19. Wahlperiode

Deutscher Bundestag
Ausschuss für Menschenrechte und humanitäre Hilfe

Wortprotokoll
der 57. Sitzung

Ausschuss für Menschenrechte und humanitäre Hilfe
Berlin, den 17. Juni 2020, 14:00 Uhr
10557 Berlin, Konrad-Adenauer-Str. 1
Paul-Löbe-Haus, Saal PLH E 800
und als Videokonferenz unter Nutzung
des Systems Cisco-WebEx

Vorsitz: Gyde Jensen, MdB

Tagesordnung - Öffentliche Anhörung

Tagesordnungspunkt 1 **Seite 6**

Öffentliche Anhörung zum Thema:

Menschenrechte und politische Teilhabe im digitalen Zeitalter

Geladene Sachverständige

Nighat Dad
Executive-Director der Digital-Rights-Foundation in Pakistan

PD Dr. Matthias C. Kettemann
Leibniz-Institut für Medienforschung, Hans-Bredow-Institut

Dr. Constanze Kurz
Chaos Computer Club

Zara Rahman
stellvertretende Direktorin bei The Engine Room

Lena Rohrbach
Referentin für Digitalisierung, Wirtschaft und Rüstungsexportkontrolle, Amnesty International

Dr. Kristin Shi-Kupfer
Mercator Institute for China Studies

Joachim Nikolaus Steinhöfel
Rechtsanwalt

Strukturierter Fragenkatalog zur öffentlichen Anhörung des Ausschusses für Menschenrechte und humanitäre Hilfe zum Thema „Menschenrechte und politische Teilhabe im digitalen Zeitalter“

A. Bedrohung von Menschenrechten durch den Einsatz digitaler Kontroll- und Überwachungssysteme

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)

2. Die kommunistische Führung Chinas versucht in enger Koordination von staatlichen und Partei-Strukturen sowie privaten und dennoch vom Staat abhängigen Unternehmen eine Totalüberwachung und Kontrolle der gesamten Bevölkerung in allen öffentlichen und privaten Bereichen durchzusetzen, insbesondere von ethnischen und religiösen Minderheiten. Welche Strategie nutzt die kommunistische Führung unter Xi Jinping nicht nur national, sondern auch regional und immer stärker global, um die neue Rolle Chinas als ökonomische und digitale Supermacht auch dafür einzusetzen, die universellen Menschenrechte im Sinne der autoritären Ideologie der KP Chinas umzudefinieren? (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.)

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)

B. Digitale Optionen und Strategien für den Schutz von Menschenrechten

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)

6. In welchen Bereichen identifizieren Sie die größten Chancen und Herausforderungen digitaler Technologien in Bezug auf Gendergerechtigkeit, Frauenrechte und politische Teilhabe von Frauen? (FDP)

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.)

C. Soziale Medien und Meinungsfreiheit

9. Welche Bedeutung haben die Begriffe Hass und Hetze im Internet angesichts der mit ihnen erstrittenen Gerichtsurteile, also taugen sie als prozessverwertbare Vorwürfe? (AfD)

10. Manipulieren Plattformen wie Google, Facebook und Twitter in Deutschland das politische Klima ebenso, wie es Whistleblower in den USA („unconscious bias“, wie beschrieben von Dr. Robert Epstein) aufdecken konnten? (AfD)

D. Regulierung des internationalen Handels mit digitalen Technologien

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)

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)

Mitglieder des Ausschusses

	Ordentliche Mitglieder	**Stellvertretende Mitglieder**
CDU/CSU	Altenkamp, Norbert Maria Brand (Fulda), Michael Brehm, Sebastian Heinrich (Chemnitz), Frank Patzelt, Martin Zimmer, Prof. Dr. Matthias	Brodesser, Dr. Carsten Damerow, Astrid Kuffer, Michael Leikert, Dr. Katja Motschmann, Elisabeth Schipanski, Tankred
SPD	Ortleb, Josephine Özoğuz, Aydan Schwabe, Frank	Castellucci, Dr. Lars Diaby, Dr. Karamba Heinrich, Gabriela
AfD	Braun, Jürgen Herdt, Waldemar	Friesen, Dr. Anton Frohnmaier, Markus
FDP	Heidt, Peter Jensen, Gyde	Köhler, Dr. Lukas Lambsdorff, Alexander Graf
DIE LINKE.	Brandt, Michel Nastic, Zaklin	Buchholz, Christine Jelpke, Ulla
BÜNDNIS 90/DIE GRÜNEN	Bause, Margarete Gehring, Kai	Amtsberg, Luise Polat, Filiz

