GEZIELTE DIGITALE ÜBERWACHUNG VON MENSCHENRECHTLER_INNEN

Wie die Überwachungsindustrie die Menschen bedroht,
die unsere Rechte verteidigen.

AMNESTY INTERNATIONAL

INHALT

Erstveröffentlichung: 2019
durch Amnesty International Ltd
Peter Benenson House, 1 Easton Street London WC1X 0DW, UK
Index: ACT 30/1385/2019
Originalsprache: Englisch

GLOSSAR

BEGRIFF	BESCHREIBUNG
DIGITALE MASSENÜBERWACHUNG	Hierbei handelt es sich um die Praxis der Überwachung einer gesamten Bevölkerung oder eines signifikanten Teils davon durch digitale Mittel. Dies geschieht vor allem durch die Überwachung der elektronischen Kommunikation, durch Digitalkameras, durch den Einsatz von Gesichtserkennungstechnologie, durch das Sammeln von Informationen in biometrischen Datenbanken oder auch durch Drohnen. Obwohl die digitale Massenüberwachung gewöhnlich von Regierungen durchgeführt wird, kann sie auch von privaten Unternehmen im Auftrag von Regierungen oder auf eigenes Betreiben vorgenommen werden.
GEZIELTE DIGITALE ÜBERWACHUNG	Im Gegensatz dazu besteht die gezielte digitale Überwachung in der Überwachung oder Ausspähung bestimmter Personen und/oder Organisationen, die für die Behörden von Interesse sein können, mittels digitaler Technologie. Zur gezielten digitalen Überwachung kann auch die Kompromittierung von Geräten durch die Installation von Malware und Spyware oder die Kompromittierung digitaler Kommunikation durch Phishing Kampagnen gehören.
PHISHING	Eine Form des Cyber-Angriffs, bei dem gefälschte Anmeldeseiten tatsächlicher Dienste (wie Gmail oder Facebook) erstellt und meist durch das Versenden gefälschter Links an die Zielpersonen verbreitet werden, um an deren Benutzernamen und Passwörter zu gelangen.
MALWARE	Bösartige Software, die zur unbemerkten Installation auf dem Computer oder Smartphone einer Zielperson gedacht ist, um an deren persönliche Daten zu gelangen oder andere Formen von Betrug durchzuführen oder Geräte zu beschädigen und/oder deren Betrieb zu stören.
SPYWARE	Eine besondere Art von Malware, die darauf ausgelegt ist, den Computer oder das Telefon des Opfers heimlich auszuspionieren, dessen Kommunikation kontinuierlich zu überwachen und private Informationen und Dateien zu stehlen.
MENSCHENRECHTSVERTEIDIGER_IN	Jemand, der sich einzeln oder mit anderen für den Schutz und/oder die Förderung der Menschenrechte auf lokaler, nationaler, regionaler oder internationaler Ebene einsetzt, ohne Hass, Diskriminierung oder Gewalt anzuwenden oder zu befürworten.

1. DIE FOLGEN GEZIELTER DIGITALER ÜBERWACHUNG

„Weltweit werden Konflikte und Angst immer häufiger dazu benutzt, Gewalt zu verbreiten, die Zivilgesellschaft zu spalten und sie zum Schweigen zu bringen. Staaten wenden sich ab von Solidarität und Gerechtigkeit. Einige Politiker_innen gefallen sich sogar darin, die Menschenrechte zu verletzen, und führen offen Krieg gegen jene, die es wagen, für das einzustehen, was richtig ist. Dies hat zur Folge, dass die Menschenrechtsbewegung mittlerweile mit Verfolgung und Repression in bisher ungeahntem Ausmaß konfrontiert ist.“

Vom weltweiten Gipfeltreffen der Menschenrechtsverteidiger_innen, 2018 in Paris[1]

Zu den Taktiken und Methoden der Repression, die nahezu ungestraft gegen Menschenrechtsverteidiger_innen eingesetzt werden, gehören persönliche Angriffe wie Drohungen, Verleumdungskampagnen, Kriminalisierung, Schläge, Tötungen und das Verschwindenlassen. Darüber hinaus haben verschiedene Staaten in Gesetz und Praxis eine Fülle von Einschränkungen der Rechte auf Versammlungs- und Vereinigungsfreiheit, auf freie Meinungsäußerung und auf Bewegungsfreiheit eingeführt.

Menschenrechtsverteidiger_innen, die mit Ungleichheit, Ausgrenzung und Diskriminierung konfrontiert sind, darunter Frauen, LGBTI, Migrant_innen, Schwarze und indigene Gemeinschaften, sind doppelt gefährdet, weil sie nicht nur wegen ihres Engagements angegriffen werden, sondern auch aufgrund dessen, wer sie sind. Die Angriffe, denen sie ausgesetzt sind, haben ganz spezielle Merkmale und besondere Folgen, dazu gehört auch geschlechtsspezifische Gewalt. Auch werden sie häufig begleitet von struktureller Ungleichheit und dem systematischen Ausschluss der Betroffenen bei der Verteilung von Ressourcen und von einflussreichen Positionen.[2]

Diese Taktiken haben eine abschreckende Wirkung auf Menschenrechtsverteidiger_innen und hindern sie daran, abweichende Meinungen zu vertreten, Verstöße aufzudecken und sich für Veränderungen einzusetzen. Immer häufiger beobachtet Amnesty International, dass Staaten Methoden voneinander abschauen und Tools und Technologien für eine Strategie der Kontrolle und Repression importieren.

