Deutscher Bundestag

Ausschuss für Menschenrechte
und humanitäre Hilfe

Ausschussdrucksache
19(17)93

STELLUNGNAHME AMNESTY INTERNATIONAL

ÖFFENTLICHE ANHÖRUNG DES AUSSCHUSSES FÜR MENSCHENRECHTE UND HUMANITÄRE HILFE DES DEUTSCHEN BUNDESTAGES AM 17. JUNI 2020

Lena Rohrbach, Referentin für Menschenrechte im digitalen Zeitalter, Wirtschaft und Rüstungsexportkontrolle.

Stand: 08.06.2020

1. Welche mittelfristigen und langfristigen Auswirkungen hat die dynamisch steigende Instrumentalisierung digitaler Technologien durch autoritäre Akteure für die praktische Durchsetzung der Menschenrechte national wie international, und welche Akteure können Menschenrechte dagegen in digitalen Räumen mit welchen Strategien verteidigen? (CDU/CSU)

3. Wie wirken die Werte Transparenz und Datenschutz im digitalen Zeitalter zusammen und was sind Ihrer Ansicht nach die größten Bedrohungen für die Menschenrechte und die politische Beteiligung im digitalen Zeitalter, insbesondere in Hinblick auf Menschenrechtsverteidiger, Whistleblower und andere Gruppen, die moderne Informationstechnologien nicht nur nutzen, sondern mit deren Hilfe auch besonders drangsaliert werden? (DIE LINKE.)

Die Fragen 1 und 3 werden gemeinsam beantwortet. Die Stellungnahme konzentriert sich auf Menschenrechtsverteidiger_innen, die Probleme ergeben sich aber nahezu analog für Journalist_innen, Aktivist_innen, Oppositionelle und andere Personen.

Einführung

Menschenrechtsorganisationen, darunter auch Amnesty International, beobachten seit Jahren einen schrumpfenden Spielraum für die Zivilgesellschaft in zahlreichen Ländern. Auch die Bundesregierung hat das Problem der **"Shrinking Spaces"** wiederholt als ein solches benannt.[1] Der UN-Sonderberichterstatter für die Situation von Menschenrechtsverteidiger_innen spricht gar von einem Krieg gegen die Zivilgesellschaft.[2] Zu den Taktiken der Repression gegen Menschenrechtsverteidiger_-innen gehören Diffamierung, Drohungen, Kriminalisierung zivilgesellschaftlichen Engagements bis hin zu physischen Angriffen, Verschwindenlassen und Tötungen.[3]

1 Etwa in ihrem Menschenrechtsbericht (2014 –2016) als ein Brennpunktthemen., S. 145 ff., https://www.auswaertiges-amt.de/blob/229010/327fbf67bbec639a36b7a3a9694887aa/12--mr-bericht-bureg-data.pdf

2 Michel Forst, 12/2018, World report on the situation of Human Rights Defenders, https://www.protecting-defenders.org/sites/protecting-defenders.org/files/UNSR%20HRDs-%20World%20report%202018.pdf

3 Siehe auch weiterführende Berichte 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)

Im Zuge der digitalen Transformation lässt sich außerdem ein zunehmender Einsatz digitaler Technologie zur Repression der Zivilgesellschaft beobachten - **“Shrinking Spaces” im digitalen Wandel.** Immer häufiger beobachtet Amnesty International, dass Staaten ihre Vorgehensweisen, Inhalte von Gesetzen und konkrete Technologien voneinander abschauen, ex- und importieren. Beobachten lässt sich die Entwicklung eines **“Werkzeugkastens” von Methoden und Technologien**, die zur Einschüchterung und für Angriffe auf die Zivilgesellschaft eingesetzt werden. Dabei sind besonders gängige Werkzeuge in verschiedenen Staaten im Einsatz und üben eine abschreckende Wirkung (sogenannte Chilling Effects) auf Menschenrechtsverteidiger_innen aus, die zu Selbstzensur führt. Zu diesem Werkzeugen gehören die gezielte digitale Überwachung der Zivilgesellschaft und eine verstärkte Kontrolle und Zensur ihres Informationszugangs und -austausches.

Einschränkungen der Meinungs- und Informationsfreiheit, politische Teilhabe

Insbesondere **im Vorfeld von Wahlen und während öffentlicher Proteste,** aber teils auch als permanente Maßnahme gehören zu diesen Werkzeugkasten **Internet-Shutdowns** (das Nicht-verfügbar-machen des Internets aus dem Staatsgebiet heraus, soweit technisch möglich) oder das **partielle Sperren** bestimmter Webseiten, Social Media Plattformen oder Dienste. Gefährdet sind insbesondere Länder, deren Regierungen auch den **Aufbau national abschottbarer Internet-Strukturen / “Cyber-Souveränität”** vorantreiben. Diese sind kaum resilient gegenüber Zensur und Überwachung und bieten der Zivilgesellschaft wenig Umgehungsmöglichkeiten. Zu diesen Ländern gehören **Iran, China (“Great Firewall”/”Golden Shield Project”) und Russland („Gesetz über das souveräne Internet“).**

Einige jüngste Beispiele für Internet-Shutdowns: So sperrte die Regierung der Demokratischen Republik **Kongo** in den vergangenen zwei Jahren immer wieder den Zugang zum Internet und zu sozialen Medien, um regierungskritische Proteste zu unterbinden. **Benin** sperrte im April 2019 den Internetzugang im Vorfeld von Wahlen und erschwerte damit Kritik an den Wahlen, bei denen es keine Oppositionskandidat_innen gab. Zu diesem noch recht frühen Zeitpunkt im Jahre waren allein in Subsahara-Afrika[4] bereits weitere Internet-Shutdowns im **Tschad, Kongo, Gabon, Mali und Zimbabwe** dokumentiert. **Myanmar** sperrte den Internetzugang im Sommer 2019 in Konfliktgebieten wie Rakhine und Chin und erschwerte damit die Berichterstattung über Menschenrechtsverletzungen durch das Militär.[5] **Venezuela** sperrte den Zugang zu Social Media Diensten insbesondere dann, wenn Oppositionsführer Juan Guaidó einen Livestream durchführen wollte.[6] Die Regierung des **Iran** legte in Reaktion auf politische Großdemonstrationen den vielfach genutzten Messenger-Dienst Telegram und anlässlich regierungskritischer Proteste für eine Woche das gesamte Internet lahm. Auch in **China** wurde die umfassende Kontrolle des Internets in den

[4] In 2016, the African Commission on Human and Peoples’ rights adopted a resolution on the right to freedom of information and expression on the internet in Africa in which it expressed its concerns over “the emerging practice of State Parties of interrupting or limiting access to telecommunications services such as the Internet, social media and messaging services, increasingly during elections.” (Quelle fehlt und übersetzen)

[5] Amnesty International, 06/2019, Myanmar: End Internet Shutdown In Rakhine, Chin States, https://www.amnesty.org/en/documents/asa16/0604/2019/en/

[6] KeepItOn, 06/2019 Targeted, Cut Off, And Left In The Dark https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf

vergangenen Jahren weiter verschärft: Tausende Webseiten und Angebote der sozialen Medien sind nach wie vor vollständig gesperrt bzw. stark zensiert, darunter Facebook, Instagram, Twitter und Menschenrechtsseiten wie die Webseiten von Amnesty International. Der Zugang zu Internet wird auch in **diskriminierender** Weise verhindert, so hat die Regierung **Bangladeschs** den Verkauf von mobilen SIM-Karten an **Rohingya-Flüchtlinge** untersagt. Diskriminierende Effekte ergeben sich auch aus der Tatsache, dass **Menschen mit Zugang zu finanziellen, technischen und informationellen Ressourcen Internetsperren leichter umgehen können als arme und marginalisierte Menschen.**

Insgesamt zählte das internationale Bündnis #KeepItOn **für das Jahre 2019 mind. 213 Shutdowns in 33 Ländern**. Die meisten Shutdowns pro Land gab es in **Indien** (121 Fälle, darunter für 175 Tage in Kashmir), **Venezuela** (mind. 12 Fälle), **Yemen** (11), **Irak** (8), **Algerien** (6) und **Äthiopien** (5). Das Bündnis hält einen Trend zu immer längeren sowie zu besonders zielgerichteten Abschaltungen fest.[7]

Internet-Shutdowns sind selbst zum Erreichen legitimer Ziele (wozu etwa die Unterdrückung von Kritik an einer Wahl klarerweise nicht gehört) ein Mittel, das den Grundsatz der **Verhältnismäßigkeit verletzt**. Sie stellen daher grundsätzlich eine **Verletzung zahlreicher Menschenrechte** dar, darunter Meinungs- und Informationsfreiheit, Versammlungs- und Vereinigungsfreiheit und Teilhaberechte. Mangelnder Zugang zu medizinischen Informationen (etwa aktuell während der COVID19-Pandemie) kann außerdem das Recht auf Gesundheit beeinträchtigen und ohne Internetzugang sind auch viele Aufgaben am Arbeitsplatz nicht durchführbar.

Um Zensurmaßnahmen umfassend durchführen zu können, kriminalisieren oder erschweren manche Staaten etwa den Einsatz von Verschlüsselungs- oder Anonymisierungswerkzeugen wie **VPN**, darunter **Russland und China**[8]. Mögliche Gegenmaßnahmen umfassen den **Aufbau alternativer technischer Infrastrukturen und das Bereitstellen von Umgehungswerkzeugen.**

Auch **strategische Klageführung** zeigte sich in einigen Fällen erfolgreich. Amnesty International unterstützt daher in **Togo** eine Klage gegen den Internet-Shutdown 2017.