Tagesordnungspunkt 1

Öffentliche Anhörung zum Thema:

Menschenrechte und politische Teilhabe im digitalen Zeitalter

Die **Vorsitzende Gyde Jensen** (MdB): Liebe Kolleginnen, liebe Kollegen, ich möchte Sie alle ganz herzlich zu unserer etwas anderen öffentlichen Anhörung begrüßen. Die Corona-Pandemie und die Zeitumstände haben uns nicht davon abgehalten, eine öffentliche Anhörung in einer etwas anderen Form durchzuführen. Sie werden sicherlich alle schon bemerkt haben oder spätestens jetzt sehen können, dass wir zum Teil in Präsenz und zum Teil mit unserem Format WebEx tagen. Wir haben zwei der Sachverständigen, die ich gleich noch namentlich begrüßen werde, hier im Ausschusssaal. Die übrigen Sachverständigen sind uns über WebEx zugeschaltet. Sie sind auch alle erreichbar, das ist die Hauptsache, denn mit Ihnen wollen wir heute ins Gespräch kommen. Ich möchte Ihnen vorab noch ein paar organisatorische Dinge mitteilen, denn wir befinden uns in einer öffentlichen Anhörung, und da sind die Gegebenheiten etwas anders. Wir versuchen, die entsprechenden Abstände einzuhalten, deswegen sitzen nur einige der Kolleginnen und Kollegen hier im Raum. Nun ein Hinweis an all diejenigen, die über WebEx zugeschaltet sind: Ich möchte Sie bitten, immer dann, wenn Sie nicht selbst sprechen, Ihre Mikrofone stumm zu schalten. Ihre Kamera können Sie gern anlassen, wenn Sie möchten, aber das ist natürlich kein Muss. Wenn Sie dann das Wort erteilt bekommen, müssten Sie Ihr Mikrofon einschalten, andernfalls kommt es hier im Raum zu einer Rückkopplung. Die Kolleginnen und Kollegen im Ausschuss wissen, wie es funktioniert. Sie können ganz normal die Mikrofone benutzen, wie wir das aus den Präsenzsitzungen kennen. Wer zusätzlich über ein Tablet die WebEx-Konferenz verfolgen will, der sollte seinen Ton, soweit es geht, ausschalten, damit es auch da nicht zu einer Rückkopplung kommt. Dann habe ich schon gesehen, dass einige Mitarbeiterinnen und Mitarbeiter sich in der WebEx-Konferenz bereits zu erkennen gegeben haben. Das sollte auch weiterhin so gehandhabt werden, dann haben wir nachher einen besseren Überblick über die Anwesenheit. Und wenn Sie sprechen bzw. sich zu Wort melden wollen und ich das nicht ohnehin gesehen habe, dann nennen Sie bitte am Anfang noch einmal Ihren Namen. Wenn ich Sie aufrufe, hat sich das natürlich erübrigt. Wenn es dann aber doch – das wollen wir nicht hoffen – zu irgendwelchen technischen Schwierigkeiten kommen sollte, dann sind wir entsprechend vorbereitet und werden mit einer Telefonkonferenz diejenigen zuschalten, die nicht präsent sein können. Aber wir hoffen mal, dass alles so wie sonst auch gut funktioniert. Nun komme ich zu den Hauptakteuren dieser Anhörung, nämlich zu den Sachverständigen. Ich begrüße alle in alphabetischer Reihenfolge: Zunächst einmal einen herzlichen Gruß nach Pakistan. Wir haben heute eine Sachverständige aus Pakistan, die englisch spricht. Eine Verdolmetschung wird es nicht geben. Darüber sind die Ausschussmitglieder vorher informiert worden. Frau Nighat Dad, ich grüße Sie in Lahore oder wo auch immer Sie sich gerade in Pakistan befinden. Vielen Dank, dass Sie an unserer Anhörung teilnehmen. Sie sind Executive Director of the Digital Rights Foundation in Pakistan. Dann begrüße ich ganz herzlich Herrn Dr. Matthias C. Kettemann vom Leibniz-Institut für Medienforschung/Hans-Bredow-Institut, Frau Dr. Constanze Kurz vom Chaos Computer Club, die bei uns im Ausschussraum sitzt, Frau Zara Rahman, stellvertretende Direktorin bei The Engine Room, Frau Lena Rohrbach, Referentin für Digitalisierung, Wirtschaft und Rüstungsexportkontrolle bei Amnesty International, Frau Dr. Kristin Shi-Kupfer vom Mercator Institute for China Studies und Herrn Joachim Nikolaus Steinhöfel, Rechtsanwalt – die beide hier im Ausschussraum präsent sind. Außerdem begrüße ich ganz herzlich, wie immer bei öffentlichen Anhörungen, die Beauftragte der Bundesregierung für Menschenrechtspolitik und humanitäre Hilfe, Frau Dr. Bärbel Kofler. Sie wird irgendwann den Raum verlassen, weil sie noch andere Termine hat. Aber schön, dass Sie trotzdem für eine Weile bei uns sind. Dann begrüße ich natürlich Sie alle hier im Ausschuss und in der WebEx-Konferenz. Aus anderen Ausschüssen sind diesmal keine Abgeordneten zu uns gekommen. Aber wenn das so wäre, müssten wir zumindest darüber befinden, ob sie Rederecht und auch Fragerecht bekommen. An dieser Stelle

