Chaos Computer Club

# Stellungnahme an den Ausschuss für Menschenrechte und humanitäre Hilfe des Deutschen Bundestags zum Thema Menschenrechte und politische Teilhabe im digitalen Zeitalter

Constanze Kurz,
Jens Kubieziel, Frank Rieger, Rainer Rehak

8. Juni 2020

**Vorbemerkung** ..... **3**
**Digitale Optionen für den Schutz von Menschenrechten** ..... **3**
Das „Darknet“ und der Schutz der Anonymität ..... 3
SecureDrop und anonyme digitale Briefkästen ..... 4
Beispiele der Darknet-Nutzung für Austausch, Recherche und Aufdecken von Missständen ..... 5
Schutz durch Verschlüsselung und Stärkung der IT-Sicherheit ..... 6
**Gesichtserkennung** ..... **9**
**Größte Bedrohungen für die Menschenrechte** ..... **10**
**Export von Überwachungssoftware** ..... **12**
EU-geförderte Forschung und einheitliche Lizenz-Regeln ..... 13
Auswertung digitaler Lebensspuren ..... 13
Beschleunigung der Exportkontroll-Genehmigungsverfahren ..... 14
Reaktion auf Veränderungen der Menschenrechtslage ..... 15
Schutz vor Überwachung fördern ..... 15
**Fazit** ..... **16**

# Vorbemerkung

Diese Stellungnahme widmet sich einigen der Fragen der Abgeordneten, die vor der öffentlichen Anhörung im Rahmen des strukturierten Fragenkatalogs schriftlich an die Sachverständigen gestellt wurden. Schwerpunkte sind die Fragen zum „Darknet“, zum technischen Schutz vor Repression, außerdem zur Gesichtserkennung sowie zur technisierten Überwachung und Kontrolle und zum Export von Überwachungstechnologien.

# Digitale Optionen für den Schutz von Menschenrechten

## Das „Darknet“ und der Schutz der Anonymität

Der Begriff des „Darknet“ ist definitorisch nicht klar umrissen. In der presseöffentlichen Diskussion wird der Begriff meist verwandt, um es als einen Ort für illegale Aktivitäten zu kennzeichnen. Aus seiner Geschichte gesehen bezeichnete der Begriff Orte im Netz, die von Suchmaschinen wie Google, Bing etc. nicht indiziert werden oder für diese unzugänglich waren. In letzter Zeit wird der Begriff allerdings oft synonym für Tor Onion Services verwendet, einer vom Tor-Projekt[1] entwickelten Anonymisierungstechnik für Webangebote. Das Tor-Projekt selbst ist heutzutage primär für den Tor-Browser bekannt.

Für diesen Fragenkatalog soll der Begriff „Darknet“ im Sinne der Tor Onion Services betrachtet werden. Die Software soll Personen eine geschützte, sichere Verbindung ins Web schaffen, die durch technische Verfahren der Anonymisierung die Privatsphäre der Nutzenden bestmöglich schützt. Dadurch kann Whistleblowing, also das Offenlegen von Missständen, nahezu anonym und somit verhältnismäßig gefahrlos betrieben werden. Daneben sollen aber auch diejenigen geschützt werden, die selbst Informationen und Daten im Web bereitstellen.

Diesen zweiten Ansatz verfolgen die Tor Onion Services. Die Domainnamen dieser Dienste enden auf .onion, und es ist nicht ohne weiteres möglich, die IP-Adresse oder den Standort der Server zu erkennen. Die Anzahl der .onion-Adressen wuchs in den letzten Jahren kontinuierlich und wird für Ende des Jahres 2018 mit 112.628 angegeben.[2] Das Tor-Projekt sowie unabhängige Untersuchungen fanden weltweit knapp 200.000 .onion-Domains. Zum

---

[1] Siehe https://www.torproject.org/

[2] Steinebach, Schäfer, Karakuz, Brandl: Detection and Analysis of Tor Onion Services, https://journals.riverpublishers.com/index.php/JCSANDM/article/view/1141/651 vom 23. Januar 2020. Die von der Studie präsentierten Zahlen scheinen belastbar zu sein. Allerdings ist die Durchführung fragwürdig. Um zu den Zahlen zu gelangen, mussten öffentlich benutzbare Tor-Server betrieben und Schwachstellen innerhalb der Tor-Software ausgenutzt werden. Dies stellt ein Risiko für die Nutzerinnen und Nutzer der Software dar. Das Tor-Projekt hat ein Research Board eingerichtet, um die Forschung zu unterstützen, https://research.torproject.org/safetyboard/ Dieses Research Board wurde für die zitierte Studie nicht befragt, das Risiko für die Nutzerinnen und Nutzer bewusst in Kauf genommen.

Vergleich: Die DENIC nennt für Deutschland allein über 16 Millionen .de-Domains.

Gleichzeitig stieg der Datenverkehr: Die Tor Onion Services nutzen derzeit eine Bandbreite von ca. 3,5 GBit/s. Dies entspricht in etwa 140 DSL-Anschlüssen mit einer Bandbreite von 25 MBit/s.[3] Beide Zahlen machen klar, dass diese Technik insgesamt sehr wenig genutzt wird, dennoch gibt es derzeit keine andere Technologie, die geschützte Verbindungen ins Web in diesem Umfang möglich macht.

Die Tor Onion Services werden zu etwa drei Vierteln als Webseiten angeboten. Das restliche Viertel verteilt sich auf Chatdienste, E-Mail und Systemadministration.[4] Eine komplette und abschließende Übersicht ist jedoch technisch bedingt schwer möglich.