Eine Taktik, die dabei von Regierungen weltweit besonders häufig eingesetzt wird, ist die der Überwachung, sei es digital oder in anderer Form. Gegenwärtig erfolgt die digitale Überwachung in einem gesellschaftlichen Umfeld, in dem der Einsatz von Technologie durch Polizei und Strafverfolgungsbehörden in den letzten Jahren exponentiell zugenommen hat. Im Namen der Bekämpfung des Terrorismus oder der Aufrechterhaltung von Recht und Ordnung wenden Regierungen eine Reihe von Überwachungsmaßnahmen an, die in die Privatsphäre von Menschen auf der ganzen Welt eingreifen.

Dazu gehören auch Maßnahmen zur digitalen Massenüberwachung und zur gezielten digitalen Überwachung. Dies geschieht vor allem durch die Überwachung der elektronischen Kommunikation, durch Überwachungskameras, durch den Einsatz von Gesichtserkennungstechnologie, durch das Sammeln von Informationen mittels biometrischer Datenbanken oder auch durch Drohnen. Länder wie Großbritannien,[3] China,[4] und die USA[5] führen Berichten zufolge Maßnahmen zur digitalen Massenüberwachung durch.

Bei der gezielten digitalen Überwachung wiederum kommen Technologien zum Einsatz, die es ermöglichen, bestimmte Personen ins Visier zu nehmen. Ihre Umsetzung erfolgt zum Beispiel durch das Abhören von Telefonen und durch digitale Technologie. Zur gezielten digitalen Überwachung kann auch die Kompromittierung von Geräten durch die Installation von Malware und Spyware oder die Kompromittierung digitaler Kommunikation durch Phishing-Kampagnen gehören. So gibt es Berichte, dass die Polizei in Großbritannien Journalist_innen unter digitale Beobachtung stellt,[6] und in den Vereinigten Arabischen Emiraten soll die Regierung Spyware zum Aufspüren von Aktivist_innen eingesetzt haben.[7] Auch aus Kolumbien wird berichtet, dass die Polizei Radiojournalist_innen digital überwachen lässt,[8] und in Äthiopien setzte die vorherige Regierung elektronische Überwachungsmaßnahmen ein, um oppositionelle Aktivist_innen im In- und Ausland auszuspionieren.[9]

Mit dem Aufkommen neuer, noch ausgefeilterer Technologien, die weithin verfügbar sind, und Gesetzen, die die freie Meinungsäußerung im Internet einschränken und in die Privatsphäre im Internet eingreifen, ist die Bedrohung durch eine gezielte digitale Überwachung noch akuter geworden.

Länder wie Thailand[10] und Bangladesch[11] haben Gesetze verabschiedet, die eine Ausweitung der elektronischen Überwachung vorsehen und Regierungen Befugnisse zum Ausspionieren elektronischer Kommunikation geben. Seit kurzem zeichnet sich ein deutlicher Trend ab, nach dem Regierungen zunehmend auf die private digitale Überwachungsindustrie zurückgreifen, um die Entwicklung von Technologien zur gezielten digitalen Überwachung in Auftrag zu geben. Diese Technologien werden dann missbraucht, um Menschenrechtsaktivist_innen rechtswidrig ins Visier zu nehmen und unter Beobachtung zu stellen. In diesem Markt tätige Unternehmen spielen mittlerweile eine gefährliche Rolle. Sie sind verantwortlich für die Entstehung neuer Unterdrückungsinstrumente und für die zunehmende Bedrohung derjenigen, die unsere Menschenrechte verteidigen.

Über diese Branche, die trotz wiederholter Forderungen nach mehr Transparenz nach wie vor im Dunkeln arbeitet, ist nur wenig bekannt. Angesichts der unzureichenden regulatorischen und rechtlichen Aufsicht können diese Unternehmen ihre Technologie frei an Länder verkaufen, in denen die Menschenrechte nicht geschützt oder respektiert werden und die ihrerseits die Technologie nutzen, um jene zu verfolgen und zu überwachen, die die Menschenrechte verteidigen.

2. GEZIELTE DIGITALE ÜBERWACHUNG LÄSST KRITISCHE STIMMEN VERSTUMMEN

Der gezielte Einsatz digitaler Überwachungstechnologien gegen Menschenrechtsverteidiger_innen wegen ihrer Arbeit ist nach internationalen Menschenrechtsstandards eindeutig illegal. Die rechtswidrige Überwachung verstößt gegen das Recht auf Privatsphäre und beeinträchtigt die Rechte auf freie Meinungsäußerung, auf Vereinigungs und Versammlungsfreiheit. Diese Rechte sind sowohl durch die Allgemeine Erklärung der Menschenrechte als auch durch den Internationalen Pakt über bürgerliche und politische Rechte (IPbpR) geschützt. Der Pakt verteidigt das Recht, Meinungen ohne Einmischung vertreten zu dürfen,[12] und schützt vor willkürlichen und rechtswidrigen Eingriffen in die Privatsphäre.[13] Laut Völkerrecht und internationalen Standards muss jeder Eingriff des Staates in das Recht auf Privatsphäre auf einem Gesetz basieren und notwendig und verhältnismäßig zum Erreichen eines legitimen Ziels sein. Darüber hinaus müssen Staaten dafür Sorge tragen, dass Personen, deren Rechte verletzt wurden, Zugang zu Rechtsmitteln haben.[14]