sehe ich keinen Widerspruch; daher schauen wir, ob noch jemand zu uns findet. Wundern Sie sich nicht, wenn sich vielleicht ein Abgeordneter über WebEx zuschaltet, denn wir haben die Einladungen natürlich an verschiedene Ausschüsse geschickt. Aber jetzt zu unserem Thema: Ich glaube, das Thema hätte gar nicht besser platziert werden können als in einer solchen von der Corona-Pandemie geprägten Zeit, in der sich wahrscheinlich alle hier im Raum schon mit WebEx oder mit diversen anderen digitalen Lösungen vertraut gemacht haben. Digitalisierung ist in dieser Zeit ein sehr viel diskutiertes Thema. Wir wollen uns heute damit beschäftigen, welche Implikationen die Digitalisierung bzw. die digitale Teilhabe für die Menschenrechte hat, und wir haben dazu interessante Sachverständige eingeladen. Ich glaube, dass es vor allem vor dem Hintergrund der Entwicklungen im internationalen Zusammenhang interessant sein wird zu erfahren, wie etwa autoritäre Regime mit Überwachungssoftware, mit Gesichtserkennung, also mit Instrumentarien, die sowohl positiv als auch negativ genutzt werden können, umgehen, und was dies vor allem in der Corona-Zeit in den Gesellschaften bewirkt. Ich will diese thematischen Überlegungen nicht weiter ausdehnen, dann das wollen wir gleich mit Ihnen besprechen. Einen Hinweis muss ich Ihnen aber noch zum Ablauf und zum öffentlichen Charakter dieser Sitzung geben. Diese Anhörung ist öffentlich; sie wird allerdings nicht, wie das vorgesehen war, live übertragen, da parallel die deutsch-französische Parlamentarierkonferenz tagt und unseren Slot blockiert. Aber ab morgen ist die Anhörung in der Mediathek abrufbar, und entsprechend wird sie auch im Parlamentsfernsehen gesendet. Dann können Sie sich einschalten, und auch die Besucherinnen und Besucher oder andere Interessierte haben die Möglichkeit, die Aufzeichnung der Anhörung im Nachhinein in der Mediathek abzurufen. Außerdem wird es ein Wortprotokoll geben, das später ebenfalls auf der Internetseite abrufbar und damit öffentlich zugänglich ist. Außerdem möchte ich Sie darauf hinweisen, dass die schriftlichen Stellungnahmen der Sachverständigen den Ausschussmitgliedern und den eingeladenen Ausschüssen vorab zugeleitet worden sind. Sofern die Sachverständigen dem zugestimmt haben, werden die Stellungnahmen nach der Anhörung auf die Ausschussseite im Internet gestellt, und vor dem Ausschusssaal sind die Statements auch noch einmal verfügbar. Zum Ablauf der Anhörung ist Folgendes zu sagen: Wir haben uns am 10. Oktober 2018 im Ausschuss darauf verständigt, zu Beginn die Sachverständigen in alphabetischer Reihenfolge mit einem Eingangsstatement zu Wort kommen zu lassen. Dieses Eingangsstatement darf den zeitlichen Umfang von fünf Minuten nicht überschreiten. Wenn ihr Zeitrahmen ausgeschöpft ist, würde ich Ihnen einen entsprechenden Hinweis geben, da wir zeitlich sehr beschränkt sind und pünktlich um 17.00 Uhr schließen müssen. Das ist auch ein Appell an alle, damit wir hier gemeinsam erfolgreich tagen können. An die Statements der Sachverständigen wird sich eine erste Fraktionsrunde anschließen, die ebenfalls nach einem Verfahren ablaufen wird, auf das wir uns geeinigt haben. Nach dem Prinzip von Rede und Gegenrede von Regierungsfraktionen und Opposition haben die Ausschussmitglieder die Möglichkeit, jeweils bis zu zwei Minuten unbegrenzt viele Fragen an bis zu zwei Sachverständige zu stellen. Das heißt, die Kolleginnen und Kollegen der Union, die beginnen werden, können sich überlegen, ob nur ein Kollege die Frage stellt oder ob sie sich die Fragen aufteilen wollen. Ich bitte aber darum, auch dann die zwei Minuten nicht zu überschreiten. Das wäre wunderbar; andernfalls würde ich Sie mit Nachdruck darauf hinweisen, dass die zwei Minuten abgelaufen sind. Direkt danach wird dann der oder die Sachverständige um die Antwort gebeten, und diese Antwort darf vier Minuten nicht überschreiten. Auch darauf würde ich gegebenenfalls noch einmal hinweisen, damit Sie nicht durcheinander kommen. Ein Hinweis noch an die Zuhörer: Wenn Sie zum Auftakt Fotos oder Screenshots hier im Raum machen wollen, dann können Sie das gern tun. Danach bitte ich dann um ein bisschen mehr Ruhe im Ausschussgeschehen. Ansonsten freue ich mich auf die Anhörung und würde jetzt die Sachverständigen in der alphabetischen Reihenfolge aufrufen. Frau Nighat Dad, Sie sind die erste Sachverständige und Sie haben jetzt fünf Minuten Zeit für Ihr Eingangsstatement.

