrahmen zu zusätzlicher Legitimität verhelfen und könnte gewährleisten, dass ein einheitlicher Menschenrechtsstandard von allen relevanten Akteuren in gleichem Maße als verbindlich anerkannt und beachtet wird.

Sebastian Schweda
schweda@amnesty-digital.de
PGP: 492F CF12 B7DD B3D3 C603 A0C9 7514 DA29 CBAE F03C

[1] United Nations Human Rights Council, The promotion, protection and enjoyment of human rights on the Internet, A/HRC/20/L.13, angenommen am 5.7.2014, http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement

[2] United Nations General Assembly, The right to privacy in the digital age, A/RES/68/167, abgedruckt in A/68/456/Add.2, 10.12.2013 (angenommen am 18.12.2013), https://www.un.org/ga/search/view_doc.asp?symbol=A/68/456/Add.2, S. 139 f.

[3] Auch die Erklärung des Ministerkomitees des Europarates zu den vom Europarat veröffentlichten Prinzipien zur Internet Governance weist darauf hin, dass Staaten keine Handlungen vornehmen sollten, die unmittelbar oder mittelbar Personen oder Einrichtungen außerhalb ihres eigenen Hoheitsgebietes schaden würden.

[4] Die aktuelle Version 1.1 der Charta vom 29.5.2014 ist auf Deutsch abrufbar unter: http://internetrightsandprinciples.org/site/wp-content/uploads/2014/06/IRPC_booklet_29May2014_German.pdf

[5] http://netmundial.br/netmundial-multistakeholder-statement

[6] Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users, 16. April 2014, https://wcd.coe.int/ViewDoc.jsp?id=2184807

[7] African Declaration on Internet Rights and Freedoms, http://africaninternetrights.org/declaration/

MITARBEITEN - WIE GEHT DAS?

Die Themenkoordinationsgruppe „Menschenrechte im digitalen Zeitalter“ steht jedem offen: Interessierte sind bei uns jederzeit herzlich willkommen! Wer hineinschnuppern oder gleich mitarbeiten will, den laden wir ein, mit uns in Kontakt zu treten. Wir suchen engagierte Mitstreiter/innen, die Interesse an der Frage haben, wie sich die technische Entwicklung auf die Durchsetzung der Menschenrechte auswirkt. Idealerweise – aber nicht zwingend! – bringt Ihr bereits grundlegende thematische Kenntnisse mit, empfehlenswert ist außerdem ein grundlegendes Wissen über die Arbeit von Amnesty International.

WIE SIEHT UNSERE ARBEIT AUS?

Als Themenkoordinationsgruppe „Menschenrechte im digitalen Zeitalter“ haben wir ein breites Aufgabenfeld. Wir erarbeiten Positionen und beteiligen uns an der Strategiefindung von Amnesty International – sowohl in der deutschen Sektion als auch auf internationaler Ebene. Darüber hinaus sind wir für die Entwicklung und Durchführung von Kampagnen und Aktionen zuständig. Wir betreiben Lobbyarbeit sowie Presse- und Öffentlichkeitsarbeit rund um das Thema „Menschenrechte im digitalen Zeitalter“. Außerdem betreuen wir Gruppen, die zu unserem Thema arbeiten, erstellen Infomaterial und sind Ansprechpartner bei allem, was unser Thema betrifft.

Da unsere Mitglieder über ganz Deutschland verteilt sind, läuft ein Großteil unserer Kommunikation virtuell ab (durch Mailinglisten und Telefonkonferenzen). Ergänzt wird dies durch regelmäßige „reale“ Treffen.

Wenn wir Euer Interesse geweckt haben, schreibt uns eine E-Mail an:
digital@amnesty.de

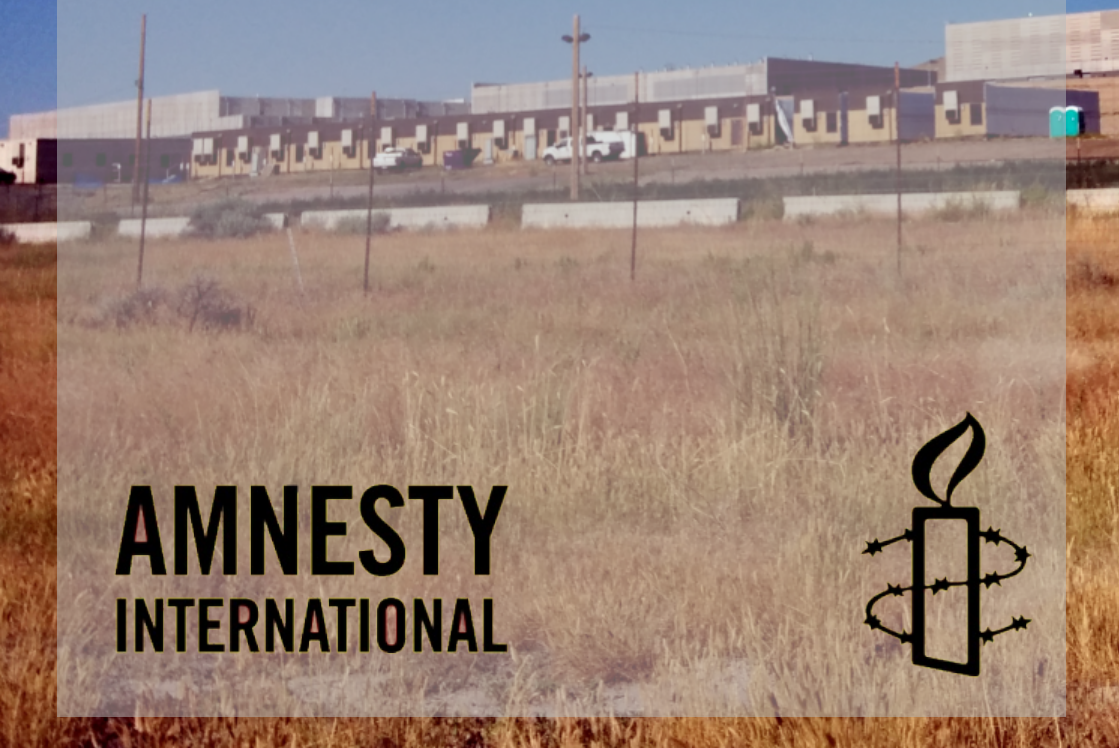
Wir freuen uns auf Euch!
Eure Themenkoordinationsgruppe Menschenrechte im digitalen Zeitalter

AMNESTY INTERNATIONAL Sektion der Bundesrepublik Deutschland e.V.
Themenkoordinationsgruppe Menschenrechte im Digitalen Zeitalter
Zinnowitzer Straße 8 . 10115 Berlin
E: digital@amnesty.de . W: https://amnesty-digital.de

SPENDENKONTO 80 90 100 . Bank für Sozialwirtschaft . BLZ 370 205 00
IBAN: DE 233 702050 0000 8090100 . BIC: BFS WDE 33XXX
Verwendungszweck: 2923

Fingerprints CAcert-Rootzertifikate (SHA-1) für die S/MIME-Zertifikate der deutschen Sektion:
- Class 1: 13:5C:EC:36:F4:9C:B8:E9:3B:1A:B2:70:CD:80:88:46:76:CE:8F:33
- Class 3: AD:7C:3F:64:FC:44:39:FE:F4:E9:0B:E8:F4:7C:6C:FA:8A:AD:FD:CE

https://amnesty-digital.de



AMNESTY
INTERNATIONAL