Oft ist es für Menschenrechtsverteidiger_innen praktisch unmöglich nachzuweisen, dass sie überwacht werden, sei es aufgrund technischer Hindernisse oder weil die Überwachung verdeckt erfolgt.[15] Doch auch in Fällen, in denen der Nachweis eines Überwachungsversuchs bzw. einer aktiven Infizierung nicht möglich ist,[16] kann schon die Tatsache, mit der ständigen Gefahr einer möglichen Überwachung leben zu müssen, eine Menschenrechtsverletzung darstellen.[17] Unabhängig davon, ob der Überwachungsversuch erfolgreich ist oder nicht, schürt ein gezieltes Vorgehen gegen Menschenrechtsaktivist_innen Angst und beeinträchtigt ihre Möglichkeiten, ihrer Arbeit ohne unrechtmäßige Störungen weiter nachzugehen.[18] In vielen Fällen führt dies dazu, dass diejenigen, die die Menschenrechte verteidigen, sich selbst zensieren und ihre Rechte auf Meinungs-, Vereinigungs- und Versammlungsfreiheit nicht wahrnehmen. Erschwerend kommt hinzu, dass sich Menschenrechtsverteidiger_innen gegen böswillige Strafverfolgung zur Wehr setzen müssen. Die Strafverfolgung wird mithilfe von Informationen, die durch die Überwachung gewonnen, missbraucht und manipuliert werden, aufgenommen. In der Folge reiben sich die betroffenen Menschenrechtsverteidiger_innen in Gerichtsverfahren auf, statt ihre Energie und Ressourcen für ihre eigentliche Tätigkeit einsetzen zu können.[19] Die Bedrohung durch Überwachung kann sich nachteilig auf die psychische Gesundheit von Menschenrechtsverteidiger_innen auswirken. Zudem können Informationen dazu verwendet werden, in der Öffentlichkeit Details preiszugeben, die sie persönlichen Angriffen und Verleumdungskampagnen aussetzen. All dies hat nachteilige Auswirkungen auf Gemeinschaften und Bevölkerungsgruppen, für deren Rechte die Menschenrechtsaktivist_innen kämpfen.

In Aserbaidschan ist es beispielsweise für Menschenrechtsaktivist_innen, die unter der ständigen Bedrohung durch Überwachung stehen und aus Angst vor Angriffen ihr Zuhause verlassen, schwierig, mit ihren Angehörigen daheim zu kommunizieren, da sie befürchten, dass auch sie ins Visier genommen werden.[20] In Usbekistan sind Personen, die von Cyberangriffen betroffen waren und ihr Zuhause verlassen haben, nach wie vor Ziel digitaler Überwachungskampagnen.[21] Dies bedeutet effektiv, dass Menschenrechtsverteidiger_innen in Angst leben und das Gefühl haben, sich ständig umschauen zu müssen, wohin sie auch gehen. Überwachung ist eine höchst effektive Methode, um Personen, die sich für die Menschenrechte einzusetzen, zu entmutigen oder sie daran zu hindern, abweichende Meinungen zu äußern oder Menschenrechtsverletzungen offenzulegen.[22]

3. FALLSTUDIE:

CYBERANGRIFFE GEGEN DIE PAKISTANISCHE MENSCHENRECHTS-AKTIVISTIN DIEP SAEEDA

„Jedes Mal, wenn ich nun eine E-Mail öffne, bin ich nervös. Es ist mittlerweile so schlimm, dass ich meine Arbeit nicht mehr machen kann – meine soziale Arbeit leidet darunter.“ Diep Saeeda [23]

2018 setzte sich Diep Saeeda, eine prominente pakistanische Menschenrechtsverteidigerin, aktiv dafür ein, die Verantwortlichen für das Verschwindenlassen von Raza Khan, ebenfalls Menschenrechtsverteidiger, zur Rechenschaft zu ziehen. In dieser Zeit wurde Diep Saeeda zum Ziel einer Cyberangriffskampagne. Eine Facebook-Nutzerin, die sich als afghanische Frau namens Sana Halimi ausgab, die in Dubai lebe und für die UN arbeite, kontaktierte Diep Saeeda mehrmals über die Messenger-Anwendung von Facebook. Sie behauptete, Informationen über Raza Khan zu haben. Diese Nachrichten enthielten Dateianhänge, die mit einer Malware namens „StealthAgent“ infiziert waren. Das Öffnen dieser Anhänge hätte dazu geführt, dass die Mobilgeräte von Diep Saeeda infiziert worden wären. Amnesty International geht davon aus, dass es sich um ein fingiertes Facebook-Profil handelte. Diep Saeeda wurde von „Sana Halimi“ nämlich auch dazu gebracht, ihre E-Mail-Adresse preiszugeben, woraufhin sie E-Mails erhielt, die mit einer Windows-Spyware namens „Crimson RAT“ infiziert waren.

Diep Saeeda erhielt auch E-Mails, die vermeintlich vom Personal des Ministerpräsidenten von Punjab versendet wurden und die falsche Informationen über ein angeblich bevorstehendes Treffen des regionalen Bildungsministeriums und des Institute for Peace and Secular Studies, bei dem Diep Saeeda arbeitet, enthielten. Hinzu kamen E-Mails, die von angeblichen Studierenden stammten, und in denen sie um Rat oder Nachhilfe gebeten wurde. Aus den Recherchen von Amnesty International geht hervor, dass in Pakistan bereits zahlreiche weitere Menschenrechtsverteidiger_innen auf diese Weise ins Visier genommen wurden.