SVe **Nighat Dad** (Executive-Director der Digital-Rights-Foundation in Pakistan): Wunderbar. Ich

beginne also mit meiner Erklärung, die ich bereits schriftlich eingereicht hatte. Im südasiatischen Kontext sind digitale Räume und bürgerliche Freiheiten gefährdet durch regressive Gesetze und Bestimmungen sowie auch durch den Einsatz von Überwachungstechnologien, mit dem die Kontrolle der Regierungen über die Bevölkerung verstärkt werden soll. Verschärft wurde dies durch die Covid-19-Pandemie, mit der die Toleranz gegenüber der Nutzung von Technologie zur Verfolgung von Bürgern zunahm. Durch das Fehlen jeglicher Verfallsklauseln oder regulatorischer Rahmenbedingungen zur Überwachung des Einsatzes dieser Technologien ist sehr beunruhigend, wie sich eine Überlassung dieses Raums langfristig auswirken könnte. Darüber hinaus werden Online-Räume und Technologien nicht von allen Menschen einheitlich erlebt. Je nach Geschlecht, sexueller Orientierung oder Klasse ist der Zugang zum Internet unterschiedlich. Frauen besitzen seltener ein Gerät und haben seltener einen Social-Media-Account. Nach dem „Mobile Gender Gap Report 2019“ der Industrievereinigung der GSM-Mobilfunkanbieter (GSMA) herrschte in Pakistan das größte Geschlechtergefälle beim Mobilfunk, da Frauen dort mit einer um 37 Prozent geringeren Wahrscheinlichkeit als Männer ein Mobiltelefon besaßen. Die Barrieren sind dabei sowohl wirtschaftlich als auch gesellschaftlich.
31 Prozent der Frauen, die in Pakistan kein Mobiltelefon besitzen, geben an, dass die Missbilligung seitens ihrer Familie das Haupthindernis für den Besitz eines Handys darstelle. Dies bedeutet, dass selbst wenn Frauen Zugang zu einem Mobiltelefon bekämen, diese Geräte ohne eine größere Veränderung patriarchaler Einstellungen zu einer Quelle von Überwachung werden oder sogar zu Gewalt führen können, wenn eine als solche empfundene Indiskretion in Online-Räumen beobachtet wird. Trotz dieser Herausforderungen haben Frauen allerdings Online-Räume zur Einrichtung von Netzwerken und zum Aufbau feministischer Bewegungen genutzt. Sie nutzen diese Räume, so unzulänglich sie auch sein mögen, um Debatten über Genderfragen anzustoßen, um über ihre Erfahrungen zu sprechen und um mächtige Peiniger zur Rechenschaft zu ziehen, indem Online-Solidaritätsnetzwerke eingesetzt werden, mit denen traditionellen Machtverhältnissen entgegengewirkt werden soll. Da diese Räume allerdings zunehmend von Aktivisten und Menschenrechtsverteidigern genutzt werden, entwickeln sich die Überwachung und die Erosion von Persönlichkeitsrechten zu einem Problem für die körperliche Sicherheit vieler Menschenrechtsverteidiger. Da digitale Technologien häufig für Mobilisierungsmaßnahmen und wichtige Debatten über soziale Gerechtigkeit eingesetzt werden, setzen sie Menschenrechtsverteidiger auch neuen Bedrohungen aus, die häufig zu Schikanen und Gewalt durch staatliche und nichtstaatliche Akteure führen. Wird nichts dagegen unternommen, können digitale Räume eine allgemeine Selbstzensur erleiden und erheblich schrumpfen. Es wird immer angeprangert, dass im Globalen Süden mittels regressiver Gesetze internationale Menschenrechtsnormen verletzt würden, doch wenn wir uns die europäischen Länder ansehen, die hier Maßstäbe setzen sollten, werden sie ihnen oft nicht gerecht. Im gesetzlichen Bereich wurden beispielsweise mit dem von der britischen Regierung vorgelegten Weißbuch über Online-Schädigungen (Online Harms White Paper) und dem deutschen Netzwerkdurchsetzungsgesetz (NetzDG) Rahmenbedingungen geschaffen, um mächtige Technologie-Giganten zur Verantwortung zu ziehen. Gleichzeitig haben sie aber auch im Übermaß staatliche Macht und Regulierungsbefugnisse ermöglicht, die unter Umständen missbräuchlich gegen das Recht auf freie Meinungsäußerung eingesetzt werden könnten, insbesondere gegen Journalisten und Menschenrechtsverteidiger. Genau solche Gesetze werden nun von autoritären Regierungen verabschiedet, die sich auf „international bewährte Verfahren“ berufen. Wir erwarten von den Abgeordneten, die in mächtigen Parlamenten sitzen, es besser zu machen und bei den von ihnen vorgeschlagenen Eingriffen überlegter vorzugehen, da sie internationale Auswirkungen haben. Wir alle wissen, dass die Online-Sphäre Raum für Widerstand bieten und bestimmten Gruppen helfen kann, sich zu mobilisieren, um den Mächtigen die Wahrheit zu sagen. Das gilt heute mehr denn je, und wir können das derzeit überall auf der Welt beobachten. Meiner Meinung nach sind diese Gruppen, ein Zusammenschluss von Bewegungen und örtlichen Organisationen,