Bezüglich der angebotenen Dienste ist zwischen solchen zu unterscheiden, die ein Interesse daran haben, von Nutzern gefunden zu werden, und solchen, die das gern vermeiden wollen. Zu ersterem gehören Angebote, die verschiedene Dinge verkaufen wollen. Dabei wird häufig der Handel mit Betäubungsmitteln als Beispiel genannt, aber auch kommerzielle Foren- oder E-Mail-Anbieter finden sich dort. Diese Online-Angebote haben ein großes Interesse daran, von potentiellen Nutzern gefunden zu werden, und betreiben auch eine diesbezügliche Optimierung des Angebotes.[5]

Auf der anderen Seite sind solche Angebote, die Menschenrechtsverletzungen oder anderes Unrecht bekannt machen wollen und sich beispielsweise für Proteste über das Darknet organisieren bzw. miteinander Informationen austauschen. Die Anbieter haben in ihren Ländern mit Verfolgung zu kämpfen und daher nicht das Interesse und oft nicht das Wissen, ihr Tun entsprechend zu „bewerben“. Dies bedingt häufig ein bewusstes Verstecken der Dienste.

## SecureDrop und anonyme digitale Briefkästen

Verschiedene internationale Medienhäuser nutzen außerdem die Software „SecureDrop“[6], um einen anonymen Briefkasten für Informationen zur Verfügung zu stellen, den beispielsweise Whistleblower und andere Hinweisgeber nutzen können. SecureDrop erstellt eine Webseite mit einer .onion-URL. Darüber können Quellen und Hinweisgeber Dokumente auf sicherem Wege an Medienhäuser weitergeben. Derzeit gibt es weltweit

---

[3] Zum Vergleich: Beim 36. Chaos Communication Congress wurde von den ca. 17.000 Besucherinnen und Besuchern in der Spitze eine Bandbreite von 44,1 GBits/s verbraucht. Dies entspricht also etwa dem Zehnfachen der weltweiten Bandbreite der Tor Onion Services.

[4] Steinebach, Schäfer, Karakuz, Brandl: Detection and Analysis of Tor Onion Services, https://journals.riverpublishers.com/index.php/JCSANDM/article/view/1141/651 vom 23. Januar 2020.

[5] Vgl. Owen, Gareth: Tor – Hidden Services and Deanonymisation, https://media.ccc.de/v/31c3_-_6112_-_en_-_saal_2_-_201412301715_-_tor_hidden_services_and_deanonymisation_-_dr_gareth_owen vom 30. Dezember 2014.

[6] https://securedrop.org/

über vierzig Instanzen[7], darunter sind einige namhafte internationale Medienhäuser, wie Süddeutsche Zeitung, Financial Times, Forbes usw.

Die Plattform „Globaleaks" bietet ebenfalls eine Software, mit der Dokumente über Tor Onion Services versandt werden können. Einige Webseiten nutzen diese Software,[8] nach Angaben der Entwickler von Globaleaks konnten mit Hilfe der Software beispielsweise Menschenrechtsverletzungen in Indonesien oder illegaler Elfenbeinhandel in Ländern Afrikas aufgedeckt werden.

Auch Verbände von Journalistinnen und Journalisten wie etwa der Deutsche-Journalisten-Verband (DJV) machen regelmäßig Schulungen für ihre Mitglieder, um zu vermitteln, wie die Tor-Technologie funktioniert und wie sie für den digitalen Informantenschutz verwendet werden kann. Auch die Menschenrechtsorganisation Amnesty International erfährt regelmäßig von Menschenrechtsaktivisten, dass diese besondere Foren- oder Chatsoftware nutzen, die mittels Tor Onion Services funktionieren, um sich und ihre Arbeit zu schützen.

## Beispiele der Darknet-Nutzung für Austausch, Recherche und Aufdecken von Missständen

Eines der größten Angebote innerhalb der Tor Onion Services ist die Webseite von Facebook unter der URL https://facebookcorewwwi.onion. Dieses Angebot wurde von Facebook explizit ins Leben gerufen, um Menschen, die von einer Zensur des Internets betroffen sind, eine Zugangsmöglichkeit zu schaffen. Der Konzern gibt an, dass der Facebook-Darknet-Zugang monatlich von mehr als einer Million Menschen genutzt wird und damit als Mittel zur Zensurumgehung von weltweit hoher Bedeutung ist.

Verschiedene Medienorganisationen unterhalten ebenfalls Angebote als Tor Onion Service. Die New York Times[9] und die Deutsche Welle[10] etwa seien hier als Beispiele genannt. Der Journalist Barton Gellman, der für die Washington Post schreibt, erläuterte beispielhaft sein technisches Vorgehen zum Schutz von Whistleblowern und beschreibt die Tatsache, dass ihm viele Quellen per SecureDrop Dokumente zuschicken.[11]

Die Umgehung von Zensur und Kontrolle ist auch der Grund, warum etwa die BBC und die Deutsche Welle seit Ende 2019 ihre Angebote ins Darknet stellen. Die Deutsche Welle hat dabei besonders China und den Iran im Visier. Als Erfolg werten die Verantwortlichen im Sender die Resonanz von Nutzern beispielsweise aus dem Iran. Auch Nicht-Regierungs-Organisationen wie Reporter ohne Grenzen nutzen seit Jahren das Tor-Netzwerk, um

---

[7] Vgl. https://securedrop.org/directory/

[8] Vgl. https://www.globaleaks.org/who-uses-it/

[9] Siehe https://www.nytimes3xbfgragh.onion/

[10] Siehe https://www.dwnewsvdyyiamwnp.onion/

[11] Vgl. Gellmann: Since I Met Edward Snowden, I've Never Stopped Watching My Back, https://www.theatlantic.com/magazine/archive/2020/06/edward-snowden-operation-firstfruits/610573/ vom 21. Mai 2020.