Cybercrime Laws

Ein weiteres Werkzeug stellen sogenannte **"Cybercrime laws"** dar, die die freie Meinungsäußerung und das Teilen von Informationen online einschränken oder Telekommunikationsunternehmen verpflichten, sensible Daten über ihre Nutzer_innen ohne hinreichende unabhängige Kontrolle an Behörden weiterzugeben. Menschenrechtliche problematische Gesetze dieser Art haben etwa **Ägypten[9], Pakistan[10], China, Iran, Bangladesch[11], Thailand[12], die besetzen palästinensischen Gebiete[13], Bahrain, Saudi-**

---

[7] KeepItOn, 06/2019 Targeted, Cut Off, And Left In The Dark https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf

[8] Amnesty International, 07/2017, VPN-Verbot bedroht Internetfreiheit https://www.amnesty.de/informieren/aktuell/russische-foederation-vpn-verbot-bedroht-internetfreiheit

[9] Amnesty International, 07/2018, Egyopt: Proposed laws an assault on online freedoms https://www.amnesty.org/en/latest/news/2018/07/egypt-proposed-laws-an-assault-on-online-freedoms/

[10] Amnesty International, 01/ 2020, 2019 in review - Pakistan: Crackdown on human rights intensifies https://www.amnesty.org/en/latest/news/2020/01/2019-pakistan-in-review/

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

[12] Tech Crunch, 02/2019, Thailand passes controversial cybersecurity law that could enable government surveillance https://techcrunch.com/2019/02/28/thailand-passes-controversial-cybersecurity-law/

Arabien[14] **und weitere Länder** beschlossen. Obwohl Gesetze zur Bekämpfung online ausgeübter Straftaten selbstverständlich legitim sein können (nach einer Erfassung der UN Conference on Trade and Development (UNCTAD) verfügen 154 Länder über irgendeine eine Form von Cybercrime-Gesetzgebung[15]), genügen viele dieser Gesetze nicht den Anforderungen an ein präzises und "vorhersehbares" Gesetz. Mit ihnen werden Blogger_innen und Online-Journalist_innen unter **Formulierungen verfolgt, die zu breit und vage gefasst** sind und mit ungenügend definierten Begriffen arbeiten (etwa "Terrorismus", "Fake News" oder "Diffamierung"). Neben teils langjährigen Gefängnisstrafen für die Betroffenen führt die daraus resultierende Rechtsunsicherheit zu "Chilling Effects" auf die gesamte Zivilgesellschaft.

Privatsphäre / Überwachung

Während die oben genannten Werkzeuge insbesondere die Meinungs- und Informationsfreiheit verletzen, verletzt Überwachung primär das Recht auf Privatsphäre. Da es sich bei dem Recht auf **Privatsphäre um ein "befähigendes Recht"** (enabling right) handelt, das - ähnlich wie das Recht auf Meinungsfreiheit - Menschen in die Lage versetzt, andere Rechte wahrzunehmen, sind gewöhnlich auch weitere Rechte betroffen. Der **Einsatz digitaler Überwachungstechnologien** durch Polizei, Strafverfolgungsbehörden und Geheimdienste hat in den letzten Jahren **exponentiell zugenommen**. Hierzu gehören Maßnahmen der Massenüberwachung, wie sie insbesondere von Geheimdiensten durchgeführt werden, ebenso wie eine zunehmende gezielte Überwachung von Menschenrechtsverteidiger_innen, Journalist_innen, Oppositionellen und anderen Personen. Maßnahmen umfassen die Überwachung der elektronischen Kommunikation, Überwachungskameras, den Einsatz von Gesichtserkennungstechnologie und anderen biometrischen Technologien (siehe zu letzteren Antworten auf Fragen 4 und 12)

Massenüberwachung

Anlasslose Massenüberwachung, wie sie insbesondere von Geheimdiensten etwa der USA, Großbritanniens, Chinas, Deutschlands[16] und anderer Länder durchgeführt wird, stellt einen unverhältnismäßigen Eingriff - und damit eine **Menschenrechtsverletzung** - in das Recht auf Privatsphäre und weitere Menschenrechte dar. Oftmals fehlt es dabei zudem an Transparenz, unabhängiger Kontrolle und gesetzlichen Grundlagen, oder letztere sind zu breit und vag gefasst.

Massenüberwachung betrifft Menschen selbst dann, wenn sie nicht im Netz der Nachrichtendienste landen: Aufgrund von "Chilling Effects" kann bereits die Tatsache, mit der ständigen **Gefahr einer möglichen Überwachung leben zu müssen, eine Menschenrechtsverletzung darstellen**, auch, wenn die Überwachung nicht tatsächlich erfolgt ist oder zumindest nicht nachgewiesen werden kann.[17]

---

[13] Amnesty International, 12/2017, Palestine: Reform Restrictive Cybercrime Law Amended Draft Better, But Still Short Of International Standards https://www.amnesty.org/en/documents/mde15/7632/2017/en/

[14] Amnesty International, 01/2019, Saudi Arabia: Censorship of Netflix is latest proof of crackdown on freedom of expression https://www.amnesty.org/en/latest/news/2019/01/saudi-arabia-censorship-of-netflix-is-latest-proof-of-crackdown-on-freedom-of-expression/

[15] UNCTAD unterscheidet für die Erhebung nicht zwischen legitim ausgearbeiteten und menschenrechtlich problematischen Gesetzen. https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx

[16] Lena Rohrbach, 10/2016, Die Illegalen Fünf, https://www.amnesty.de/journal/2016/oktober/die-illegalen-fuenf

[17] 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; siehe auch: Amnesty International, A Dangerous

Gezielte Überwachung

Im Gegensatz zur Massenüberwachung nimmt gezielte Überwachung einzelne Individuen in den Blick. Gezielte Überwachung kann im Rahmen der **Überwachung von Telekommunikationsnetzen** erfolgen (ähnlich der Massenüberwachung) oder durch eine gezielte Kompromittierung von Smartphones, Computern und anderen von den Betroffenen genutzten Geräten. Letzteres - das **"staatliche Hacken"** - ermöglicht eine größer Bandbreite an Eingriffen in die Privatsphäre der Betroffenen, da auch Informationen erfasst werden können, die sich nicht in Transit befinden. Die gezielte Infiltration von Smartphones und Computern kann es ermöglichen, **Dateien von der Festplatte des betroffenen Gerätes auszulesen (und zu verändern oder zu löschen), Geodaten zu protokollieren oder den aktuellen Aufenthaltsort zu erfragen, die Kamera unbemerkt anzuschalten, um private Räume zu filmen oder kompromittierendes Material zu erlangen, und Screenshots des Bildschirms anzufertigen (und zu versenden).**

Zudem ermöglicht die Kompromittierung des Endgerätes es, auch Ende-zu-Ende-**verschlüsselte Kommunikation mitzulesen**. So kann beispielsweise auch Kommunikation über den weitverbreiteten Messengerdienst **WhatsApp** überwacht werden. Mit diesem Argument wird der Einsatz sogenannter **"Staatstrojaner"** auch in Deutschland gerechtfertigt und seine Ausweitung gefordert. Die Bundesregierung muss bei Debatten dieser Art stets die **mögliche Vorbildwirkung** auf Staaten mitdenken, in denen Menschenrechtsverletzungen an der Tagesordnung sind. Menschenrechtsverteidiger_innen, tatsächlich sogar alle Menschen sowie Unternehmen und Infrastrukturen weltweit sind außerdem gefährdet, wenn Regierungen ihren Dienste bekannte **Sicherheitslücken nicht melden**, damit diese sie für Überwachungsmaßnahmen ausnutzen können.

Die Kompromittierung von Geräten kann durch die Installation von Spionagesoftware erfolgen. In technisch besonders ausgefeilten Fällen ist es dafür nicht einmal mehr notwendig, die Betroffenen dazu zu bringen, aktiv einen Link anzuklicken.[18]

Oftmals unterbelichtet in der Berichterstattung über gezielte Überwachung ist die soziale Komponente. **"Social Engingeering"** im Vorfeld gezielter Überwachung beschreibt das Phänomen, dass Personen etwa im Auftrag der Regierung eine falsche Identität annehmen, um in sozialen Netzwerken oder per E-Mail / Messenger das Vertrauen des Opfers zu gewinnen. Dazu ein Fallbeispiel: Im von Amnesty International dokumentierten Fall der prominenten **pakistanischen** Menschenrechtsverteidigerin Diep Saeeda gab sich ein_e **Facebook**-Nutzer_in als UN-Mitarbeiterin aus und kontaktierte Saeeda mehrmals über den Facebook-Messenger-Anwendung. Ihre Nachrichten erhielten Dateianhänge, die beim Öffnen eine Spionagesoftware installiert hätten. Saeeda erhielt außerdem E-Mails, die vermeintlich vom Personal des Ministerpräsidenten von Punjab versendet wurden, sowie solche, die angeblichen von ihren Rat suchenden Studierenden stammten. Die Menschrechtsaktivistin berichtete Amnesty International: "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 gemeinnützige Arbeit leidet darunter."[19]

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

[18] Amnesty International, 02/2020, How to keep your communications safe in 2020 https://www.amnesty.org.nz/how-keep-your-communications-safe-2020

[19] Amnesty International, 05/2018, Pakistan: Human Rights Under Surveillance,

Technisch weniger ausgefeilte, aber oft effektive Angriffe verbergen sich hinter **(Massen-)Phishing-Angriffen**, die kostengünstig und einfach skalierbar sind und innerhalb von Minuten eine große Zahl von Opfern treffen können.[20] So wurden 2019 (sowie in Vorjahren) nach Amnesty-Recherchen in **Ägypten** zahlreiche Menschenrechtsverteidiger_innen und andere Mitglieder der Zivilgesellschaft Opfer systematischer Phishing-Angriffe, eine große Gefährdung angesichts des zunehmend harten Vorgehens gegen regierungskritische Stimmen durch die Regierung.[21] Die Angriffe erfolgen beispielsweise in Form einer Aufforderung zum Zurücksetzen des Kennworts und eines Links, der einen Mobilfunkbetreiber oder ein Social-Media-Unternehmen als Absender nachahmt. Auch bei Phishing kann Social Engineering eine Rolle spielen.

Gewonnene Informationen werden - oft in manipulierter oder aus dem Zusammenhang gerissener Weise in Strafverfahren verwendet. In der Folge reiben sich die betroffenen Menschenrechtsverteidiger_innen in **Gerichtsverfahren** auf, statt ihre Energie und Ressourcen für ihre eigentliche Tätigkeit einsetzen zu können.[22] Die Informationen werden außerdem für Erpressungen, persönliche Angriffe oder Diffamierungskampagnen dazu verwendet.