am ehesten in der Lage, sich staatlichen Schritten zur Einschränkung bürgerlicher Freiheiten zu widersetzen. Ihre Fähigkeit zu stärken, sich zu organisieren, und ihnen eine stärkere Stimme zu verleihen, ist zum Schutz der Menschenrechte im digitalen Raum unerlässlich. Die Ein- und Ausfuhr von Überwachungstechnologie muss streng reguliert werden, da Länder, die rasch zur Stelle sind, um „autoritären Regimen" Menschenrechtsverletzungen vorzuhalten, oftmals daran beteiligt sind, denselben Regimen Technologien zur Verfügung zu stellen, die gegen Menschenrechtsverteidiger, Aktivisten, Journalisten und Oppositionspolitiker als Waffe eingesetzt werden. Vielen Dank.*

Die **Vorsitzende**: Herzlichen Dank, Nighat. Wir lassen jetzt die anderen Sachverständigen zu Wort kommen. Ich rufe Sie auf, wenn die erste Frage gestellt wird. Der nächste Sachverständige ist Herr Dr. Matthias Kettemann vom Leibniz-Institut für Medienforschung/Hans-Bredow-Institut. Auch Sie haben fünf Minuten Zeit für Ihr Eingangsstatement.

SV Dr. **Matthias C. Kettemann** (Leibniz-Institut für Medienforschung, Hans-Bredow-Institut): Vielen herzlichen Dank. 2020 ist ein sehr wichtiges Jahr für Deutschland, insbesondere für Deutschlands Menschenrechtspolitik im Internet. 2020 kann Deutschland sich in verschiedenen Foren – im Sicherheitsrat und im Menschenrechtsrat der Vereinten Nationen, aber auch im Rahmen der EU-Ratspräsidentschaft – für den Schutz der Menschenrechte im Netz und für die verstärkte Teilhabe aller einsetzen. Deutschland ist auch ein Co-Champion für zwei Empfehlungen eines UNO-Berichtes zur Reform der digitalen Kooperation. Das Thema mag zwar im politischen Prozess nicht sehr präsent sein, Deutschland hat hier aber die Möglichkeit, auf Empfehlungen an den Generalsekretär der Vereinten Nationen Einfluss zu nehmen, die neue Internetregulierung auf dem Fundament der Grundsätze der Charta der Vereinten Nationen und der Achtung der Menschenrechte, insbesondere der politischen Teilhaberechte, auszugestalten. In dem Fragenkatalog des Ausschusses sind ganz zentrale Punkte angesprochen worden, auf die ich in aller Kürze eingehen möchte. Ich freue mich darauf, das dann später noch vertiefen zu können. Alle Menschenrechte gelten Offline wie Online. Die Voraussetzung dafür, Menschenrechte im Internet ausüben zu können, ist aber der Zugang zum Internet. Das sehen wir jetzt in aller Schärfe. Die Staaten müssten daher mehr tun, um einen menschenrechtskonformen Zugang für alle zum Internet zu ermöglichen. Da sind auch noch ganz konkrete Infrastrukturmaßnahmen zu tätigen. Wir brauchen auch mehr Wissen darüber, was schief läuft. Wir müssen bessere Daten erheben können. Es gibt erste Studien zur Lage des Internets in Deutschland; auch wir führen eine solche Studie durch. Forscherinnen und Forschern, aber auch Politikerinnen und Politikern müssen disaggregierte Daten über die Internetnutzung und über bestehende Diskriminierungen – insbesondere intersektionale Diskriminierungen – bei der Internetnutzung in Deutschland zur Verfügung stehen. Der Staat hat genau wie alle Akteure der Gesellschaft an einer menschenrechtskonformen Gestaltung des Netzes mitzuwirken. Dazu gehört natürlich auch, entsprechende Gesetze zu beschließen. Das Privatleben muss im Internet stark geschützt werden. Verschlüsselungen und Anonymität spielen eine wichtige Rolle. Ein Darknet-Gesetz ginge da in die falsche Richtung. Es gibt einige positive Beispiele dafür, wie das Internet genutzt werden kann, um Menschenrechtsverteidigerinnen und -verteidiger zu unterstützen. Man denke etwa an die Hashtag-Bewegung, den Online-Aktivismus zu #Metoo Aber das reicht nicht aus, um hegemoniale Strukturen, die auch im Internet die Kommunikationsprozesse beeinflussen, zu destabilisieren. Wir müssen auf allen Ebenen der Gesellschaft, von der Bildung bis zur Politik, verstärkt darauf hinwirken, dass das Internet nicht zu einem Ausgrenzungssystem wird und dass vor allem verletzliche Gruppen nicht aus dem Internet hinausgedrängt werden, wie dies im öffentlichen Diskurs in der Offlinewelt der Fall ist. Hassrede kann daher durchaus ein Vorwurf sein, der als rechtlich relevantes Instrument eingesetzt werden kann. Das Strafrecht bietet hier schon einige wichtige Anknüpfungspunkte. Wir sehen aber, dass das Problem vor allem in der Verfolgung, in der effektiven Strafverfolgung besteht. Da brauchen wir mehr Unterstützung für die Polizei,

wir brauchen mehr Mittel. Projekte wie das in Nordrhein-Westfalen, das schon erfolgreich abgeschlossen worden ist und das sich an der Maxime „verfolgen statt löschen“ orientiert hat, brauchen mehr Unterstützung. Auch die Ausbildung der Polizei im Bereich der digitalen Forensik muss ausgebaut werden. Nun kurz zum Thema Exportkontrolle: Hier ist Deutschland gerade vor dem Hintergrund seiner Rolle im Sicherheitsrat, im Menschenrechtsrat und bei der EU-Ratspräsident gefordert, darüber nachzudenken, ob nicht eine zu lange Genehmigungsdauer Unternehmen dazu verleiten könnte, Umgehungsgeschäfte zu tätigen. Diesbezüglich muss ein besonderes Augenmerk auf Transparenz sowie auf die Nutzung der Teilung von Daten für die Formulierung einer optimalen Politik gelegt werden. Ich freue mich auf Ihre weiteren Fragen.

Die **Vorsitzende**: Herzlichen Dank, Herr Dr. Kettemann. Dann hätten wir als Nächste hier im Sitzungssaal Frau Dr. Constanze Kurz. Auch Sie haben fünf Minuten Zeit.