Durch die Cyberangriffe wurde es für Diep Saeeda schwer, ihrer Arbeit nachzugehen, und sie lebte zunehmend in Angst. Sie begann, auch E-Mails und E-Mail-Anhängen von Familienmitgliedern zu misstrauen, da sie befürchtete, jemand könne sich für sie ausgeben.

4. DIE PRIVATE DIGITALE ÜBERWACHUNGSINDUSTRIE

Eine Reihe von Regierungen kauft digitale Überwachungsinstrumente – insbesondere Spyware – von kommerziellen Überwachungsfirmen. Diese werden dann zur Verfolgung, Überwachung und Einschüchterung von Menschenrechtsverteidiger_innen und anderen Personen mit abweichender Meinung eingesetzt. Sowohl die Regierungen als auch die Unternehmen, die ihnen diese Technologie verkaufen, behaupten, sie würde allein für rechtmäßige Zwecke wie die Überwachung und Verfolgung von Terrorist_innen und Kriminellen eingesetzt. Die sich häufenden Beweise für ihre missbräuchliche Verwendung erzählen jedoch eine andere Geschichte. Zivilgesellschaftliche Organisationen wie Amnesty International haben gezielte Kampagnen gegen Personen aufgedeckt, die die Menschenrechte verteidigen, und das mit Technologien, die meist von diesen Überwachungsfirmen vermarktet werden.

Während Regierungen schon seit einiger Zeit Spyware entwickeln, ist kommerzielle Spyware relativ neu, aber ebenso invasiv und raffiniert.[24] Zu den wichtigsten Unternehmen in dieser verschwiegenen und höchst lukrativen Branche gehören die NSO Group in Israel und Luxemburg[25] sowie Finfisher in Großbritannien und Deutschland.[26]

Citizen Lab zufolge scheint allein eines davon, die NSO Group, hinter bekannten gezielten Überwachungsangriffen in mindestens 45 Ländern zu stecken.[27] Im Juni 2018 ging einem Mitarbeiter von Amnesty International eine böswillige WhatsApp-Nachricht mit Köderinhalten zu Saudi-Arabien sowie Links zu, über die mobile Spyware der NSO Group hätte installiert werden können.[28] Viele der Länder, die Überwachungstechnologie von diesen Unternehmen kaufen konnten, haben eine düstere Menschenrechtsbilanz. So wurde beispielsweise Software der NSO Group für Angriffe auf Menschenrechtsverteidiger_innen in Marokko,[29] Mexiko, Saudi-Arabien und den Vereinigten Arabischen Emiraten[30] eingesetzt.

Unternehmen wie die NSO Group müssen im Rahmen ihrer Sorgfaltspflicht nach den UN-Prinzipien für Wirtschaft und Menschenrechte geeignete Verfahren zur Gewährleistung der menschenrechtlichen Sorgfaltspflicht einsetzen, um zu verhindern, dass der Gebrauch ihrer Produkte die Menschenrechte verletzt, derartigen Missbrauch zu mindern und im Falle eines Missbrauchs wirksame Abhilfe zu leisten.[31] Darüber hinaus haben Staaten die Verantwortung, vor privaten Unternehmen zu schützen, die Menschenrechte verletzen, unabhängig davon, ob diese Verletzungen innerhalb oder außerhalb ihrer Grenzen stattfinden.

Diese im Verborgenen arbeitenden Unternehmen zur Rechenschaft zu ziehen, ist besonders schwierig. Sie verstecken sich häufig hinter Vorwänden wie „Sicherheitsbedenken“ oder „Vertraulichkeitsvereinbarungen“, um Informationen zu ihren Aktivitäten aus der Öffentlichkeit fernzuhalten. Über diese Unternehmen oder ihre Unternehmensstrukturen ist nur wenig bekannt. Viele von ihnen geben keine Informationen über Ausfuhrgenehmigungsverträge preis und haben entweder kein oder nur ein unzureichendes Verfahren zur Gewährleistung der menschenrechtlichen Sorgfaltspflicht und zur Wiedergutmachung im Missbrauchsfall. In Verbindung mit einer fehlenden regulatorischen Kontrolle und laschen Ausfuhrgenehmigungsverfahren auf nationaler wie auf internationaler Ebene ist es deshalb sehr schwierig geworden, Unternehmen dieser Branche zur Verantwortung zu ziehen.

So sind beispielsweise Instrumente wie das Wassenaar-Abkommen, eine multilaterale Vereinbarung über Exportkontrollen, darauf ausgerichtet, die Ausfuhrbestimmungen zwischen den Teilnehmerstaaten in Bezug auf Rüstungsgüter sowie Güter und Technologien mit doppeltem Verwendungszweck, die zur Entwicklung oder zum Ausbau militärischer Fähigkeiten beitragen, zu harmonisieren.[32] Das Abkommen mag zwar hilfreich sein, ist jedoch kein Forum, in dem es darum geht, Menschenrechtsprobleme zu mindern.