Auch Menschenrechtsverteidiger_innen, die ihr Land verlassen haben, sind weiterhin betroffen. 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.[23] In **Usbekistan** sind Personen, die von Cyberangriffen betroffen waren und ihr Zuhause verlassen haben, nach wie vor Ziel digitaler Überwachungsmaßnahmen.[24]

Zunehmend greifen Regierungen auf **private Unternehmen** zurück, um die Entwicklung von Technologie zur gezielten digitalen Überwachung in Auftrag zu geben.[25] In diesem Markt tätige Unternehmen spielen eine zentrale Rolle bei der Entwicklung neuer Werkzeuge. Die Branche zeichnet sich durch hohe **Intransparenz und einen eklatanten Mangel der Umsetzung menschenrechtlicher Sorgfaltspflichten** aus. Zu den wichtigsten Unternehmen gehören die **NSO Group** (Israel und Luxemburg) sowie in der EU **Finfisher** (Großbritannien und Deutschland). Private Unternehmen haben jedoch auch die Möglichkeit, Menschenrechtsverteidiger zu schützen. So zeigten ägyptischen Betroffenen einer Phishing-Kampagne Amnesty International eine **Warnmeldung ihres Email-Anbieters Gmail** erhalten hatten, die sie vor von Google erkannten mutmaßlich regierungsgesteuerten Überwachungsangriffen warnte.[26] **Facebook** meldete Erfolge bei der Warnung von

---

https://www.amnesty.org/en/documents/asa33/8366/2018/en/

[20] Amnesty International, 02/2020, How to keep your communications safe in 2020, https://www.amnesty.org.nz/how-keep-your-communications-safe-2020

[21] Amnesty International, 03/2019, Phishing attacks using third-party applications against Egyptian civil society organizations

[22] Amnesty International, 2019, Per Gesetz mundtot gemacht: Die weltweite Unterdrückung zivilgesellschaftlicher Organisationen, https://www.amnesty.de/sites/default/files/2020-02/Amnesty-Bericht-Per-Gesetz-Mundtot-Gemacht-Februar2020.pdf

[23] Amnesty International, 03/2017, False Friends: How Fake Accounts and Crude Malware Targeted Dissidents in Azerbaijan https://www.amnesty.org/en/latest/research/2017/03/False-Friends-Spearphishing-of-Dissidents-in-Azerbaijan/

[24] Amnesty International, 03/2017, Uzbekistan: "We Will Find You Anywhere" - The Global Shadow of Uzbekistani Surveillance https://www.amnesty.org/en/documents/eur62/5974/2017/en/

[25] Julie Bloch, Sukti Dhital, Rashmika Nedungadi, Nikki Reisch, 05/2019, CTRL+HALT+Defeat: State-sponsored Surveillance and the suppression of Dissent, www.justsecurity.org/64095/ctrlhaltdefeat-state- sponsored-surveillance-and-the-suppression-of-dissent/

[26] Amnesty International, 03/2019, Phishing attacks using third-party applications against Egyptian civil society organizations

Minderjährigen vor sogenanntem “Cybergrooming” durch Metadaten-Analysen.[27] Mehrere der hierbei eingesetzten Werkzeuge scheinen geeignet, nicht nur Kinder, sondern auch Menschenrechtler_innen zu schützen, bevor diese Opfer von Täuschungsversuchen und Social Engingeering werden.

Eine Verschärfung der Problematik ergibt sich durch die klandestine Natur der Menschenrechtsverletzungen, die den **Zugang zu Rechtsmitteln erschwert**. Im Gegensatz zu staatlichen Maßnahmen wie physischer Gewalt oder Inhaftierung ist eine **Überwachungsmaßnahme oft unsichtbar** und bleibt auch für die Betroffen unbemerkt. Selbst wenn sie bemerkt wird, ist die **Attribution,** also die Identifizierung der Angreifenden und Verantwortlichen, oftmals unmöglich. Um den Rechtsweg zu ermöglichen, müssen Staaten die Betroffenen von verdeckten Überwachungsmaßnahmen **benachrichtigen**, sobald dies möglich ist, ohne den Zweck der Überwachung zu gefährden.

Die Überwachung von Menschenrechtsverteidiger_innen aufgrund ihrer Arbeit verletzt das Recht auf Privatsphäre und beeinträchtigt die Rechte auf freie Meinungsäußerung, auf Vereinigungs- und Versammlungsfreiheit.

4. Was kann Gesichtserkennung (Facial Recognition Technology) und welche Auswirkungen hat diese Form der Künstlichen Intelligenz auf den Schutz, die Respektierung und Gewährleistung von Menschenrechten im nationalen sowie internationalen Kontext? (BÜNDNIS 90/DIE GRÜNEN)

12. Welche Notwendigkeit einer Regulierung von Gesichtserkennung bei ihrer (Weiter)Entwicklung, Anwendung und Exportkontrolle sehen Sie und wie könnte eine solche Regulierung auf nationalstaatlicher, supranationaler und internationaler Ebene oder unter Akteuren der Privatwirtschaft aussehen? (BÜNDNIS 90/DIE GRÜNEN)

Die Fragen 4 und 12 werden gemeinsam beantwortet.

Einführung

Gesichtserkennung bezeichnet den Prozess der Identifizierung oder Verifizierung einer Person anhand ihres Gesichts. Dabei werden Merkmale des Gesichts eingefangen (das Gesicht wird vom System als Ziel erkannt und die analoge Information in ein Set digitaler Informationen verwandelt), analysiert und verglichen. Gesichtserkennung ist eine besonders gut zugängliche Form **biometrischer Identifizierung** (neben bspw. Fingerabdrücken, Irisscans, Stimm-, Gang- oder Venenerkennung) und als solche eine Form **künstlicher Intelligenz**. Viele (wenn auch nicht alle) der im Folgenden geschilderten Menschenrechtsrisiken bestehen auch für andere Formen biometrischer Identifizierung und KI.

Durch private Akteure wird Gesichtserkennung (Facial Recognition Technology - FRT) beispielsweise im Testbetrieb von Kaufhäusern eingesetzt, die sich unter dem Stichwort “know your customer” durch Identifizierung der Person und daran angepasste Angebote

[27] Patrick Beuth, 05/2020, Facebook will auch verschlüsseltes Cybergrooming erkennen, https://www.spiegel.de/netzwelt/apps/messenger-facebook-will-auch-verschluesseltes-cybergrooming-erkennen-a-e3bbb0ac-ae65-4e04-8c6c-68e9b319b3db

und Behandlung einen höheren Umsatz erhoffen. Entsprechende Tests führten etwa Kentucky Fried Chicken und der chinesische Technologieriese Alibaba durch. Auch Facebook oder ein Smartphone, das Personen in seiner Fotogalerie identifiziert oder sich mit einem Blick entsperren lässt, verwenden FRT.

Durch öffentliche Stellen kann FRT etwa beim Ausstellen von Identitätsdokumenten (als Maßnahme gegen Identitätsdiebstahl), bei Flughafenkontrollen (Vergleich von Person und Identitätsdokument), bei Polizeikontrollen oder zur Überwachung öffentlicher Räume (in Kombination mit Videoüberwachung) eingesetzt. Zu den angegebenen Zielen gehört das Finden gesuchter Krimineller, vermisster Kinder (Indien) oder desorientierter Erwachsener und die Unterstützung von Ermittlungen (z.B. bei Aufnahmen von Verbrechen oder dessen räumlichem Umfeld)

FRT kann zwei verschiedene Grundfunktionen erfüllen:

1. **Authentifizierung/Verifizierung** beantwortet die Frage "ist dies wirklich die Person, die sie vorgibt zu sein?" (z.B. Zugang zu Räumlichkeiten nur für autorisiertes Personal, Vergleich Passfoto/Person am Flughafen, Entsperren des Smartphones). Bei der Authentifizierung/Verifizierung wird ein exaktes Match in einer Datenbank für ein einziges Gesicht gesucht. Weitere Personen sind nicht betroffen und die Durchführung der Maßnahme ist offensichtlich.
2. **Identifizierung** beantwortet die Frage "Wer ist diese Person?", etwa bei der Identifizierung von Menschen aus der Überwachung öffentlicher Räume. Dazu gehört für Deutschland etwa das Pilotprojekt Südkreuz[28] oder der Vorschlag, FRT in zahlreichen Bahnhöfen und Flughäfen einzusetzen[29]. **Die vorliegende Stellungnahme konzentriert sich primär auf den Einsatz von FRT zur Identifizierung im öffentlichen Raum** (oft als automatisierte Gesichtserkennung oder live Gesichtserkennung bezeichnet), bei der zahlreiche weitere Menschen betroffen sind und die große menschenrechtliche Risiken aufweist. Sie konzentriert sich außerdem auf den **Einsatz durch staatliche Stellen**. Viele der menschenrechtlichen Probleme, insbesondere aber nicht ausschließlich für das Recht auf Nicht-Diskriminierung, ergeben sich allerdings auch beim Einsatz von FRT zu Zwecken unter 1 und durch private Akteure.

Gesichtserkennung greift in zahlreiche Menschenrechte ein. Daher muss ihr Einsatz geeignet zum Erreichen eines legitimen Zieles, notwendig und verhältnismäßig sein und auf einer klaren gesetzlichen Grundlage beruhen. Während es **in vielen Fällen um klarerweise legitime Ziele** geht (z.B. das Finden von Straftätern oder vermissten Kindern), stellen sich schwerwiegende Fragen danach, **ob der Einsatz von FRT zur Identifizierung im öffentlichen Raum jemals ein verhältnismäßiges Mittel zum Erreichen dieser Ziele** sein kann.

Angesichts der schwerwiegenden menschenrechtlichen Risiken (darunter für die Rechte auf Privatsphäre, Gleichheit und Nichtdiskriminierung, Meinungs-, Versammlungs- und Vereinigungsfreiheit) **sollte identifizierende FRT im öffentlichen Raum nach Überzeugung von Amnesty International nicht eingesetzt werden**, solange Staaten nicht nachweisen

[28] BMI, 10/2018, Projekt zur Gesichtserkennung erfolgreich, https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2018/10/gesichtserkennung-suedkreuz.html

[29] SPON, 01/2020, Seehofer verzichtet auf Software zur Gesichtserkennung, https://www.spiegel.de/politik/deutschland/bundespolizeigesetz-seehofer-verzichtet-auf-software-zur-gesichtserkennung-a-c207b3c8-eb1a-48e9-80ce-2642b420bd55

können, dass es eine mit den internationalen Menschenrechten vereinbare Verwendung gibt. Dies wird im Folgenden begründet.