SVe Dr. **Constanze Kurz** (Chaos Computer Club): Ja, vielen Dank. Auch ich orientiere mich an dem strukturierten Fragenkatalog, den wir vorab erhalten haben, und ich werde versuchen, nicht zu wiederholen, was wir gerade schon gehört haben. Ich verweise dann auf meine schriftliche Stellungnahme. Mir sind drei Aspekte aus diesem strukturierten Fragen wichtig, die ich hier ansprechen möchte. Das sind erstens Fragen der Verschlüsselung zur Anonymisierung und Fragen zum Darknet. Bei uns ist der Begriff Darknet sehr negativ belegt; aber faktisch bedeutet die Verfügbarkeit einer Infrastruktur – die vor allem von den Staaten des Westens bereitgestellt wird –, mit der man anonymisiert kommunizieren kann, für viele Länder – gerade außerhalb Europas – die einzige Möglichkeit, Informationen ins Netz zu stellen, ohne dafür mit Repression belegt zu werden. Wenn wir heute solche technischen Instrumentarien zur Verfügung stellen, dann beinhaltet dies für andere möglicherweise die Chance, um Informationen weiterzugeben. Das heißt, wenn wir damit anfangen, Verschlüsselung zu schwächen oder aber zu verbieten bzw. wenn wir hier im Westen Hintertüren einbauen, dann hat dies für die von Repression bedrohten Menschen anderswo möglicherweise eine Bedrohung für Leib und Leben zur Folge. Wie Sie wissen, gilt das Darknet bei uns als Ort der Kriminalität; letztlich bezeichnet es aber nur die Möglichkeit, mit einer verschlüsselten und anonymisierten Technologie Informationen ins Netz zu stellen und diese Informationen dort aufzufinden. Der mit Abstand größte Anbieter im Darknet – das wissen nicht viele – ist Facebook, gefolgt von der BBC. Längst haben also auch die westlichen Social-Media-Unternehmen und auch normale Medienunternehmen damit angefangen, für nichtdemokratische Länder, aber auch für alle anderen Länder, die das wollen, im Darknet bzw. im sogenannten Darknet ihre Informationen zur Verfügung zu stellen. Das ist für uns so bedeutsam, weil wir die Infrastruktur dafür bieten, also auch die Software dafür herstellen. Organisationen wie das Projekt TOR werden mit westlichen Geldern finanziert und sind enorm wichtig in diesem Zusammenhang. Wir haben auch noch ein paar andere Beispiele dafür in der schriftlichen Stellungnahme aufgeführt. Ein zweites wichtiges Element ist die Software Securydrop, die die Möglichkeit bietet, Informationen zum Beispiel an Medienunternehmen weiterzugeben. Diese Software haben viele internationale Medienhäuser mittlerweile in Benutzung. Auch hier gilt: Wann immer im Westen zum Beispiel für Zwecke der Strafverfolgung oder für die Geheimdienste in solche Software Hintertüren eingebaut würden, hätte dies unmittelbar negative Auswirkungen für Menschen in Diktaturen. Um dieses Thema abzuschließen: Die Verschlüsselung ist die Basis für all diese Techniken. Die Art und Weise, wie wir damit umgehen, hat immer auch weitreichende Folgen für die