Informationen auszutauschen. Im Darknet sind aber auch Greenpeace, Amnesty International oder die Freedom of the Press Foundation zu finden.[12]

## Schutz durch Verschlüsselung und Stärkung der IT-Sicherheit

Sichere technische Verfahren können für Aktivisten, Menschenrechtler, Journalisten oder Oppositionelle Hilfe im digitalen Raum sein, um sich und ihre Quellen zu schützen. Die genannten Gruppierungen oder Einzelpersonen agieren in vielen Staaten unter größtem persönlichen Risiko. Für sie ist es daher wichtig, unbeobachtet mit sicheren Werkzeugen zu kommunizieren und Nachrichten auch veröffentlichen zu können.

Ein grundlegendes Mittel für die sichere Kommunikation ist die Verschlüsselung. Dies sichert auf technischem Wege, dass Fremde keinen Einblick in die kommunizierten Inhalte erlangen können. Im Rahmen der wissenschaftlichen Forschung wurden zahlreiche Algorithmen entwickelt, die diese Forderung erfüllen. Für die von Repression oder Überwachung betroffenen Menschen in Staaten ohne ausreichende menschenrechtliche Standards ist es essenziell wichtig, dass diese Algorithmen weder abgeschwächt noch mit Hintertüren versehen werden.

Eine Abschwächung eines Verschlüsselungsverfahrens hat das Ziel, dass es durch den Einsatz von leistungsfähigen Computern doch möglich ist, die Verschlüsselung zu brechen. Die Idee einer Hintertür hingegen besteht darin, dass staatliche Stellen oder weitere Dritte einen „Zweitschlüssel" besitzen, mit dem der Inhalt der Kommunikation eingesehen werden kann. Der Effekt bei beidem wäre, dass absichtlich eine technische Schwachstelle in das Verschlüsselungsverfahren eingebaut ist.

Zunehmend wird aber nicht mehr nur die Verschlüsselung selbst angegriffen, sondern die informationstechnischen Systeme (Handys, Laptops) zum Ziel. Durch dieses Hacking soll auf die unverschlüsselten Daten vor bzw. nach dem verschlüsselten Versand zugegriffen werden. Dies öffnet jedoch dem Missbrauch Tür und Tor und schwächt die Gesamtsicherheit aller Systeme. Verschiedene Länder zeigen schon jetzt, dass sie ähnliche Techniken gegen die Bevölkerung einsetzen, und es ist zu erwarten, dass dies mit den obigen Techniken genauso passiert.

Neben den Risiken, die eine Abschwächung von Verschlüsselungsverfahren und das Hacking von Telefonen und Computern mit sich bringt, erhöht sich das Entdeckungsrisiko der von Repression bedrohten Gruppen. Daher dürfen sie nicht ein- oder umgesetzt werden, wie es auch die Eckpunkte zur Deutschen Kryptopolitik von 1999 bereits betonen. Ähnlich fatal würde sich eine Pflicht zur Benutzung von Klarnamen oder zur Authentifizierung mittels eines Ausweisdokuments auswirken. Dies schwächt immer die Betroffenen und stärkt die Regime, indem die „Ziele" von Überwachung namentlich benannt werden.

Neben dem Versuch, die Verschlüsselung an sich zu schwächen oder die informationstechnischen Systeme zu hacken, gibt es einen weiteren Ansatz.

---

[12] Vgl. auch https://www.mdr.de/medien360g/medienwissen/darknet-tor-medien-100.html vom 17. Februar 2020.

Dieser wird sowohl in Großbritannien als auch in den Vereinigten Staaten verfolgt. Allerdings versuchen zunehmend auch einige europäische Behörden, diesen Ansatz zu übernehmen. Dabei sollen Internet-Unternehmen überredet oder angeregt werden, ihre Dienstleistungen zwar verschlüsselt zu gestalten. Allerdings sollen die Unternehmen auf staatliche Anforderung die Schlüssel herausgeben oder zusätzliche Schlüssel für das Mitlesen in die Kommunikation einschleusen.

Dieses Vorgehen weist für die Menschenrechte einen gravierenden Schwachpunkt auf: Sobald ein Land, egal unter welchen lokalen rechtlichen Hürden und Voraussetzungen, einen solchen Zugriff auf verschlüsselte Kommunikation etabliert hat, werden auch andere Länder diesen Zugang von den Internet-Unternehmen einfordern. Da die Rechtssysteme in Diktaturen und Ländern mit schwachen Menschenrechtsstandards grundsätzlich als nicht vertrauenswürdig anzusehen sind, obwohl sie formal das gleiche Ergebnis liefern (beispielsweise eine richterliche Anordnung), stehen die Internet-Unternehmen vor unlösbaren Dilemmata: Wenn sie nicht riskieren wollen, in den betreffenden Staaten ausgesperrt zu werden, können sie schlechterdings das örtliche Rechtssystem offen in Frage stellen.

In der Praxis sind die Kommunikationsprodukte westlicher Internet-Unternehmen wie Google für Menschenrechtsaktivisten in repressiven Staaten oftmals das einzige halbwegs vertrauenswürdige Arbeitsmittel, weil sie mit starker, hintertürfreier Verschlüsselung gebaut werden. Sollten Gesetzgeber im Westen diese Unternehmen zwingen, Hintertüren für die Strafverfolgung oder gar für Geheimdienste – etwa durch Mechanismen für das Hinzufügen von zusätzlichen Schlüsseln – in ihre Produkte einzubauen, würde der Zugang zu diesen Mechanismen ohne jeden Zweifel auch von den Behörden menschenrechtsverletzender Länder eingefordert werden.

Im Rahmen der Snowden-Veröffentlichungen sind verschiedene Versuche westlicher Geheimdienste bekannt geworden, den Einbau von Hintertüren von kommerziellen Unternehmen systematisch zu fordern oder selbst vorzunehmen. Erst die Veröffentlichung und die breite Debatte danach konnte die Praxis zurückdrängen. Derzeit können sich die meisten westlichen Internet-Unternehmen noch auf den technisch korrekten Standpunkt stellen, dass sie keine technische Möglichkeit haben, an die geforderten Kommunikationsinhalte zu gelangen, und entsprechende Begehrlichkeiten abweisen. Wäre aber einmal der Damm gebrochen, gäbe es kein Halten mehr.