Auf nationaler Ebene, wie z. B. in Israel,[33] werden Ausfuhrgenehmigungen trotz menschenrechtlicher Bedenken meist erteilt, da strategische Erwägungen oft schwerer wiegen als menschenrechtliche Bedenken. Die Europäische Union verfügt zwar über klarere Bestimmungen hinsichtlich der Menschenrechte, aber dennoch erteilen die Mitgliedstaaten auch weiterhin Lizenzen für Überwachungstechnologie, und dies trotz Bedenken und Beweisen für frühere Missbrauchsfälle, die eigentlich zur Verweigerung von Ausfuhrgenehmigungen führen sollten.[34] Gleichzeitig wird die Fähigkeit von Unternehmen, ihren eigenen menschenrechtlichen Verpflichtungen in unterschiedlichen Rechtsräumen nachzukommen, durch Geheimhaltungsbestimmungen erschwert.

All dies sorgt für ein rechtliches und regulatorisches Vakuum, das den Verkauf und den Transfer von digitaler Überwachungstechnologie ohne angemessene Sicherheitsvorkehrungen erlaubt. Je länger sich diese Unternehmen und die Staaten, die Technologie von ihnen kaufen, der Kontrolle entziehen können, desto stärker wird der Handlungsspielraum für abweichende Meinungen und die Verteidigung der Menschenrechte eingeschränkt.

Wir müssen Überwachungsversuchen durch Staaten, die rechtswidrig durch Privatunternehmen hergestellte Technologie zur Überwachung von Menschenrechtsaktivist_innen einsetzen, dringend ein Ende setzen.

5. MENSCHENRECHTLICHE VERPFLICHTUNGEN VON STAATEN UND UNTERNEHMEN

Die Verpflichtungen zur Achtung und zum Schutz von Menschenrechtsverteidiger_innen sind in einer Reihe von Instrumenten auf internationaler, regionaler und nationaler Ebene festgehalten. Staaten sind verpflichtet, diese Standards zu wahren, um ein sicheres und förderliches Umfeld zu gewährleisten, in dem Menschenrechtsverteidiger_innen frei von der Angst vor Angriffen arbeiten und ihre wichtige Arbeit zum Schutz und zur Förderung aller Menschenrechte fortsetzen können.[35]

Die UN-Erklärung über Menschenrechtsverteidiger_innen (1998)[36] beruht auf bereits vorhandenen und bindenden internationalen Instrumenten. Die Erklärung bekräftigt das Recht, die Menschenrechte zu verteidigen, und legt die Verpflichtungen der Staaten hinsichtlich der besonderen Rolle und Situation von Menschenrechtsaktivist_innen fest. Sie definiert die damit verbundenen Verantwortlichkeiten und Pflichten der Staaten und macht deutlich, dass es die Staaten sind, die letztlich die Verantwortung dafür tragen, Menschenrechtsverteidiger_innen zu schützen, mutmaßliche Menschenrechtsverletzungen, die gegen sie begangen werden, zu verhindern und wirksam dagegen vorzugehen und dafür zu sorgen, dass sie ihre Arbeit in einem sicheren und förderlichen Umfeld verrichten können. Darüber hinaus hebt die Erklärung die entscheidende Rolle der Menschenrechtsverteidiger_innen bei der Durchsetzung der Menschenrechte sowie bei der Entwicklung und Diskussion neuer menschenrechtlicher Vorstellungen und Prinzipien und dem Einsatz für ihre Anerkennung hervor.

Nationalstaaten sind nach internationalen Menschenrechtsstandards verpflichtet, die Menschenrechte vor dem Missbrauch durch Dritte zu schützen. Dazu gehört auch die Verpflichtung, das Verhalten nichtstaatlicher Akteur_innen, die ihrer Kontrolle unterstehen, zu regulieren, um zu verhindern, dass sie Menschenrechtsverletzungen verursachen oder dazu beitragen, auch dann, wenn dies in anderen Ländern geschieht.

Wie in den UN-Leitprinzipien für Wirtschaft und Menschenrechte dargelegt,[37] haben auch Unternehmen eine Verantwortung für die Achtung der Menschenrechte, unabhängig davon, wo in der Welt sie tätig sind. So müssen Unternehmen den UN-Leitprinzipien zufolge proaktive Schritte unternehmen, um sicherzustellen, dass sie im Rahmen ihrer globalen Geschäftstätigkeit keine Menschenrechtsverletzungen verursachen oder dazu beitragen und dass sie auf Menschenrechtsverletzungen reagieren, wenn diese auftreten. Im Rahmen dieser Verantwortung sollten Unternehmen Verfahren zur Gewährleistung ihrer Sorgfaltspflicht auf dem Gebiet der Menschenrechte einsetzen, „um ihre nachteiligen menschenrechtlichen Auswirkungen zu ermitteln, zu verhüten und zu mildern und Rechenschaft darüber abzulegen, wie sie ihnen begegnen“.