internationale Menschenrechtslage. Der Verzicht auf Hintertüren ist daher von besonderer Bedeutung. Wir haben außerdem versucht, die Frage nach den größten Bedrohungen für die Menschenrechte durch die Digitalisierung zu beantworten, indem wir eine Liste erstellt haben – was gar nicht so einfach war. Was sind eigentlich in der digitalisierten Welt die größten Bedrohungen weltweit für die Menschenrechte? An erster Stelle steht hier sicherlich jede Form von anlassloser Massenüberwachung, die heute mit digitalen Mitteln möglich ist. Verfolgt wird dieser Ansatz

im Wesentlichen in Bezug auf Telekommunikationsmetadaten, aber auch auf Telekommunikationsinhaltsdaten. Dazu hat es gerade – wie Sie sicherlich wissen – im Mai 2020 eine Entscheidung des Bundesverfassungsgerichts gegeben, das aktuelle BND-Urteil. Außerdem gibt es das Verfahren eines der Beschwerdeführer vor dem Europäischen Menschenrechtsgericht in Bezug auf anlasslose Massenüberwachung. Dazu werden wir sicherlich noch Urteile bekommen. Aber diese Frage, über die bei uns vor den höchsten Gerichten gestritten wird, ist anderswo eine Frage von Leben und Tod, oder sie entscheidet darüber, ob man in einem Folterkeller landet oder ob die eigene Familie noch frei leben kann. Selbstverständlich sollte Europa hier ein Vorbild sein. Dabei geht es nicht nur um Telekommunikationsdaten, sondern natürlich auch um neuere Technologien, die massenhaft eingesetzt werden sollen, wie zum Beispiel die Biometrie, also die automatisierte Gesichtserkennung. Auch Deutschland kann hier seine Hände nicht mehr in Unschuld waschen, weil die Innenminister bereits angekündigt haben – zuletzt war das Thomas de Maizière –, diese flächendeckend einsetzen zu wollen. Die automatisierte Gesichtserkennung wirft zwar immer noch technische Probleme auf, sie ist aber im letzten Jahrzehnt sehr viel besser geworden. Wir haben noch eine weitere Liste erstellt, auf die wir in unserer schriftlichen Stellungnahme nicht so ausführlich eingegangen sind. Da geht es – da ja auch die politische Teilhabe im Fokus dieser Anhörung steht – um Technologien wie E-Voting oder computerisierte Wahlen, bei denen die Manipulationsgefahr sehr hoch ist. Dazu zählt aber auch die ganze Problematik des sogenannten Cyberwar. Dabei geht es um Entitäten, die überhaupt keine rechtlichen Rahmenbedingungen akzeptieren, die eklatant gegen das Völkerrecht verstoßen und in der Regel zum Militär oder zu Geheimdiensten gehören und die sozusagen hinter unserem Rücken Krieg gegen unsere zivile Infrastruktur führen. Abschließend möchte ich noch – ich will das aber nicht weiter ausführen, weil wir das eben schon angesprochen hatten – darauf hinweisen, dass wir sehr konkrete Vorschläge gemacht haben, wie der Export von Überwachungssoftware von Europa aus nach unserem Dafürhalten künftig geregelt werden sollte. Ich verweise da auf unsere schriftliche Stellungnahme. Vielen Dank.