Diese Erfahrung hat beispielsweise das Unternehmen Blackberry gemacht, das zeitweise Marktführer im Bereich mobiles Messaging war. Blackberry hatte jedoch seine Verschlüsselung so gestaltet, dass auf Anforderung eine Entschlüsselung möglich war. Selbstverständlich bekam das Unternehmen, sobald westliche Strafverfolger und Geheimdienste davon Gebrauch gemacht hatten, auch entsprechende Anforderungen aus Saudi Arabien und ähnlichen Ländern, verbunden mit der Drohung des Verbots und harter Strafen gegen Mitarbeiter im Weigerungsfall. Blackberry gab letztlich den Forderungen nach. Die Firma spielt heute im Mobiltelefonmarkt keine Rolle mehr und ist damit ein warnendes Beispiel für heutige Internet-Unternehmen.

Ein weiterer Risikofaktor beim absichtlichen Einbau von Mechanismen für die Entschlüsselung durch die Betreiber-Unternehmen ist die verdeckte Verwendung dieser Systeme durch Geheimdienste, die durch Cyber-Angriffe Kontrolle über die entsprechenden Zugriffsberechtigungen erlangen können. Der griechische Vodafone-Fall[13] zeigt deutlich, dass einmal installierte Abhörsysteme ein vorrangiges Ziel von geheimdienstlichen Cyber-Angriffen sind, weil sie hier einen einfachen, gezielten Zugriff auf Kommunikation ihrer Ziele – wie zum Beispiel Journalisten und Menschenrechtsaktivisten – bekommen.

Ein besserer Schutz kann in der Stärkung der IT-Sicherheit bestehen. Dies kann auf verschiedenen Wegen geschehen, vor allem:

> Stärkung der wissenschaftlichen Forschung auf dem Gebiet der IT-Sicherheit,
>
> Förderung spezieller Maßnahmen (Auditierung, Penetrationstests),
>
> Training von betreffenden Personengruppen in sicherer Benutzung von IT-Systemen und in IT-Sicherheitsmaßnahmen.

Eine Stärkung der Forschungsvorhaben zur sicheren Programmierung und zu IT-Schutzmaßnahmen etc. schafft die theoretischen Grundlagen. Dies hilft langfristig, die IT-Sicherheit zu verbessern.

Mit der Förderung spezieller Maßnahmen wie Audits wird ein Beitrag zur Verbesserung der IT-Sicherheit einzelner Softwarepakete geleistet. Hiermit ist es möglich, Anstrengungen genau auf solche Software zu konzentrieren, die von den betroffenen Personengruppen bevorzugt benutzt wird. Durch Auditierung von Code und Konfiguration, Penetrationstests und weitere Maßnahmen kann der Sicherheitsstand der Software beurteilt werden. Aufgefundene Fehler und Schwachstellen bieten die Grundlage dafür, Verbesserungen zu entwickeln.

Schulungen der Nutzerinnen und Nutzer helfen ganz konkret, sowohl beim Vermeiden von Nutzungsfehlern als auch bei der besseren Anpassung an die Bedürfnisse und Erfordernisse. Viele Probleme entstehen bei der (falschen) Benutzung von IT-Systemen. Hier kann eine Schulung helfen, typische Risiken zu erkennen und Software fehlerfrei zu benutzen.

---

[13] Vgl. „Griechenlands Premier wurde abgehört“, SPIEGEL Online, https://www.spiegel.de/netzwelt/web/spionageskandal-griechenlands-premier-wurde-abgehoert-a-398835.html vom 3. Februar 2006.

## Gesichtserkennung

Die wichtigsten Abnehmer von Gesichtserkennungssystemen, aber auch von Iris- oder Fingerabdruckscannern sind nach wie vor staatliche Institutionen, gefolgt von Flughäfen. In die Anschaffung und den Unterhalt biometrischer Kontrollsysteme wird in diesen beiden Bereichen weltweit Jahr für Jahr mehr Geld gesteckt. Das Speichern der Körperdaten erfolgt in der Regel bei staatlichen Stellen. Auch in Deutschland erfassen und speichern Einwohnermeldeämter und Ausländerbehörden heute standardmäßig biometrische Daten, die bei der Beantragung von Personalausweisen, Pässen oder anderen hoheitlichen Ausweisdokumenten verpflichtend abzugeben sind.

Weniger die Eingriffe in Menschenrechte als die praktische Funktionsfähigkeit der biometrischen Gesichtserkennungssysteme stehen oft im Mittelpunkt der Diskussionen, wenn in den letzten Jahren Pilotversuche zur automatisierten Erkennung in der Öffentlichkeit durchgeführt und diskutiert wurden. Dadurch, dass solche Versuchsreihen zur Gesichtserkennung in der Praxis nach wie vor viele falsch-positive Treffer melden, tritt in den Hintergrund, dass die Technologien zwar fehlerbehaftet sind, jedoch im letzten Jahrzehnt erhebliche Fortschritte gezeigt haben und damit für Passanten zur Bedrohung werden. Denn gerade das Gesicht wird typischerweise exponiert, so dass ein optisches Scannen und Auswerten der biometrischen Aufnahmen unbemerkt vorgenommen werden kann. Die Fehler, die in vielen biometrischen Softwareprodukten zu fälschlichen Treffern führen, sind oft diskriminierend für bestimmte Personengruppen und weisen inhärente Verzerrungen auf.[14] Solche Fehler können in der Praxis fälschliche Fahndungsaufrufe und schwerwiegende falsche Anschuldigungen nach sich ziehen.[15]

Gesichtsdatenbanken und biometrische Gesichtserkennungsverfahren wurden in den letzten Jahren dennoch weltweit zum Standardinstrument von Geheimdiensten und Strafverfolgern.[16] Hinzu tritt die Entwicklung, dass biometrische Kontrolle nicht mehr nur punktuell, sondern großflächig zum Einsatz kommt oder geplant wird.[17] Gesichtserkennungssysteme werden neben der Identifizierung von Personen künftig auch stärker zur Analyse des Verhaltens von Menschen genutzt. Eine automatische Auswertung nimmt

---

[14] Vgl. Face Recognition Vendor Test des NIST, https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt mit zweihundert getesteten Gesichtserkennungssystemen.