Die unternehmerische Verantwortung für die Achtung der Menschenrechte besteht unabhängig von der Fähigkeit oder Bereitschaft eines Staates, seinen eigenen Menschenrechtsverpflichtungen nachzukommen, und geht über die Einhaltung nationaler Gesetze und Vorschriften zum Schutz der Menschenrechte hinaus. So wird in den Leitlinien zur Auslegung der UN-Leitprinzipien ausdrücklich darauf hingewiesen, dass ein Unternehmen zu einer Menschenrechtsverletzung beitragen kann, wenn es „Daten über die Nutzer von Internetdiensten einer Regierung zur Verfügung stellt, die diese Daten dazu verwendet, menschenrechtswidrig politische Dissidenten aufzuspüren und zu verfolgen“.[38]

Darüber hinaus ist es möglich, dass ein Unternehmen, das Technologie zur Überwachung verkauft, an jeder nachfolgenden Menschenrechtsverletzung, bei der diese Technologie zum Einsatz kommt, mitschuldig ist. Ein Expertengremium der Internationalen Juristenkommission (International Commission of Jurists – ICJ) hat die Frage der Mittäterschaft von Unternehmen an Menschenrechtsverletzungen eingehend untersucht und geklärt, woraus eine zivil- und strafrechtliche Haftung für eine solche Mittäterschaft entstehen könnte. Das ICJ-Gremium vertrat die Auffassung, dass eine hinreichend enge rechtliche Verbindung vorliegen könnte, wenn das Verhalten des Unternehmens den Missbrauch ermöglicht, verschlimmert oder erleichtert hat und das Unternehmen wusste oder eigentlich hätte wissen müssen, dass der Missbrauch stattfinden würde und dass im Wesentlichen ein Unternehmen den Missbrauch unter anderem durch die Bereitstellung von Waren oder Dienstleistungen ermöglichen, verschlimmern oder erleichtern könnte.[39]

6. EMPFEHLUNGEN

„Staaten sollten ein sofortiges Moratorium für die Ausfuhr, den Verkauf, die Weitergabe, die Nutzung oder die Wartung privat entwickelter Überwachungsinstrumente verhängen, bis eine menschenrechtskonforme Schutzregelung eingeführt wurde." David Kaye, UN-Sonderberichterstatter für Meinungsfreiheit [40]

Staaten tragen letztendlich die Verantwortung dafür, Menschenrechtsverteidiger_innen zu schützen, Menschenrechtsverletzungen gegen sie oder ihre Menschenrechtsarbeit zu verhindern und dem Vorwurf von Menschenrechtsverletzungen effektiv nachzugehen. Außerdem müssen sie gewährleisten, dass Menschenrechtsaktivist_innen ihre Arbeit in einem sicheren und förderlichen Umfeld verrichten können. Es bleibt noch viel zu tun, um all diejenigen, die ihre Stimme erheben und sich gegen Unrecht wehren, anzuerkennen und zu schützen, auch vor gezielter digitaler Überwachung.

6.1 STAATEN

Amnesty International fordert alle Staaten auf,

- ein Moratorium für den Verkauf und die Weitergabe von Überwachungstechnologie zu verhängen, bis ein angemessener regulatorischer Rahmen im Sinne der Menschenrechte geschaffen ist;

- Informationen zu allen bisherigen, aktuellen oder zukünftigen Verträgen mit privaten Überwachungsunternehmen dadurch offenzulegen, dass sie auf Informationsanfragen antworten oder proaktiv Informationen bereitstellen;

- Ausfuhrgenehmigungen zu verweigern, wenn ein substantielles Risiko besteht, dass der betreffende Export zur Verletzung von Menschenrechten genutzt werden könnte – sei es durch rechtswidrige Überwachung oder weil das Bestimmungsland über unzureichende rechtliche, verfahrenstechnische und technische Schutzvorkehrungen verfügt, um Missbrauch zu verhindern;

- dafür zu sorgen, dass alle entsprechenden Technologien vor der Weitergabe überprüft werden;

- für Transparenz hinsichtlich des Umfangs, der Art, des Werts und des Ziels von Überwachungsexporten zu sorgen;

- sicherzustellen, dass Verschlüsselungsprogramme und legitime digitale Sicherheitstools keinen Exportkontrollen unterworfen werden;

- nationale Gesetze zu implementieren, die der digitalen Überwachung Grenzen setzen, um zu gewährleisten, dass
  - Überwachung präzise formulierten und öffentlich zugänglichen Gesetzen unterliegt,
  - eine Überwachung sich nur gegen bestimmte Personen richtet, von einer kompetenten, unabhängigen und unparteiischen Justizbehörde autorisiert ist und Zeit, Art, Ort und Umfang der Überwachung begrenzt sind,
  - digitale Überwachung einer detaillierten Aufzeichnung unterliegt, dokumentierten rechtlichen Verfahren für eine richterliche Anordnung entspricht und die betroffenen Personen benachrichtigt werden, sobald dies möglich ist, ohne den Zweck der Überwachung zu gefährden;

- dafür zu sorgen, dass jegliche digitale Überwachung öffentlichen Kontrollmechanismen unterliegt, darunter
  - ein Genehmigungsverfahren,
  - öffentliche Bekanntmachungen und Konsultationen beim Erwerb neuer Überwachungstechnologie,
  - regelmäßige Veröffentlichungen von Berichten;

- angemessene Mechanismen für den innerstaatlichen Rechtsbehelf in Fällen rechtswidriger und/oder missbräuchlicher gezielter digitaler Überwachung zu gewährleisten.