Auswirkungen auf das Recht auf Privatsphäre und die Menschenwürde

Der Einsatz von Gesichtserkennung zur Identifizierung ist eine Form von Überwachung, die einen tiefgreifenden Eingriff in das Recht auf Privatsphäre darstellt. Obwohl das Recht auf Privatsphäre historisch (v.a. im amerikanischen Raum) mit dem "privaten Raum" verknüpft ist, hat sich dieses Verständnis gewandelt und es wird grundsätzlich auch ein **Recht auf Privatsphäre im öffentlichen Raum** anerkannt.

Einschränkungen von Menschenrechten dürfen nicht isoliert betrachtet werden, sondern müssen in ihrer gemeinsamen Wirkung mit bereits existierenden Eingriffen gewürdigt werden. In Deutschland hat das Bundesverfassungsgericht dies für Privatsphäre in einer Weise ausformuliert, die als **"Überwachungsgesamtrechnung"** bekannt ist. Diese durchzuführen ist für FRT von besonderer Bedeutung, denn **Gesichtserkennung schließt den für viele Menschen letzten überwachungsfreien Rückzugsraum**. In einer Zeit potentiell vollständiger Überwachung der elektronischen Kommunikation und von Smartphone- und anderen Metadaten weltweit und insbesondere in Ländern, in denen Menschenrechtsverteidiger_innen, Journalist_innen und Oppositionelle zusätzlich mit verwanzten Wohnungen rechnen müssen, ist der öffentliche Raum der letzte freie mögliche Treffpunkt. So berichteten Menschenrechtler_innen aus **Belarus** Amnesty International, aufgrund der umfassenden Überwachung ihrer digitalen Geräte und Wohnungen träfen sie sich für wichtigen Informationsaustausch draußen. Sie berichteten sogar, selbst Treffpunkt und Zeiten für solche Treffen würden ebenfalls im öffentlichen Raum besprochen, da sie die Erfahrung gemacht hätten, dass die Polizei aufgrund der Kommunikationsüberwachung sonst bereits am Treffpunkt warte.[30] Jenseits solch drastischer Fälle ist - auch in **Deutschland** - der öffentliche Raum derjenige, in dem Proteste stattfinden, Menschen zum Gewerkschaftstreffen, ihrer Affäre, der Abtreibungsberatung oder den Anonymen Alkoholikern gehen. **Gesichtserkennungstechnologie ist geeignet, die freie und unbeobachtete Bewegung im öffentlichen Raum vollständig zu beenden.** Werden die **Informationen aus FRT gar mit Informationen aus der Kommunikationsüberwachung kombiniert, kann ein vollständiges Bild des Alltags aller Menschen entstehen**, bis hin zu permanenten Aufzeichnungen unseres gesamten Lebens. Wie die EU Grundrechteagentur festhält, kann der Einsatz von FRT daher sogar **die Menschenwürde verletzen**: "[T]he impact on what people may perceive as surveillance technologies on their lives may be so significant as to affect their capacity to live a dignified life."[31] Auch der Europäische Datenschutzbeauftragte argumentiert, die **massenhafte Objektifizierung menschlicher Gesichter** zu privat-kommerziellen oder auch öffentlichen Sicherheitsinteressen verletzte die Menschenwürde.[32]

Der Einsatz von FRT zur Identifizierung im öffentlichen Raum erfordert eine umfassende Überwachung, Sammlung, Speicherung und Analyse sensibler personenbezogener Daten **ohne individualisierten begründeten Verdacht** eines im Sinne der Straftatenprävention,

---

[30] Amnesty International, 2016, It's enough for people to feel it exists, https://www.amnesty.org/download/Documents/EUR4943062016ENGLISH.PDF

31 FRA, 2019, Facial recognition technology: fundamental rights considerations in the context of law enforcement https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

32 Wojciech Wiewiórowski,10/2019, Facial recognition: A solution in search of a problem? https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en

Strafverfolgung oder Gefahrenabwehr irgendwie näher definierten Fehlverhaltens - was einer **anlasslosen Massenüberwachung gleichkommt**. Ein zielgerichteter Einsatz ist nicht möglich, denn zufällig vorbeikommende Personen sind geradezu konstituierendes Merkmal öffentlicher Räume - **auch dann, wenn sie nicht vom Algorithmus gesucht werden, sind sie betroffen.** Einer Umfrage der EU Grundrechteagentur zufolge lehnen es über 80 Prozent der europäischen Bevölkerung ab, Bilder ihres Gesichtes zu Identifikationszwecken mit öffentlichen Stellen zu teilen.[33] Beim Einsatz im öffentlichen Raum wird jedes gescannte Gesicht analysiert, die Auswertung hat ggf. Einfluss auf zukünftige Entscheidungen des Algorithmus. Dies gilt auch dann, wenn die Daten umgehend wieder gelöscht werden oder regelrecht "nur durch das System fließen". So hat das **BVerfG** anlässlich des vergleichsweise weniger eingriffsintensiven Kfz-Scannings festgestellt (und dabei ein eigenes früheres Urteil korrigiert): "Eine automatisierte Kraftfahrzeugkennzeichenkontrolle begründet Eingriffe in das Grundrecht auf informationelle Selbstbestimmung aller Personen, deren Kennzeichen in die Kontrolle einbezogen werden, **auch wenn das Ergebnis zu einem „Nichttreffer" führt und die Daten sogleich gelöscht werden**."[34]

Europaweit haben Gerichte die Unverhältnismäßigkeit von Massenüberwachung festgestellt[35], insbesondere dann, wenn sie von Behörden mit operativen Befugnissen (wie Polizeien) und gegen die eigene Bevölkerung eingesetzt wird. Amnesty International ist der Ansicht, dass **anlasslose Massenüberwachung niemals einen verhältsnismäßigen Eingriff** in die Rechte auf Privatsphäre, freie Meinungs-, Versammlungs- und Vereinigungsfreiheit darstellen kann und daher **immer Menschenrechte verletzt. Dies gilt folglich auch für identifizierende FRT im öffentlichen Raum.**

Auswirkungen auf Meinungs-, Vereinigungs- und Versammlungsfreiheit

Gesichtserkennung im öffentlichen Raum greift tief in die Rechte auf Meinungs-, Vereinigungs- und Versammlungsfreiheit ein. Sie wird durch Staaten zunehmend zur **Überwachung von Protesten**, aber auch anderen Großereignissen wie Festivals oder Sportevents genutzt. Der Einsatz von Gesichtserkennung führt zu **Chilling Effects** und kann Menschen davon abhalten, die betroffenen Räume zu betreten oder an Protesten teilzunehmen. Das Bemühen der **Demonstrierenden in HongKong**, sich durch Masken vor FRT zu schützen, ist ein besonders sichtbares Beispiel. In **Russland**, das FRT derzeit stark ausbaut, klagen Menschenrechtsverteidiger_innen gegen die Anwendung von FRT zur Überwachung von Demonstrationen und die diesbezügliche Speicherung ihrer Daten.[36]

Die Auswirkungen von Überwachung auf die Versammlungsfreiheit hat das **BVerfG** bereits 1983 zusammengefasst: "Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise **auf eine**

33 FRA, 2019, Fundamental Rights Survey, https://fra.europa.eu/en/project/2015/fundamental-rights-survey

34 BVerfG, 12/2018, Beschluss des Ersten Senats vom 18. Dezember 2018 - 1 BvR 142/15 -, http://www.bverfg.de/e/rs20181218_1bvr014215.html

35 Für einen Überblick vgl.Ella Jakubowska, 05/2020, Ban Biometric Mass Surveillance, https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance

36 Amnesty International, 01/2020, Russia: Intrusive facial recognition technology must not be used to crackdown on protests, https://www.amnesty.org/en/latest/news/2020/01/russia-intrusive-facial-recognition-technology-must-not-be-used-to-crackdown-on-protests/

Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten **freiheitlichen demokratischen Gemeinwesens** ist."[37]

Insbesondere in Staaten, in denen Menschen gefährdet sind, für Protest inhaftiert zu werden, ihren Arbeitsplatz oder gar ihr Leben zu verlieren, ist Gesichtserkennung ein Instrument, das **jeglichen Protest ersticken** könnte. Es **multipliziert das Machtungleichgewicht** zwischen Staat und Bevölkerung um ein Vielfaches. Doch auch in Staaten, in denen die Teilnahme an Demonstrationen in den meisten Fällen weniger Risiken aufweist, wirkt FRT lähmend. Anlässlich einer Untersuchung des dreijährigen Probeeinsatzes von FRT durch die London Metropolitan Police antworteten insbesondere junge Menschen (38%) und People of Colour, dass sie ein Gebiet meiden würden, wenn dort FRT eingesetzt würde.[38]

Auswirkungen auf das Recht auf Gleichheit und Nicht-Diskriminierung

FRT kann massive **Auswirkungen auf marginalisierte Gruppen** haben und das Recht auf Gleichheit und Nichtdiskriminierung untergraben.

Erstens ist FRT aufgrund ihrer technischen Funktionsweise besonders geeignet, gezielt gegen Personen mit bestimmten in der Antidiskriminierungsgesetzgebung geschützten Merkmalen eingesetzt zu werden, da sich diese in Gesichtsmerkmalen niederschlagen (etwa bei ethnischer Zugehörigkeit, Alter oder Geschlecht).[39] Chinesische Wissenschaftler_innen publizierten staatlich finanzierte Untersuchungen zu den **Fähigkeiten von FRT, Menschen anhand ihrer ethnischen Zugehörigkeit zu kategorisieren**.[40] Berichten zufolge bewarb der chinesische Hersteller Hikvision seine FRT-fähigen Kameras damit, dass sie zwischen **Uiguren and Han-Chinesen unterscheiden** könnten (der Hersteller löschte diese Werbung nach kritischen Medienanfragen von seiner Webseite).[41] **Chinesische Behörden nutzen FRT als wichtigen Baustein des Überwachungsapparates in der Region Xinjiang**.[42] FRT weist das grundsätzliche Risiko auf, von Staaten (oder privaten Akteur_innen) eingesetzt zu werden, um zwischen Menschen auf Grundlage geschützter Merkmale zu unterscheiden, die Bewegungen dieser Menschen weiter aufzuzeichnen, sie zu diskriminieren und - wie im Falle Chinas - zu verfolgen. Kategorisieren und Diskriminieren können zwar auch Menschen, FRT ermöglicht dies aber in einem automatisiertem, potentiell unsichtbaren und ungleich viel größerem Umfang.