[15] Jeremy Fox: Brown university student mistakenly identified as Sri Lanka bombings suspect, Boston Globe, https://www2.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lanka-bombings-suspect/0hP2YwyYi4qrCEdxKZCpZM/story.html vom 28. April 2019.

[16] Auch in Deutschland, siehe Stefan Krempl: BKA und LKAs weiten Einsatz von Gesichtserkennung deutlich aus, https://www.heise.de/newsticker/meldung/Ueberwachung-BKA-und-Interpol-weiten-Einsatz-von-Gesichtserkennung-deutlich-aus-4712956.html vom 30. April 2020.

[17] Auch in Deutschland erklärte der damalige Bundesinnenminister Thomas de Maizière erstmals 2017 im Rahmen eines Tests von drei Gesichtserkennungssystemen am Berliner Bahnhof Südkreuz seine Idee einer flächendeckenden Gesichtserkennung.

dann nicht nur Bezug auf Körper-Merkmale, sondern auch auf Bewegungen und Verhalten: Beispielsweise Gang, Mimik, Stimme oder Gestik können von Software analysiert werden, um eine Sprach- oder Emotionserkennung durchzuführen.

Die aktuelle Pandemie hat sich für Gesichtserkennungssysteme zudem als Katalysator erwiesen, die ohne viel Diskussion zum Einsatz gebracht wurden. Ein Beispiel ist das von der Pandemie besonders betroffene Russland, wo in der Millionenstadt Moskau automatisierte Gesichtserkennung besonders gegen Menschen bestimmter Ethnien eingesetzt wird.[18]

Gesichtserkennung als Kontrollmaßnahme bedroht die Menschenrechte und diskriminiert Personengruppen vor allem dann, wenn sie automatisiert durchgeführt wird. Sie gehört schon heute zu den größten Bedrohungen für die Menschenrechte und die politische Beteiligung. Daher ist ein Verbot automatischer Gesichtserkennung in der Öffentlichkeit zu fordern, dabei insbesondere der Einsatz durch staatliche Akteure.

## Größte Bedrohungen für die Menschenrechte

Durch die Digitalisierung fast aller Lebensbereiche in den letzten fünfzehn Jahren sind bestimmte Menschenrechte besonderen Bedrohungen ausgesetzt, die erst durch das Vorhandensein von Technologien entstanden sind. Dazu gehören das Menschenrecht auf Privatheit von Kommunikation und allgemein die Persönlichkeitsrechte sowie die Menschenwürde. Die Tatsache, dass die gesamte Kommunikation über informationstechnische Geräte nun digital vollzogen wird, eröffnet Überwachern neue Möglichkeiten, die zuvor schlichtweg nicht bestanden. Tausende oder auch Millionen Menschen mit technischen Hilfsmittel gleichzeitig zu überwachen, zu rastern und die gewonnenen Daten auszuwerten, war in vordigitaler Zeit undenkbar, ist heute jedoch nicht nur möglich, sondern wird auch vollzogen.

Zu den größten Menschenrechtsbedrohungen zählen Datensammlungen und -auswertungen, die aufgehäuft werden, ohne dass ein bestimmter Grund vorliegt. Insbesondere bei der Telekommunikation ist es in etlichen Ländern Standard geworden, Daten auf Vorrat zu speichern. Bei dieser anlasslosen Massenüberwachung der Telekommunikation werden ohne konkreten Verdacht Verkehrs- und Inhaltsdaten ausgeleitet und ausgewertet.

Insbesondere Geheimdienste, aber auch Polizeien in nicht-demokratischen Staaten machen davon Gebrauch. Mit automatisierten oder manuellen Methoden ist das Aufdecken von Kontaktnetzwerken aus den Daten möglich, wodurch etwa ganze Dissidentengruppen und sonstige staatskritische Stimmen entdeckt und dann verfolgt werden können. Diese Gruppen können entweder über Verkehrsdatenanalysen aufgedeckt werden, wenn keine

---

[18] Ein Quarantänegebot für 2.500 Menschen, die aus China einreisten, soll nach Angaben des Moskauer Bürgermeisters Sergei Sobjanin mittels biometrischer Erkennung durchgesetzt werden. Verlassen die Betroffenen ihre Wohnungen, sollen Kameras im Stadtgebiet deren Gesichter erkennen und sie automatisch melden, siehe Gabrielle Tétrault-Farber: Moscow deploys facial recognition technology for coronavirus quarantine, https://www.reuters.com/article/us-china-health-moscow-technology-idUSKBN20F1RZ vom 21. Februar 2020.

Schutzmaßnahmen wie Darknet-Kommunikationswege oder andere Maßnahmen der Anonymisierung zur Verfügung stehen, oder aber beim Ausspähen der genutzten Kommunikationsgeräte durch staatliches Hacking.