6.2 UNTERNEHMEN

Amnesty International fordert Unternehmen auf,

- sich öffentlich zur Achtung der Menschenrechte sowie der Arbeit und Sicherheit von Menschenrechtsverteidiger_innen zu verpflichten;

- angemessene Verfahren zur Gewährleistung ihrer menschenrechtlichen Sorgfaltspflicht einzuführen, wie sie in internationalen Wirtschafts- und Menschenrechtsinstrumenten wie den UN-Leitprinzipien für Wirtschaft und Menschenrechte und den OECDRichtlinien für multinationale Unternehmen festgelegt sind, um sicherzustellen, dass ihre Aktivitäten oder die ihrer Tochtergesellschaften, Unterauftragnehmer_innen und Zulieferer_innen die Rechte von Menschenrechtsverteidiger_innen respektieren und ihre legitime Arbeit nicht behindern;

- im Rahmen ihrer Verantwortung zur Prüfung der Einhaltung der menschenrechtlichen Sorgfaltspflicht für alle vorgeschlagenen Weitergaben belastbare Risikobewertungen zu Menschenrechtsfragen durchzuführen, die wiederum von den Exportbehörden geprüft und veröffentlicht werden sollten;

- Transparenz bei Verkäufen und Verträgen zu gewährleisten;

- vor der Unterzeichnung von Verträgen in Ländern Konsultationen mit Menschen vor Ort durchzuführen;

- vertragliche Schutzmaßnahmen gegen Menschenrechtsverletzungen vorzusehen;

- Design- und Entwicklungsoptionen umzusetzen, die Menschenrechtsstandards berücksichtigen;

- für regelmäßige Audits der Prüfprozesse zu sorgen, deren Ergebnisse öffentlich bekannt gegeben werden;

- ein angemessenes Verfahren für die Meldung von Technologiemissbrauch sowie Beschwerdemechanismen einzurichten und

- solide Mechanismen für die Entschädigung von Personen, die Opfer unrechtmäßiger Überwachung geworden sind, oder andere Formen der Wiedergutmachung einzurichten.

6.3 INVESTOR_INNEN

Amnesty International fordert alle Investor_innen auf,

- darauf zu achten, dass sie durch ihre Investition in Überwachungsunternehmen nicht zu Menschenrechtsverletzungen beitragen. Zu diesem Zweck sollten sie eine angemessene Transparenz und die Einhaltung von Verfahren zur Gewährleistung ihrer menschenrechtlichen Sorgfaltspflicht von den Überwachungsunternehmen verlangen.

- Investor_innen sollten die jeweiligen oben genannten Empfehlungen den Überwachungsfirmen mitteilen, an denen sie beteiligt sind, und deren Umsetzung einfordern.

ANMERKUNGEN / QUELLEN

1 Siehe Website zum weltweiten Gipfeltreffen der Menschenrechtsverteidiger_innen 2018 „Human Rights Defenders World Summit 2018“ unter **https://hrdworldsummit.org/the-summit/#context**

2 Weitere Informationen finden Sie in den folgenden Berichten von Amnesty International: Human Rights Defenders under threat – A shrinking space for civil society (Index: ACT 30/6011/2017); Deadly but preventable attacks: Killings and enforced disappearances of those who defend human rights (Index ACT 30/7270/2019); Per Gesetz mundtot gemacht: Die weltweite Unterdrückung zivilgesellschaftlicher Organisationen (Index ACT 30/9647/2019) und Challenging power, fighting discrimination – A call to action to recognize and protect women human rights defenders (Index: ACT 30/1139/2019)

3 Amnesty International, Encryption: A Matter of Human Rights (Index: POL 40/3682/2016); Amnesty International UK, Campaigners win vital battle against UK mass surveillance at European Court of Human Rights, **www.amnesty.org.uk/press-releases/campaigners-win-vital-battle-against-uk-mass-surveillance-european-court-human**; The UK government has been spying on Amnesty – so we're going to court, **www.amnesty.org.uk/blogs/ether/uk- government-spying-amnesty-mass-surveillance-court**

4 Informationen zu den verschiedenen Massenüberwachungsprogrammen in China finden Sie unter **www.hrw.org/tag/mass-surveillance-china**

5 Amnesty International, Encryption: A Matter of Human Rights (Index: POL 40/3682/2016)

6 Dominic Ponsford, „Surveillance court says Met grabs of Sun reports' call records 'not compatible' with human rights law“, 17. Dezember 2015, **www.pressgazette.co.uk/surveillance-court-says-met-was-right-grab-sun-journalists- call-records-hunt-plebgate-sources/**

7 Citizen Lab, „The Million Dollar Dissident NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender“, 2016, **https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/**

8 Komitee zum Schutz von Journalisten, „Claims police spied on two journalists revive surveillance fears of Colombia's press“, 2016, **https://cpj.org/blog/2016/02/claims-police-spied-on-two-journalists-revive-surv.php**

9 Amnesty International, Encryption: A Matter of Human Rights (Index: POL 40/3682/2016)

10 Tech Crunch, „Thailand passes controversial cybersecurity law that could enable government surveillance“, 28. Februar 2019, **https://techcrunch.com/2019/02/28/thailand-passes-controversial-cybersecurity-law/** und Reuters, “Thailand defends cybersecurity law amid concerns over rights abuse”, 1 Mar 2019, **https://www.reuters.com/article/us-thailand-cyber/thailand-defends-cybersecurity-law-amid-concerns-over-rights-abuse-idUSKCN1QI4KA**

11 Amnesty International „Bangladesh: New Digital Security Act is attack on freedom of expression“, November 2018, **www.amnesty.org/en/latest/news/2018/11/bangladesh-muzzling-dissent-online/**

12 Artikel 19, Internationaler Pakt über bürgerliche und politische Rechte

13 Artikel 17, Internationaler Pakt über bürgerliche und politische Rechte

14 Artikel 2(3), Internationaler Pakt über bürgerliche und politische Rechte

15 Amnesty International, Human Rights Defenders Under Threat - A Shrinking Space for Civil Society (Index: ACT 30/6011/2017)

16 Der Versuch einer Überwachung kann auf verschiedene Weise erfolgen, beispielsweise durch das Versenden bösartiger Links, die Spyware enthalten, oder durch andere Methoden. Diese Versuche können gelingen oder auch fehlschlagen. Sind sie erfolgreich, sind die Geräte des Nutzers möglicherweise infiziert und gefährdet.