---

37 BVerfG, 12/1983, 15.12.1983, BVerfGE Bd. 65, S. 1 ff ("Volkszählungsurteil"), https://www.bverfg.de/e/rs19831215_1bvr020983.ht

38 London Policing Ethics Panel, 05/2019, Final Report on Live Facial Recognition, http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/live_facial_recognition_final_report_may_2019.pdf

39 Kaye, 05/2019, Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/18/PDF/G1914818.pdf?OpenElement

40 Cunrui Wang, Qingling Zhang, Wanquan Liu, Yu Liu, Lixin Miao, 2018, Facial feature discovery for ethnicity recognition, https://onlinelibrary.wiley.com/doi/full/10.1002/widm.1278; Lu Qiao1, Yajun Yang, Pengcheng Fu, Sile Hu, Hang Zhou, Jingze Tan, Yan Lu, Haiyi Lou, Dongsheng Lu, Sijie Wu, Jing Guo, Shouneng Peng, Li Jin, Yaqun Guan, Sijia Wang, Shuhua Xu, Kun Tang, 2016, Detecting Genome-wide Variants of Eurasian Facial Shape Differentiation: DNA based Face Prediction Tested in Forensic Scenario, https://www.biorxiv.org/content/biorxiv/early/2016/07/11/062950.full.pdf;

41 Charles Rollet, 11/2019, Hikvision markets Uyghur Ethnicity Analysis, now covers up,]https://ipvm.com/reports/hikvision-uyghur

42 Amnesty International, 09/2018, Up to one million detained in Chias Mass "Re-Education" drive, https://www.amnesty.org/en/latest/news/2018/09/china-up-to-one-million-detained/; Paul Mozur, 04/2019, One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

Zweitens weisen die existierenden Gesichtserkennungssysteme besonders hohe Fehlerraten bei Personen auf, die zu marginalisierten Gruppen gehören. Beim Einsatz von FRT können diese daher häufiger etwa unschuldig ins Visier von Strafverfolgung geraten, was zu individueller Diskriminierung sowie zu **"overpoliced Communities"** beiträgt. Untersuchungen bestätigen regelmäßig, dass FRT höhere **Fehlerraten für People of Color und Frauen** aufweist. Die Ursache hierfür liegt in den für das "Training" der zugrundeliegenden Algorithmen genutzten (teils kommerziell verfügbaren) Datensets, die wenig Vielfalt aufweisen und in denen weiße Männer überrepräsentiert sind (dem sogenannten **"historic bias"**). Die American Civil Liberties Union (ACLU) verglich in einem Feldversuch die Fotos der US Repräsentantenhaus mit Hilfe der kommerziell frei verfügbaren Amazon-FRT "Rekognition" (Kosten: $12,33) mit einer Liste von 25 000 Straftäter_innen. Die Software schlug 28 Politiker_innen als Kriminelle vor. Davon waren 40% People of Colour, obgleich diese im Kongress nur 20% der Mitglieder stellen.[43] Auch bei FRT gibt es dabei **intersektionale Diskriminierung**, d.h. wer mehrere Merkmale aufweist, ist besonders betroffen - etwa schwarze Frauen. FRT hat außerdem Probleme, **nicht-binäre oder genderfluide** Menschen zu identifizieren.[44] Unzureichend untersucht ist bisher, wie fehlerhaft FRT bei der Identifizierung von Menschen mit Behinderung und Menschen mit Gesichtsoperationen arbeitet.

Die beschriebene Diskriminierung wird zusätzlich dadurch verstärkt, dass etwa in den USA People of Colour in polizeilichen Fotodatenbanken überrepräsentiert sind, so dass es für sie eher zu fehlerhaften "Matches" kommt.

Ihrer Natur nach sind Maschinelle Lernsysteme wie FRT prädisponiert, vorhandene Vorurteile weiterzutragen und zu verstärken. Amnesty Internationals **"Toronto-Declaration"** erklärt das Zusammenspiel von KI und Diskriminierung, möglicherweise auch ohne dass sich Nutzer_innen der Risiken bewusst sind.[45]

Das zweite Problem - die höhere Fehlerrate - ist prinzipiell zukünftig behebbar. In der Tat wird FRT immer präziser auch beim Erkennen der genannten Gruppen. Insbesondere teure, hochentwickelte FRT-Systeme haben hierbei in den jüngsten Jahren enorme Fortschritte gemacht.

Das erste Problem ergibt sich jedoch aus der Funktionsweise von FRT, ist insofern nicht behebbar und kann - im besten Fall - nur durch **menschenrechtliche Safeguards wie eine effektive Anti-Diskrimierungs-Gesetzgebung abgeschwächt** werden. Es gibt zudem ein Wechselspiel beider Probleme: Wo FRT genutzt wird, um gezielt eine Gruppe z. B. aufgrund ihrer ethnischen Zugehörigkeit herauszufiltern und zu verfolgen, bringt eine Optimierung ihrer Fehlerraten keine Verbesserung, sondern gerade eine Verschlechterung der Situation für die Betroffenen mit sich. Auch das UN Committee on the Elimination of Racial Discrimination **(CERD)** warnt, der Einsatz von FRT gefährde die Rechte marginalisierter Gruppen, darunter die Rechte auf Informations-, Versammlungs- und Vereinigungsfreiheit.[46])

---

[43] Jacob Snow, 07/2018, Amazon's Facial Recognition Software Falsely Matched 28 Members of Congress With Mugshots, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

[44] Stefan Wojcik, Emma Remy, 09/2015, The Challenge of Using Machine Learning to Identify Gender in Images, https://www.pewresearch.org/internet/2019/09/05/the-challenges-of-using-machine-learning-to-identify-gender-in-images/

45 The Toronto Declaration, https://www.torontodeclaration.org/

46 Committee on the Elimination of Racial Discrimination (CERD), 05/2019, Draft General Recommendation No. 36 on preventing and combating racial profiling.

FRT stellt bereits ihrer Funktionsweise nach ein tiefgreifendes Risiko für das Recht auf Nicht-Diskrimierung dar, das nicht grundsätzlich behoben werden kann.

Auswirkungen auf das Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren

FRT stellt eine schwerwiegende Herausforderung für das Recht auf einen effektiven Rechtsbehelf dar, da Betroffene möglicherweise **nicht wissen**, ob ihr Gesicht erfasst wurde. Aufgrund des **Opakheit**, also der mangelnden Einsehbarkeit und Nachvollziehbarkeit der Entscheidungen von deep-learning KI, kann es zusätzlich unmöglich sein, herauszufinden, **wie das FRT-System zu einer Entscheidung kam**. Dies ist angesichts der bei den meisten Systemen noch immer hohen **Fehlerraten** von besonderer Bedeutung. Selbst bei einer scheinbar geringen prozentualen Fehlerrate werden angesichts der Masse der algorithmisch verarbeiteten Gesichter in stark frequentierten öffentlichen Räumen viele Menschen **falsch identifiziert und ggf. zu Unrecht durch die Polizei kontrolliert, in manchen Ländern möglicherweise auch inhaftiert oder gefoltert**.[47]

Die Notwendigkeit einer Regulierung

In den letzten Jahren hat der Einsatz von FRT stark zugenommen. Eine weitere Expansion ist anzunehmen: FRT wird **zunehmend kostengünstiger**, die zugrundeliegenden KI Anwendungen immer **präziser**, es ist zunehmend mehr **Rechenstärke verfügbar** und durch weiter zunehmende Verbreitung von Social Media finden sich immer Bilder von Gesichtern im Internet. Die Versprechungen der Hersteller steigen - so wirbt Amazon auf seiner Webseite damit, seine FRT-Software “Rekognition” könne nun auch Angst erkennen[48]. Neue Anwendungsfälle werden erprobt, teils mit massiven Menschenrechtsrisiken. Berichten zufolge stellt der türkische Staatskonzern KARGU eine Kamikaze-Drohne mit Gesichtserkennung her, “die Ziele auf Basis automatisierter Gesichtserkennung ausmache”.[49]

All dies geschieht spielt sich in einem weltweiten **Regulierungsvakuum** ab, da Entwicklung und Einsatz von FRT die **Gesetzgebung überholt** haben - ein häufiges Problem für die Gewährleistung eines effektiven Schutzes der Menschenrechte im digitalen Zeitalter. Der Mangel an Regulierung und Kontrollmechanismen hinsichtlich Entwicklung, Verkauf und Einsatz ist angesichts der gravierenden Menschenrechtsrisiken alarmierend. Eingriffe in Menschenrechte dürfen nur auf einer klaren gesetzlichen Grundlage stattfinden. Sofern klare Regulierungen existieren, handelt es sich um **ad hoc Maßnahmen** auf lokaler Ebene, die oft auf Grundlage zivilgesellschaftlicher Initiativen entstanden. Eine solche positive Ausnahme stellen einige Städte in den USA dar, die 2019 und 2020 FRT im öffentlichen

---

[47] vgl. zu Fehlerraten für Deutschland anlässlich des Pilotprojektes Südkreuz Stellungnahme Chaos Computer Club: 10/2018, Biometrische Videoüberwachung: Der Südkreuz-Versuch war kein Erfolg, https://www.ccc.de/en/updates/2018/debakel-am-suedkreuz

[48] Amazon, 08/2019, Amazon Rekognition verbessert Gesichtsanalyse, https://aws.amazon.com/de/about-aws/whats-new/2019/08/amazon-rekognition-improves-face-analysis/

[49] heise online, 11/2019, Studie: Auf der schiefen Bahn zu Killer-Robotern, https://www.heise.de/newsticker/meldung/Studie-Auf-der-schiefen-Bahn-zu-Killer-Robotern-4584790.html Unklar ist, ob die KARGU-Drohne eine spezifische Person oder nur überhaupt ein Gesicht (also die Anwesenheit eines Menschen) erkennt. Deutlich macht das Beispiel in jedem Fall, welche Einsatzgebiete für FRT künftig denkbar sind.