Seit dem Jahr 2013, als Edward Snowden in Zusammenarbeit mit internationalen Medien eine überfällige Debatte über die anlasslose Massenüberwachung lostrat, ist das Wissen um die tatsächlichen technischen Fähigkeiten westlicher Geheimdienste erheblich gestiegen. Das Ausmaß der Massenüberwachung war zuvor öffentlich nicht bekannt. Ob diese anlasslose Überwachung und Rasterung von Daten in Europa mit der Menschenwürde, dem Menschenrecht auf Privatheit von Kommunikation und den Persönlichkeitsrechten vereinbar ist, war und ist Gegenstand von gerichtlichen Verfahren in Europa und weltweit. An Artikel 7 (Achtung des Privat- und Familienlebens) und Artikel 8 (Schutz personenbezogener Daten) der Charta der Grundrechte der Europäischen Union muss sich die Massenüberwachung ebenso messen lassen wie an der Europäischen Menschenrechtskonvention, hier insbesondere an Artikel 8.[19]

Für die Geheimdienste anderer Staaten als den sog. „Five Eyes" (USA, Großbritannien, Australien, Neuseeland, Kanada) ist die Informationslage über massenhafte Datensammlungen in der Regel deutlich schlechter, vor allem in Diktaturen sind jenseits von Medienberichten typischerweise wenig oder keine Informationen über das technische Gebaren der Geheimdienste verfügbar.

Neben der anlasslosen Massenüberwachung muss auch das Vordringen gezielter Überwachung in immer intimere Bereich von Menschen als erhebliche und wachsende Bedrohung der Menschenrechte betrachtet werden. Die Menschenwürde gebietet es, jedem Menschen seinen unantastbaren Kern seines privaten Lebens einzuräumen. Diese Intimsphäre, die einen weit persönlicheren Bereich als die Privatsphäre beschreibt, ist aber mittlerweile der digitalen Überwachung eröffnet, schon weil wir informationstechnische Geräte mitten in unsere Leben gepflanzt haben.

Neben der oben erwähnten Gesichtserkennung und weiteren automatisierten Biometriesystemen ist die Körperdaten-Rasterung und -Auswertung als ein erhebliches Menschenrechtsproblem zu konstatieren. Einer automatisierten Diskriminierung oder Repression anhand von Körpermerkmalen, die auch verdeckt stattfinden kann, steht technisch kaum mehr etwas im Wege.

Weitere erhebliche Menschenrechtsbedrohungen gehen von technischen Entwicklungen aus, die hier nur kurz umrissen werden können:

- der „Cyberwar" staatlicher und militärischer Stellen, der Völkerrecht und Menschenrechte missachtet und weitgehend unter dem Radar der Öffentlichkeit abläuft und der zugleich die strukturelle IT-Sicherheitskrise ausnutzt und diese auch aktiv weiter befeuert;

---

[19] Ob die Massenüberwachung Großbritanniens, die durch Snowden an die Öffentlichkeit kam, gegen die Europäische Menschenrechtskonvention verstößt, wird nach zwei mündlichen Anhörungen noch in diesem Jahr der Europäische Menschenrechtsgerichtshof entscheiden, siehe http://hudoc.echr.coe.int/eng?i=001-186048, App. No. 58170/13.

- die Nutzung von Wahlcomputern und eVoting-Verfahren, die eine erhebliche Manipulationsgefahr aufweisen und ein Anlass für Vertrauenskrisen in politische Beteiligung sein können;

- Internetzensur sowie Internetblockaden bis hin zu -abschaltungen;

- verdeckte Manipulationen im Rahmen von weitgreifenden Desinformationskampagnen, die gesellschaftliches Vertrauen in politische Beteiligung gezielt zerrütten können.

## Export von Überwachungssoftware

Mit seinem Urteil zum BND-Gesetz[20] hat das Bundesverfassungsgericht die grundsätzliche Geltung der Abwehrrechte des Grundgesetzes gegenüber einer Telekommunikationsüberwachung auch für Ausländer im Ausland etabliert. Neben dem konkret betroffenen BND-Gesetz hat das Urteil auch Auswirkungen auf angrenzende Bereiche: Mit dem fortgesetzten Export von Überwachungstechnologien an nicht-demokratische Länder leisten Deutschland und weitere Staaten in Europa derzeit unmittelbare Hilfe bei der Überwachung von Menschen in Diktaturen und Staaten, die weit entfernt von menschenrechtlichen Standards sind. Mit dem Urteil wird deutlich, dass die derzeitige Tendenz zur höheren Gewichtung von wirtschaftlichen und außenpolitischen Interessen auch bei der Bewertung des Exports von Überwachungstechnologien so nicht weiter fortgeführt werden kann und ein Primat der Menschenrechte hergestellt werden muss. Im Rahmen des laufenden Trilog-Verfahrens zur Dual-Use-Verordnung auf EU-Ebene[21] bietet sich derzeit die Gelegenheit, dies umzusetzen. Das Europäische Parlament hat die Europäische Kommission im Rahmen des Trilogs bereits aufgefordert, Menschenrechte bei den Exportkontrollen von Überwachungssystemen stärker zu berücksichtigen.

Die Praxis der Exportkontrolle stellt eine problematische Vermischung von Interessen und Werten dar: Mit den gleichen Instrumenten und Mechanismen wird versucht, außen- und sicherheitspolitische Interessen, Terrorabwehr und Menschenrechtsschutz parallel zu realisieren. In der Abwägung werden die Menschenrechte als bestenfalls gleichwertiges Ziel gegenüber den anderen Zielen angesehen, nicht aber als übergeordnete Basis und als Wertesystem allen Handelns. Die für die Exportkontrolle relevante Einordnung von Staaten und Organisationen als Menschenrechtsverletzer findet oft genug erst nach öffentlicher Berichterstattung und mit einiger Verzögerung statt und ist häufig von geopolitischer Opportunität geleitet. Hier gilt es einerseits eine Beschleunigung der politischen und bürokratischen Prozesse zu erreichen, mit denen das Bild zur Menschenrechtslage und Überwachungssituation in potentiellen Exportstaaten fortlaufend aktualisiert wird und zeitnah zu einer entsprechenden Klassifizierung führt. Andererseits ist die Verankerung des

---

[20] 1 BvR 2835/17, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/05/rs20200519_1bvr283517.html vom 19. Mai 2020.