17 Amnesty International, A Dangerous Alliance: Governments Collaborate with Surveillance Companies to Shrink the Space for Human Rights Work, (Blog, 16. August 2019)

18 Global Justice Clinic, NYU School of Law, Attempted digital surveillance as a completed human rights violation: Why targeting human rights defenders infringes on rights. Submission to the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 1. März 2019, **https://chrgj.org/wp- content/uploads/2019/05/190301-GJC-Submission-on-Surveillance-Software.pdf**

19 Amnesty International Per Gesetz mundtot gemacht: Die weltweite Unterdrückung zivilgesellschaftlicher Organisationen (Index: ACT 30/9647/2019)

20 Amnesty International, False Friends: How Fake Accounts and Crude Malware Targeted Dissidents in Azerbaijan (Blog, 9. März 2017)

21 Amnesty International, „We Will Find You Anywhere“ - The Global Shadow of Uzbekistani Surveillance (Index: EUR 62/5974/2017)

22 Amnesty International, Human Rights Defenders Under Threat - A Shrinking Space for Civil Society (Index: ACT 30/6011/2017)

23 Amnesty International, Pakistan: Human Rights Under Surveillance (Index: ASA 33/8366/2018)

24 Just Security, „CTRL+HALT+Defeat: State-sponsored Surveillance and the suppression of Dissent“, von Julie Bloch, Sukti Dhital, Rashmika Nedungadi und Nikki Reisch, 15. Mai 2019, **www.justsecurity.org/64095/ctrlhaltdefeat-state- sponsored-surveillance-and-the-suppression-of-dissent/**

25 Business and Human Rights Resource Centre, „Amnesty backs legal action against Israel firm NSO group over spyware used against human rights defenders“, Mai 2019, **www.business-humanrights.org/en/amnesty-backs-legal-action-against-israeli-firm-nso-group-over-spyware-use-against-human-rights-defenders**

26 Amnesty International, „New tool for spy victims to detect government surveillance“ (News, 20. November 2014)

27 Citizen Lab, „HIDE AND SEEK. Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries“, September 2018, **https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45- countries/**

28 Amnesty International, „Amnesty International among targets of NSO-powered campaign“, 1. August 2018, aktualisiert am 1. Oktober 2018 **www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/**

29 Amnesty International, „Morocco: Human Rights Defenders Targeted with NSO Group's Spyware“, 2019 **www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/**

30 Citizen Lab, „HIDE AND SEEK. Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries“, September 2018, **https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45- countries/**

31 UN-Leitprinzipien für Wirtschaft und Menschenrechte, **www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf** **https://www.globalcompact.de/wAssets/docs/Menschenrechte/Publikationen/leitprinzipien_fuer_wirtschaft_und_menschenrechte.pdf**

32 **www.wassenaar.org/the-wassenaar-arrangement/**

33 Amnesty International, Amnesty International affidavit in support of Israeli petition, (Index: ACT 10/0332/2019) und „Israel: Amnesty International engages in legal action to stop NSO Group's web of surveillance“, (News, 13. Mai 2019)

34 Amnesty International, „EU: States push to relax rules on exporting surveillance technology to human rights abusers”, (News, 11. Juni 2018)

35 Amnesty International, Amnesty International Comments on the European Commission Dual-Use Export Proposal (Index POL 10/1558/2017)

36 Erklärung über das Recht und die Verpflichtung von Einzelpersonen, Gruppen und Organen der Gesellschaft, die allgemein anerkannten Menschenrechte und Grundfreiheiten zu fördern und zu schützen, 1998, UN-Dok. A/RES/53/144

37 UN-Leitprinzipien für Wirtschaft und Menschenrechte, www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf **https://www.globalcompact.de/wAssets/docs/Menschenrechte/Publikationen/leitprinzipien_fuer_wirtschaft_und_menschenrechte.pdf**

38 OHCHR, The Corporate Responsibility to Respect Human Rights: An Interpretive Guide, 2012, S.17, **www.ohchr.org/Documents/Publications/HR.PUB.12.2_En.pdf**

39 ICJ, Report of the ICJ Expert Legal Panel on Corporate Complicity in International Crimes, 2008, **www.icj.org/report-of-the-international-commission-of-jurists-expert-legal-panel-on-corporate-complicity-in-international- crimes/**

40 OHCHR, Surveillance and human rights, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN-Dok. A/HRC/41/35, 28. Mai 2019

AMNESTY INTERNATIONAL Deutschland e. V.
Zinnowitzer Straße 8 . 10115 Berlin
T: +49 30 420248-0 . F: +49 30 420248-488 . E: info@amnesty.de

SPENDENKONTO . Bank für Sozialwirtschaft
IBAN: DE23 3702 0500 0008 0901 00 . BIC: BFS WDE 33 XXX .

AMNESTY INTERNATIONAL