Raum im Grundsatz verboten haben. Auch **Rechtssprechung** ist bisher kaum zu finden. Im September 2019 urteilte der UK High Court über den weltweit ersten expliziten FRT-Fall.[50]

Auf **globaler Ebene fehlt es an einer Regulierung von biometrischer Überwachung** inklusive Gesichtserkennung. Zwar gibt es Bemühungen, internationale Standards durch die **Vereinten Nationen** zu etablieren. Auf geleakten Dokumenten beruhenden Berichten der Financial Times zufolge wurde die Initiative der UN International Telecommunication Union allerdings von IT-Unternehmen ins Leben gerufen, darunter chinesischen FRT-Anbietern, die in der Provonz Xinjiang aktiv sind.

Auf europäischer Ebene existieren ebenfalls eher Versatzstücke eines Regulationsrahmens. Auf FRT anwendbare - teils verbindliche, teils eher unverbindliche - Dokumente sind

- Directive 2016/680 Data Protection Law Enforcement Directive (Art. 10, Anwendung auf Strafverfolgungsbehörden)
- Regulation 2016/679 General Data Protection Regulation (GDPR) (Art. 9, keine Anwendung bei Strafverfolgungsbehörden)
- EU Agency for Fundamental Rights (FRA), Facial Recognition Technology : fundamental rights considerations in the context of law enforcement.
- Europäischer Datenschutzausschuss, Guidelines 3/2019 on processing of personal data through video devices
- Working Party 29, Opinion 3/2012 on developments in biometric technologies
- European Commission (EC), White Paper on AI

Art. 10 der Richtlinie 2016/680 verlangt zur Verarbeitung biometrischer Daten für Zwecke der Strafverfolgung eine strikte Erforderlichkeitsprüfung. Amnesty International ist der Ansicht, dass identifizierende Videoüberwachung im öffentlichen Raum unverhältnismäßig ist und dieser Prüfung nicht gerecht werden kann.

Einer Untersuchung der Organisation AlgorithmWatch[51] nutzt die Polizei **in mindestens zehn EU-Ländern** aktuell Software zur Gesichtserkennung. Acht weitere wollen die Technik demnach bald einführen. Nach Angaben von AlgorithmWatch enthalten die Datenbanken zum Beispiel in den **Niederlanden** auch Fotos von Verdächtigen, die nie eines Verbrechens angeklagt wurden. Die EU-Grundrechteagentur kritisiert einen **Mangel an Transparenz** und die Schwierigkeit, an Informationen über den Einsatz und insbesondere Tests von FRT zu gelangen[52], die im Übrigen weltweit besteht, so dass präzise Zahlen über die Verbreitung von FRT fehlen.

Innerhalb der EU haben nationale Datenschutzaufsichten wie die französische CNIL, ICO in UK und Schwedens Datainspektionen die Sorge geäußert, dass **viele derzeitige Anwendungen illegal** sind.[53] Wie die **EU Grundrechteagentur** kritisiert, gibt es in der EU

---

[50] UK Hight Court, 04/09 2019, https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf

51 Nicolas Kayer-Brill, 12/2019, AlgorithmWatch deckt auf: In mindestens 10 EU Staaten nutzt die Polizei automatisierte Gesichtserkennung, https://algorithmwatch.org/story/polizei-gesichtserkennung-europa/

52 FRA, 2019, Facial recognition technology: fundamental rights considerations in the context of law enforcement https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

53 Ella Jakubowska, 05/2020, Ban Biometric Mass Surveillance, https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf, S.8

trotz des bestehenden Einsatzes von FRT außerdem keine Regularien dazu, wie und warum welche Personen auf eine **"Watchlist"** aufgenommen werden.[54]

Das **Weißbuch** der EU zur Künstlichen Intelligenz erwog in einer geleakten früheren Entwurfsversion ein bis zu 5-jähriges **Moratorium für Gesichtserkennung** im öffentlichen Raum durch öffentliche wie private Akteure. In der im Februar 2020 veröffentlichen Version ist dieser Vorschlag bedauerlicherweise nicht mehr zu finden. FRT wird, wie andere biometrische Überwachung, zwar als "high risk" Technologie eingestuft, was zweifellos richtig ist, aber leider ohne Konsequenzen bleibt.

Nach Ansicht von Amnesty International braucht es mit hoher Dringlichkeit

- **einen sofortigen Stop der Verwendung**, Entwicklung, Produktion, des Verkaufs und des Exports von Gesichtserkennungstechnologien zu Identifikationszwecken im öffentlichen Raum sowohl durch staatliche Stellen als auch durch Akteure des privaten Sektors. Hierfür sollte sich die Bundesregierung innerhalb der EU und auf internationaler Ebene einsetzen sowie für Deutschland mit gutem Beispiel vorangehen. Deutschland sollte den UN Sonderberichterstatter für das Recht auf Meinungsfreiheit, David Kaye, in seiner Forderung nach einem **weltweiten Überwachungstechnologie-Moratorium**, darunter FRT, unterstützen.[55]
- Zur dringend notwendigen Reform der Regulierung der **Exportkontrolle** von u.a. Gesichtserkennungstechnologie siehe Antwort auf Frage 11.
- eine adäquate finanzielle und personelle Ausstattung der nationalen **Datenschutzbehörden** der EU Mitgliedstaaten sowie ähnlicher Instrumente weltweit
- die rechtlich verbindliche Festlegug von **menschenrechtlichen Sorgfaltspflichten** im Sinne der UN Leitprinzipien für Wirtschaft und Menschenrechte für private Unternehmen, die in nahezu allen Einsatzfällen von FRT beteiligt sind - mindestens durch Entwicklung und Verkauf, oftmals darüber hinaus (z.B. Clearview AI[56]). Hierfür sollte die Bundesregierung ein **nationales Gesetz** erlassen und sich **auf EU-Ebene** (auch im Rahmen der Ratspräsidentschaft) sowie multilateral, etwa im Rahmen des **UN Treaty Process**, engagieren. Sorgfaltspflichten komplementieren sinnvoll Regulierungen privater Akteure wie die DSGVO.
- Bei der **öffentlichen Beschaffung und Zusammenarbeit** mit privaten Unternehmen sollten staatlicher Stellen nur auf private Akteure zurückgreifen, die Sorgfaltspflichten umsetzen und nicht in Menschenrechtsverletzungen involviert sind.
- Staaten weltweit sollten **Transparenzberichte** über den tatsächlichen sowie geplanten Einsatz (inklusive Testeinsätze), die Ziele, involvierte Akteure, Rechtsgrundlagen und menschenrechtliche Einschätzungen aller biometrischen Datenerhebung und -verwendung veröffentlichen. Dies ermöglicht demokratische Kontrolle und zivilgesellschaftliche Debatte. Die Bundesregierung sollte mit gutem Beispiel vorangehen.

---

54 FRA, 2019, Facial recognition technology: fundamental rights considerations in the context of law enforcement https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

55 Kaye,05/2019, Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/18/PDF/G1914818.pdf?OpenElement https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/18/PDF/G1914818.pdf?OpenElement

56 Vgl. https://clearview.ai/ sowie Kashmir Hill, 01/2020, The Secretive Company That Might End Privacy as We Knwon It, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

- **Öffentliche Fördergelder** dürfen nicht die Entwicklung von Technologie fördern, die Menschenrechte verletzten. Diesbezüglich fragwürdige Fälle gab es etwa im Kontext von EU Horizon 2020[57].
- Auch FRT, die nicht identifizierende FRT im öffentlichen Raum darstellt, bringt teils massive Menschenrechtsrisiken mit sich und geht regelmäßig mit auch tiefgreifen Eingriffen in Menschenrechte einher. Sie muss geeignet und notwendig zum Erreichen eines legitimen Zieles sein und den Test der **Verhältnismäßigkeit** bestehen. Ihr Einsatz benötigt eine den Kriterien der Rechtssicherheit genügende **gesetzliche Grundlage**. Diese sollte u.a. klare Regeln für die Erhebung, Speicherung, den Zugang zu und die Löschfristen von **Daten** enthalten. Eine Protokollierung, die Information der betroffenen Personen und eine unabhängige **Kontrolle** muss sichergestellt und der Rechtsweg möglich sein.
- Die von Amnesty International und Acccess Now entwickelte "Toronto Declaration"[58] enthält weitere menschenrechtliche **Anforderungen an den Einsatz von KI**, um insbesondere das Recht auf Gleichheit und Nicht-Diskriminierung zu schützen. Sie ist auch auf FRT anwendbar. Die Erklärung richtet sich an Staaten und private Akteure und enthält auch einen Abschnitt zum Zugang zu Recht.

5. Können Sie konkrete Beispiele nennen, in denen das Darknet – genauer: die helle Seite des Darknets – Journalisten und Menschenrechtlern unter dem Schutz der Anonymität Austausch, Recherche und das Aufdecken von Missständen in Autokratien und Diktaturen erst ermöglicht, also Voraussetzung für jede regimekritische Tätigkeit ist, und wie bewerten Sie in diesem Zusammenhang den vom BMI geforderten Darknetparagraphen? (SPD)

Der nicht trennscharfe, umgangssprachliche **Begriff "Darknet"** bezeichnet einen Teil des Internets, der nicht durch gängige Browser oder Suchmaschinen aufrufbar ist. Werkzeuge wie **Tor-Browser** erlauben es, Darknet-Seiten direkt (d.h. die URL muss bekannt sein) oder über Darknet-Suchmaschinen und Adressbücher aufzurufen.

Ein konkretes Beispiel im Sinne der Frage ist die Whistleblowing-Software GlobaLeaks, die auf "Darknet"-Diensten basiert, um die Identität der Whistleblower zu schützen. Sie ist enorm weit und in über 20 Sprachen verbreitet, zahlreiche NGOs, Medien und Initiativen greifen oder griffen auf sie zurück, darunter **Transparency International und Amnesty International**. Auch die **italienische Anti-Korruptionsbehörde** erlaubt es über eine GlobaLeaks Anwendung, Korruptionsfälle zu melden, und greift dafür auf Onion Services zurück.