[21] Vgl. https://www.europarl.europa.eu/legislative-train/theme-europe-as-a-stronger-global-actor/file-review-of-dual-use-export-controls seit September 2016.

Menschenrechts auf Privatheit der Kommunikation und der Nutzung von informationstechnischen Systemen als separates Schutzziel in den entsprechenden Gesetzen und Verordnungen notwendig. Andernfalls ist nicht zu erwarten, dass sie adäquat umgesetzt werden.

## EU-geförderte Forschung und einheitliche Lizenz-Regeln

Im Rahmen staatlich geförderter Forschungsvorhaben wird regelmäßig Dual-Use-Technologie entwickelt, die für Überwachungssysteme nutzbar ist und dort auch praktisch verwendet werden.[22] Spracherkennung, Bildverarbeitung, Objekterkennung, Machine Learning, Biometrie, Data Fusion, aber auch klassische IT-Sicherheitsforschung generieren oft Erkenntnisse, Algorithmen, Methoden und Software, die in Überwachungssystemen missbraucht werden können. Im Rahmen eines grundlegenden Primats der Menschenrechte sollte die Verwendung der im Rahmen von EU-geförderten Projekten erzeugten Ergebnissen und Software durch die Festlegung einer Verwendungslizenz reguliert werden, die ihre Benutzung in Überwachungssystemen ausschließt. Dass mit Steuergeldern finanzierte Forschung und Entwicklung in Systeme fließt, die für eklatante Menschenrechtsverletzungen verwendet werden, sollte nicht weiter hingenommen werden.

Dazu ist kein Aufbau von aufwendigen Infrastrukturen oder umfangreichen Berichtssystemen nötig, die die Forschung weiter bürokratisieren würden. Erforderlich ist lediglich eine einheitliche Verwendungslizenz für mit deutschen und europäischen Mitteln geförderte Projektergebnisse, analog zur Zivilklausel vieler deutscher Universitäten und Hochschulen. Eine legale Verwendung der Ergebnisse in Produkten und Systemen, die für Überwachungszwecke konzipiert, gebaut und verkauft werden, wäre damit grundsätzlich ausgeschlossen.

## Auswertung digitaler Lebensspuren

Überwachungstechnologie umfasst inzwischen nicht nur spezialisierte Systeme zur Telekommunikationsüberwachung. Es wäre kurzsichtig, sich bei der Betrachtung des Problems nur auf Cyber-Angriffsmittel, Trojaner und Telekommunikationsüberwachungssysteme zu konzentrieren. Vielmehr geht der technische Trend in repressiven Staaten und Diktaturen zu integrierten Überwachungskomplexen, die Daten aus allen Systemen, in denen digitale Lebensspuren anfallen, miteinander verknüpfen. Menschen werden anhand ihres digitalen Schattens verfolgt, über Daten etwa aus Bezahlvorgängen, digitalen ÖPNV-Tickets, Mobiltelefon-Daten, Überwachungskameras mit automatischer Gesichtserkennung und Personenverfolgung und durch Abgrasen von Social-Media-Datenströmen. Alle diese und weitere Datenquellen werden integriert und mit konventioneller Data-Fusion-Software, aber auch Machine Learning analysiert.

Die Profileration solcher Systeme muss zusätzlich zu den bisher betrachteten Einzeltechnologien in den Fokus gebracht werden. Dabei sollte die

---

[22] Vgl. Christian Bergmann: EU finanziert Überwachungstechnik für den BND, https://www.zeit.de/digital/datenschutz/2017-02/bnd-ueberwachung-sprache-eu/komplettansicht vom 22. Februar 2017.

Regulierung vom Zweck der Verwendung her erfolgen und nicht versucht werden, der sich schnell entwickelnden Technologie hinterherzuhecheln. Systeme, die dafür gebaut und geeignet sind, Überwachung mit ansonsten „alltäglichen“ Datenquellen zu realisieren, sollten vom Export ausgeschlossen werden.

Bei aktiven Cyber-Angriffsmitteln müssen nicht nur die Angriffswerkzeuge selbst – wie Trojaner und automatisierte Exploit-Werkzeuge – erfasst werden, sofern sie nicht für Forschungszwecke, sondern für den Einsatz als Überwachungs- und Repressionsmittel konzipiert, gebaut und beworben werden. Die Definitionen müssen sich auch auf die Kommando- und Kontroll-Systeme erstrecken, mit denen Cyber-Angriffskampagnen zum gezielten und neuerdings auch massenweisen Angriff auf digitale Geräte und Netze koordiniert werden.

Um die Compliance der IT-Sicherheits-Community mit Exportregeln zu gewährleisten, ist es dringend nötig, dass sich die Exportkontrollen auf die Überwachungsprodukte konzentrieren und nicht die Forschung zum Auffinden und Beheben von Sicherheitslücken beeinträchtigt wird. Derzeit sind europäische Staaten direkt oder über Mittelsmänner aktiv am Ankauf von Sicherheitslücken (Exploit-Handel) beteiligt. Dadurch wird ein grauer Markt mit immer weiter steigenden Preisen etabliert, der dann auch von undemokratischen Staaten und Akteuren gern genutzt wird. Eine mögliche Lösung des Problems wäre die steuerliche oder direkte Förderung von Bug-Bounty-Programmen gerade für kleinere Software-Hersteller. Sie würden dadurch in die Lage versetzt, von Forschern gefundene Sicherheitslücken direkt anzukaufen und zu beheben, um sie so dem Graumarkt zu entziehen.