Der vom **BMI** geforderte **Strafrechts-Paragrafen 126a / Darknet-Paragraph** könnte nach Analyse renommierter Juristen[59] dazu führen, Personen zu kriminalisieren, die

57 Nach Berichte der NGO EDRi verfolgen mit dem Horizon 2020 finanzierten Projekt "SPIRIT" fünf strafverfolgungsnahe Akteure aus vier EU-Staaten das Projektziel, FRT mit Social Media Informationen und vielen weiteren Quellen zu verknüpften: Ella Jakubowska, 05/2020, Ban Biometric Mass Surveillance,https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf S. 32. Vgl. für weitere fragwürdige Projekte Daneil Leufer, Fieke Jansen,01/2020, The EU is funding dystopian Artificial Intelligence projects, https://www.euractiv.com/section/digital/opinion/the-eu-is-funding-dystopian-artificial-intelligence-projects/

58 The Toronto Declaration, https://www.torontodeclaration.org/declaration-text/english/

59 Matthias Bäcker, Sebastian Golla, 03/2019, "Darknet"-Gesetz bedroht sozial wünschenswerte Internet-Dienste

Anonymisierungs- und Verschlüsselungsdienste bzw. deren Infrastruktur zur Verfügung stellen. Bei der Bereitstellung von Tor-Infrastruktur ist **Deutschland das aktivste Land**[60]. Eine Kriminalisierung des Betreibens von Tor-Infrastruktur in Deutschland hätte daher massive Auswirkungen weltweit. Eine Kriminalisierung von Tor und verwandten Werkzeugen ginge mit einem **enormen menschenrechtlichen und auch darüber hinausgehenden Kollateralschaden** einher und wäre nach Ansicht von Amnesty International trotz des legitimen, wichtigen Ziels des Gesetzes **unverhältnismäßig.**

Tor-Browser ermöglichen ein weitgehend **anonymisiertes, verschlüsseltes** Surfen. Viele **Menschenrechtsverteidiger_innen**, Journalist_innen und andere Menschen nutzen Tor und ähnliche Werkzeuge für ihre Recherchen, direkten Zugang zu Wissen oder Gesundheitsinformationen. **Auch Amnesty International nutzt Tor** für eigene Recherchen und um an zensierte Informationen zu gelangen. Außerdem basieren eine Reihe von Sharing-Anwendungen, über die Kommunikation und Dokumente ausgetauscht werden können, auf Onion Services, etwa das von Exilmedien genutzte OnionShare. Auch **größere Internetdienste** integrieren diese in ihre Produkte, darunter etwa Firefox. Je nach Definition gehört sogar der größte Teil des Internets, nämlich etwa Bankserver, Systeme von Krankenhäusern, Datenbanken, DNS-Server etc. zum Darknet (manchmal wird dieser Teil auch als deep web bezeichnet, in jedem Fall handelt es sich um Bereiche, die nicht von jedem aufgerufen werden können).

Im Übrigen wird Tor **in der überwiegenden Zahl** der Fälle genutzt, um “normale” Seiten und Dienste im World Wide Web aufzurufen und auch dabei den Schutz der Anonymität zu haben und/oder Zensur zu umgehen.

7. Wie können die Rechte von MenschenrechtsverteidigerInnen, AktivistInnen, JournalistInnen und politischen Oppositionellen weltweit in Zukunft besser im digitalen Raum geschützt werden? (FDP)

8. Wie können wir die politische Beteiligung im digitalen Zeitalter fördern und gleichzeitig Menschenrechte schützen, und welche neuen Möglichkeiten bieten digitale Technologien für den Schutz der Menschenrechte und die Stärkung politischer Beteiligung, ohne die am meisten benachteiligten Menschen zurückzulassen? (DIE LINKE.)

Die Fragen 7 und 8 werden gemeinsam beantwortet. Sie sind recht umfassend, weshalb die folgenden Vorschläge nur sehr knapp begründet werden, um den Rahmen dieser Stellungnahme nicht zu sprengen.

- Zu den dringend notwendigen Maßnahmen gegen den **Handel** mit digitalen Technologien, die ein Menschenrechtsrisiko aufweisen, **siehe Antwort auf Frage 12**.
- **Verbot** von Technologien mit unvertretbaren Menschenrechtsrisiken. Es braucht beispielsweise ein umfassendes nationales und internationales Verbot der Entwicklung, der Herstellung und des Einsatzes von **autonomen tödlichen und weniger tödlichen Waffensystemen** oder des Einsatzes von **Gesichtserkennung**

---

https://netzpolitik.org/2019/darknet-gesetz-bedroht-sozial-wuenschenswerte-internet-dienste/

60 heise online, 01/2019, Missing Link: Von Zwiebeln, Knoten und Moneten- der Anonymisierungsdienst Tor in Zahlen https://www.heise.de/newsticker/meldung/Missing-Link-Von-Zwiebeln-Knoten-und-Moneten-Tor-in-Zahlen-4287404.html?seite=2

zur Identifizierung im öffentlichen Raum (siehe dazu auch Fragen 4 und 12) auf nationaler, supranaterionaler und internationaler Ebene.

- Förderung und gesetzliche Verankerung von **Netzneutralität**. Angebote wie **"Facebook Free Basics"** verletzen die Netzneutralität. Einen gleichberechtigten Zugang zum Internet für alle Menschen weltweit zu gewährleisten, der niemanden zurücklässt, darf nicht allein Unternehmen überlassen werden.
- **Überwachung** darf nur stattfinden, wenn ein hinreichender Verdacht vorliegt und die Überwachungsmaßnahme gezielt, verhältnismäßig, durch eine unabhängige Instanz kontrolliert und notwendig zum Erreichen eines legitimen Ziels ist. Deutschland sollte mit gutem Beispiel vorangehen, BND- und G10-Gesetz entsprechend reformieren und die unabhängige Kontrolle von Nachrichtendiensten und Polizeien verbessern.
- **Internet-Plattformen** müssen die Menschenrechte wahren und entsprechend reguliert werden. In einem ersten Schritt sollte es Unternehmen **untersagt werden, den Zugang zu ihren Diensten davon abhängig zu machen, dass Nutzer_innen der Erhebung und Verwendung ihrer persönlichen Daten** zu Werbezwecken „zustimmen". Starke **Datenschutz- und Anti-Diskriminierungsgesetze, Privacy by design and by default, Datenportabilität und Interoperabilität** sind wichtige Kernelemente einer Regulierung. Diese dürfte auf Unterstützung treffen: Nach einer **Umfrage**[61] von Amnesty International in Deutschland halten es 70% aller Befragten für ein Problem, dass ihre Daten zur Erstellung **detaillierter Profile und gezielter Werbung** genutzt werden. 63% finden, dass die Bundesregierung „Big Tech" strenger regulieren sollte. **Nur 16% sehen keinen Handlungsbedarf.**
- Aus der staatlichen Verpflichtung, die Menschenrechte nicht nur zu achten, sondern auch zu schützen und zu gewährleisten, ergibt sich die Verpflichtungen, staatlicherseits die Sicherheit der Online-Kommunikation zu gewährleisten. Dazu gehört die **Identifizierung und Reparatur von Sicherheitslücken**. Insbesondere darf die Sicherheit technischer Infrastrukturen nicht unterminiert werden (etwa durch das Ausüben von Druck auf Herstellerfirmen, **Backdoors** einzubauen, oder das Vorrathalten oder gar Ankaufen von **Zero-Day-Schwachstellen**). Unbekannte IT-Sicherheitslücken gefährden unzählige Nutzer_innen – von der eigenen Verwaltung und Bevölkerung über zahlreiche Unternehmen bis hin zu Menschenrechtsverteidiger_innen in anderen Ländern.
- Förderung der Sicherheit und Zugänglichkeit digitaler Kommunikation (Infrastruktur ebenso wie Kenntnisse und Policies) von Bevölkerung und Zivilgesellschaft im eigenen Land und weltweit. Förderung von Ende-zu-Ende-**Verschlüsselung**[62] und von Werkzeugen zur **Anonymisierung** (insbesondere dürfen diese nicht behindert werden, siehe dazu Antwort auf Frage 5), **Haftung** von IT-Herstellern und Diensteanbietern für Mängel des Privatsphärenschutzes und IT-Sicherheitsmängel, **Privacy and Security by Design and Default** durch Förderungen, Anreize, gesetzliche Vorgaben und im Vergaberecht.
- **Einführung verbindlicher menschenrechtlicher Sorgfaltspflichten** für Unternehmen im Sinne der UN Leitprinzipien für Wirtschaft und Menschenrechte. Eine verbindlich vorgeschriebene Risikoanalyse der eigenen Unternehmenstätigkeit mit Durchführung entsprechender Gegenmaßnahmen hätte Auswirkungen auf ein

[61] Amnesty International, 12/2019, 6 von 10 Deutschen fordern bessere Regulierung beim Datenschutz, https://www.amnesty.de/allgemein/pressemitteilung/deutschland-amnesty-umfrage-6-von-10-deutschen-fordern-bessere

[62] Ausführlich hierzu: https://www.amnestyusa.org/wp-content/uploads/2017/04/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf. Siehe auch

breites Spektrum von Menschenrechtsrisiken von Hate Speech auf Social Media Plattformen bis zum Einsatz von KI.

11. Autokratien und Diktaturen nutzen u. a. aus europäischen Ländern stammende Überwachungssoftware, um Journalisten, Bürgerrechtler, Menschenrechtsverteidiger u. a. zu „durchleuchten“ und zu überwachen – oft mit gravierenden persönlichen Folgen für die Betroffenen. Bedarf es hier weiterer Vorgaben für den Export von Überwachungssoftware? (SPD)

Diese Frage lässt sich **mit einem klaren Ja beantworten**. Die derzeitige Exportkontrolle für Überwachungssoftware ist **lückenhaft, wenig effektiv und sehr langsam.**

Exportkontrolle in der Europäischen Union

Für Deutschland und andere Mitgliedsstaaten der EU ist die Exportkontrolle insbesondere auf der europäischen Ebene verankert. Diese weist unter anderem folgende Probleme auf:

Nicht alle Güter, die zu Menschenrechtsverletzungen beitragen, sind von den Exportkontrolle erfasst. So ist es derzeit etwa möglich, **Software zur Gesichtserkennung nach China zu exportieren, ohne, dass die dortige Menschenrechtslage eine Rolle spielt**, da biometrische Überwachungstechnologie derzeit nicht von der für die Exportkontrolle von Überwachungstechnologie zuständigen **Dual Use Verordnung** erfasst wird.