Die im derzeitigen Trilog auf EU-Ebene zur Dual-Use-Verordnung bereits absehbare Tendenz läuft Gefahr, ein bürokratisches Ungetüm zu generieren, das in der Praxis in den Unternehmen nur schwer und nur zu hohen Kosten umsetzbar ist. Da viele Technologie-Entwicklungszweige Dual-Use-Charakter in Bezug auf Überwachungssysteme haben, wäre eine Ausweitung der Exportkontrolle auf mehr Branchen sinnvoll und notwendig. Mit dem derzeitigen Verfahren ist dies jedoch mit erheblichen, aber unnötigen Belastungen für die Unternehmen verbunden und trifft daher auf massiven Widerstand seitens der Industrie- und Wirtschaftsverbände. Nötig ist daher eine drastische Vereinfachung und Erleichterung der Prüfmethoden, mit denen Unternehmen feststellen können, ob ein potentieller Kunde als Exportziel aufgrund der Menschenrechtssituation nicht in Frage kommt. Die dafür nötigen Informationen und Software müssen zeitnah, kostenlos und in freier Software implementiert zur Verfügung stehen und nicht wie derzeit als teures Subskriptions-Modell abgebildet werden.

### Beschleunigung der Exportkontroll-Genehmigungsverfahren

Die Praxis der derzeitigen Exportkontroll-Genehmigungsverfahren ist selbst für gutwillige Unternehmen, die Dual-Use-Technologien produzieren, kaum akzeptabel. Die wesentlichen Probleme dabei sind die Unvorhersagbarkeit und Länge der Bearbeitungszeit und die Unschärfe der dabei angewandten Kriterien. Wenn Exportkontrollanträge, wie es derzeit typisch ist, eine Bearbeitungszeit von mehr als sechs Monaten benötigen, entstehen starke

Anreize, Umgehungswege zu finden und zu etablieren. Damit werden Unternehmen aus Gründen der Marktfähigkeit motiviert, sich dem deutschen Exportkontroll-Regime zu entziehen. Wenn die Umgehungswege aus rein praktischen Erwägungen der schnellen Lieferfähigkeit einmal etabliert sind, drohen sie auch für Exporte in Länder mit Menschenrechtsverstößen benutzt zu werden. Andere EU-Länder schaffen es in deutlich kürzerer Zeit, die entsprechenden Anträge zu bearbeiten. Eine effiziente, schnelle Bearbeitung von Exportkontrollanträgen ist nötig, um die bessere Akzeptanz des Exportkontrollregimes und damit seine Wirksamkeit zu gewährleisten.

### Reaktion auf Veränderungen der Menschenrechtslage

In der Praxis werden komplexe Überwachungssysteme nicht einfach nur ausgeliefert und funktionieren dann für eine lange Zeit ohne weitere Wartung. Typischerweise gibt es durch die Anbieter oder deren Dienstleister regelmäßige Software-Updates, Hilfe bei Konfigurationsänderungen, Schulungen und ähnliche Angebote, lange nachdem das System installiert wurde.

In den letzten Jahren gab es mehrere Fälle von erheblicher Verschlechterung der Menschenrechtslage in verschiedenen Staaten. Es steht auch in Zukunft zu erwarten, dass sich ehemals „Verbündete“, an die bisher problemlos Überwachungstechnik geliefert werden konnte, zu undemokratischen Menschenrechtsverletzern entwickeln. Deutsche und europäische Hersteller sollten daher bei einer solchen Veränderung aktiv durch die zuständigen Behörden benachrichtigt werden und gezwungen sein, dann solche Update- und Support-Aktivitäten einzustellen. Dabei muss besonderes Augenmerk darauf gelegt werden, dass insbesondere spezialisierte Hersteller von Überwachungstechnologie Service-Abteilungen im nicht-europäischen Ausland geschaffen haben und über Lizenz-Abkommen über Drittstaaten arbeiten. Auch für solche Abteilungen muss ein Verbot der technischen Unterstützung dann gelten.

### Schutz vor Überwachung fördern

Der Widerstand aus der Industrie gegen eine effektive Verhinderung des Exports von deutscher und europäischer Überwachungstechnologie ist auch eine Folge der Fehlsteuerung von Fördermitteln im Bereich der Forschung zur IT-Sicherheit. Ausgehend von den postulierten Bedarfen der für die öffentliche Sicherheit zuständigen Behörden wurden in den letzten Jahren immer mehr Forschungs- und Entwicklungsprojekte finanziert, die im Kern Basistechnologien für Überwachungssysteme sind.

Stattdessen sollten die deutschen und europäischen Förder-Prioritäten so umgestellt werden, dass Technologien zum Schutz vor Überwachung schwerpunktmäßig gefördert werden. Die ubiquitäre Digitalisierung macht die Entwicklung solcher Schutz-Technologien zu einem zwingenden Erfordernis für den Erhalt der Demokratie in Europa. Deutschland und Europa haben international im Bereich Privacy-Technologien eine gute Ausgangsposition, die durch umfangreiche, gezielte Förderung zu einer weltweit marktdominierenden Position ausgebaut werden könnte, die Arbeitsplätze und Exporte in ethisch vertretbaren Bereichen schafft.

## Fazit

Der Schutz von Menschenrechten weltweit wird immer stärker zu einer Frage der Technologiepolitik. Personen, die von Menschenrechtsverletzungen betroffen sind oder darüber berichten, sind auf technische Mittel zur Sicherung ihrer Arbeit zwingend angewiesen. Alle Bestrebungen in den demokratischen Staaten, technische Mittel zur Anonymisierung und Verschlüsselung von Kommunikation und Information für die Zwecke von Strafverfolgung und Geheimdiensten einzuschränken oder zu durchlöchern, führen unmittelbar zu einer drastischen Verschlechterung der Situation für diese Personen in ihren Ländern. Die Rolle Deutschlands und der EU bei der Ausrüstung von unterdrückerischen Regimen mit Überwachungssystemen und Dual-Use-Technologien für Menschenrechtsverletzungen bedarf einer grundlegenden Neubewertung und einer Reform des Exportkontroll-Regimes.