Die Verordnung reagiert zudem **sehr langsam** auf die Entwicklung neuer Technologien. Anhang I der Verordnung enthält eine Liste der Waren, für die eine Ausfuhrgenehmigung aus der EU gesetzlich vorgeschrieben ist. Diese gemeinsame Kontrollliste von Dual Use Gütern implementiert verschiedene multilaterale Exportkontrollregelungen, darunter insbesondere das Wassenaar-Arrangement. Jedes dieser Kontrollsysteme verfügt über eine eigene, international vereinbarte Kontrollliste. Entscheidungen über die Kontrolle von Gütern werden daher durch die jeweiligen multilateralen Kontrollsysteme getroffen und erst danach in den Anhang der Dual Use Verordnung übernommen. Dieser Prozess bedarf der Zustimmung vieler internationaler Akteure und **dauert regelmäßig mehrere Jahre**, womit die Kontrolle dem **sehr schnellen Entwicklungszyklus im IKT-Bereich** nicht annähernd gerecht werden kann.

Der derzeitigen Exportkontrolle **mangelt es zudem an Transparenz** über die vergebenen Exportlizenzen und an der Implementierung **menschenrechtlicher Sorgfaltspflichten** durch die Herstellerunternehmen.

Der schnelle technische Fortschritt macht Regulierung in diesem Bereich zwar besonders anspruchsvoll. Die **EU Kommission** hat in ihrem ersten Vorschlag[63] zur Reform der EU Dual Use Verordnung jedoch bereits sinnvolle Vorschläge gemacht, wie die gegenwärtige, lückenhafte Exportkontrolle von Überwachungssoftware verbessert werden kann. Auch die

[63] Nach dem Arabischen Frühling betonte das Europäische Parlament in verschiedenen Resolutionen die Bedeutung der Exportregulierung von Überwachungstechnologie. Das Parlament wies unter anderem auf den „sehr unvollständigen Charakter” der Dual Use Regulierung hin, “wenn es um eine wirksame und systematische Exportkontrolle schädlicher IKT-Technologien in nichtdemokratische Länder geht“. Die Einwände des Parlaments wurden von der Europäischen Kommission aufgegriffen, die 2016 einen umfassenden Vorschlag zur Neufassung der Verordnung Nr. 428/2009 vorlegte. Am 17. Januar 2018 nahm das Parlament den Vorschlag mit einer Reihe von Änderungen an.

Vorschläge des Parlamentes wurden von Menschenrechtsorganisationen, darunter Amnesty International, allgemein begrüßt.

Amnesty International ist besorgt über die sich seitdem anschließenden, langwierigen und wenig ambitionierten Verhandlungen des Rates und den jüngsten Kompromissvorschlag der Kommission, **der weit hinter dem ursprünglichen Vorschlag zurückbleibt.**

Folgende Punkte sollten umgesetzt werden, um die genannten Probleme abzustellen und einen Schutz der Menschenrechte[64] beim Handel mit Überwachungstechnologie zu gewährleisten:

- Eine **hinreichend breite Definition** des Gegenstands der Kontrolle, um auch neue Technologien wie etwa biometrische Überwachung und Systeme zur Vorratsdatenspeicherung zu umfassen;
- **Menschenrechtliche Sorgfaltspflichten** für die exportierenden Unternehmen entlang der UN Leitprinzipien für Wirtschaft und Menschenrechte. Diese sollten ihre Exporttätigkeiten unter anderem auf Menschenrechtsrisiken prüfen müssen, diesen vorbeugen und gegebenenfalls vom Verkauf absehen.
- Schnelle und effektive Verfahren, um neue Güter in den Anhang der Verordnung zu übernehmen, also der Kontrolle zu unterwerfen. Eine Möglichkeit hierfür stellt eine sogenannte **EU-autonome Liste** dar.
- Ein Verfahren, um Exporte von Gütern auch dann zu stoppen, wenn sie nicht in der Liste der zu kontrollierenden Güter verzeichnet sind – aber dennoch ein Risiko für die Menschenrechte darstellen. **("Catch-All")**
- **Menschenrechtsaspekte** müssen ein **normatives Kriterium** für die Entscheidung über die Vergabe von Exportgenehmigungen an die europäischen Unternehmen darstellen. Staaten dürfen keine Genehmigungen erteilen, wenn ein signifikantes Risiko besteht, dass der Export zu Menschenrechtsverletzungen beiträgt.
- **Mehr Transparenz** darüber, für welche Güter nationale Behörden der Mitgliedsstaaten eine Exportgenehmigung erteilt oder verweigert haben, einschließlich der Art, Wertes, Ziellandes und letztlichen Nutzers.

Die kommende **EU-Ratspräsidentschaft** bietet für Deutschland eine besondere Chance, sich für die **Umsetzung** dieser Reformpunkte stark zu machen.

Insbesondere angesichts der praktischen Schwierigkeiten, einen Konsens auf europäischer Ebene zu erreichen, sollte die Bundesregierung aber auch **mit gutem Beispiel vorangehen**. Sie sollte die Möglichkeiten nach Artikel 8 Dual Use Verordnung nutzen, über den europäischen Status Quo hinausgehende **nationale Genehmigungspflichten** für Güter zu erlassen, die nicht in Anhang I aufgeführt sind, sowie **mehr Transparenz herzustellen**.

Exportkontrolle weltweit

Jenseits der europäischen Ebene ist die Exportkontrolle von Überwachungstechnologie vielfach noch lückenhafter, sieht **keine Berücksichtigung von Menschenrechtskriterien** vor oder **findet praktisch nicht statt**. Ungünstig komplementiert wird diese mangelhafte

[64] Darüber hinausgehend gibt es außerdem eine sicherheits- und wirtschaftspolitische Dimension: Die exportierte Technik kann auch für Militär- und Wirtschaftsspionage genutzt werden und dies auch gegen die Staaten, aus denen sie exportiert wurde.

staatliche Kontrolle durch fehlende menschenrechtliche Sorgfaltspflichten seitens der exportierenden Unternehmen. So ist es einem der wichtigsten Herstellerunternehmen von Überwachungssoftware, der **israelischen NSO-Group**, möglich, an Regierungen zu verkaufen, die eine erschreckende Menschenrechtsbilanz aufweisen. Untersuchungen haben dokumentiert, dass die **NSO-Software "Pegasus"** in großem Umfang zur Überwachung der Zivilgesellschaft weltweit eingesetzt wird. Nach Berichten von Citizen Lab wurde Technologie der NSO Group bei Überwachungsangriffen in mindestens **45 Ländern** eingesetzt.[65] Betroffen waren unter anderem mindestens 24 Menschenrechtsverteidiger_innen, Journalist_innen und Parlamentarier_innen allein in **Mexiko**[66], die **marokkanischen** Menschenrechtsverteidiger Maati Monjib und Abdessadak El Bouchattaoui[67], die **saudischen** Aktivisten Omar Abdulaziz, Yahya Assiri und Ghanem Al-Masarir[68], der prominente Menschenrechtsaktivist Ahmed Mansoor aus den **VAE**[69] sowie mutmaßlich der getötete **saudische** Dissident Jamal Khashoggi[70]. Über die **Dunkelziffer** lässt sich nur spekulieren, sie dürfte jedoch sehr hoch sein.

Auch ein Mitarbeiter von Amnesty International erhielt 2018 eine WhatsApp-Nachricht mit einem Link, der angeblich Informationen zu einem Protest vor der saudi-arabischen Botschaft in Washington enthielt. Zu diesem Zeitpunkt setzte sich Amnesty intensiv für die Freilassung saudischer Menschenrechtsaktivistinnen ein. Ein Klick auf den Link hätte verdeckt die NSO-Software Pegasus installiert und dem Absender das **Mitlesen von Amnestys interner Kommunikation** und die nahezu vollständige Kontrolle über das betroffene Mobiltelefon ermöglicht.

Israel klassifiziert Überwachungssoftware als militärrelevantes Gut, über die Vergabe von Exportlizenzen entscheidet daher direkt das israelische Verteidigungsministerium. In einem derzeit laufenden und von Amnesty International angestrengten Gerichtsverfahren vor dem Tel Aviv District Court argumentiert Amnesty für einen **Entzug der Exportlizenz der NSO-Group** durch das Ministerium.[71]

Angesichts des weltweiten Missbrauchs von Überwachungstechnologie und dem Mangel an Regularien für Handel und Einsatz fordert der UN-Sonderberichterstatters für das Recht auf Meinungsfreiheit, David Kaye, ein **Moratorium**: „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."[72]

---

65 Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, Ron Deibert, 09/2018, HIDE AND SEEK. Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries,https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

66 John Scott-Railton, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert, 11/2018, Reckless VI, Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague, https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/

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

68 Amnesty International, 05/2019, Amnesty International engages in legal action to stop NSO Group's web of surveillance, https://www.amnesty.org/en/latest/news/2019/05/israel-amnesty-legal-action-stop-nso-group-web-of-surveillance/

69 Bill Marczak, John Scott-Railton, 08/2016, The Million Dollar Dissident- NSO Groups iPhone Zero-Days used against a UAE Human Rights Defender, https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

70 David D. Kirkpatrick, 12/2018, Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html

71 Amnesty International, 05/2019, Affidavit in support of Israeli petition, https://www.amnesty.org/en/documents/act10/0332/2019/en/

72 OHCHR, 05/2019, 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

Auch Amnesty International fordert alle Staaten auf, ein Moratorium für den Export von Überwachungstechnologie zu verhängen, bis ein angemessener regulatorischer Rahmen geschaffen ist.