Die **Vorsitzende**: Herzlichen Dank, Frau Dr. Kurz. Dann haben wir als Nächste in der Reihenfolge Frau Zara Rahman, die stellvertretende Direktorin bei The Engine Room. Auch Sie haben fünf Minuten Zeit.

SVe **Zara Rahman** (stellvertretende Direktorin bei The Engine Room): Vielen Dank. Wir sehen heute, dass digitale Technologien häufig von Konzernen genutzt werden, um Bürgerinnen zu überwachen, Menschenrechte zu beschränken und insgesamt Kontrolle über Menschen auszuüben. Es gibt viele Strategien, die Staaten anwenden, um ihre Bürgerinnen durch Technologie zu kontrollieren, wie zum Beispiel das Social Credit Scoring in China oder Internetsperren, wie sie im Jahr 2019 in mehr als 33 Ländern vorgekommen sind. Aber diese Strategien sind nicht nur ein Werkzeug von Autokratien, sie werden auch von sogenannten Demokratien und oft auch gegen gefährdete Bevölkerungsgruppen im eigenen Land angewendet. Zum Beispiel hat Bangladesch seit Monaten das Internet abgeschafft und den Verkauf von SIM-Karten und Handys verboten – angeblich aus Sicherheitsgründen. Jetzt während der Corona-Pandemie ist der Zugang zu aktuellen Informationen eine Frage von Leben und Tod.
Eine besonders beunruhigende Form der Überwachungstechnologie ist die Technologie zur Gesichtserkennung. Es fehlt in den meisten Ländern an Gesetzen, die die Gefahren der Gesichtserkennungstechnologie behandeln würden. Letzte Woche hat die Firma IBM bekannt gegeben, dass sie die Gesichtserkennungstechnologie nicht mehr verkaufen, entwickeln oder erforschen wird. Einen Tag später haben Amazon und Microsoft ein einjähriges Moratorium für die Benutzung der Gesichtserkennungstechnologie durch die Polizei angekündigt. Obwohl es ermutigend ist zu erleben, dass Firmen mehr Verantwortung für die sozialen Auswirkungen von neuen Technologien übernehmen wollen, sollten wir nicht warten, bis private Unternehmen ein soziales Gewissen entwickeln, bevor wir Regeln für gefährliche neue Technologien schaffen. Wir müssen auch an die Macht denken, wenn wir von Transparenz und Datenschutz reden. Sowohl Transparenz als auch

Datenschutz sind wesentliche Werte, die in unserer digitalen und analogen Welt gestärkt werden müssen. Um den Missbrauch von Macht in einer Demokratie zu verhindern, muss Folgendes klar sein: Wer Macht hat, muss transparent sein, und je mächtiger jemand ist, desto transparenter sollte er sein. Als Gegenstück brauchen Menschen mit weniger Macht, normale Bürgerinnen zum Beispiel, starke Datenschutzrechte, um ihre Selbstbestimmtheit zu schützen, und um Rechte und Meinungsfreiheit effektiv zu nutzen. Wenn Personen, die viel Macht haben, aber wenig Transparenz bieten, diese Macht missbrauchen, dann brauchen wir Whistleblower, um wichtige Informationen ans Licht zu bringen. Frau Dr. Kurz ist auf die Bedeutung von anonymisierter Kommunikation schon eingegangen. Die digitale Welt bietet auch neue Möglichkeiten für die digitale Teilhabe. Ein Beispiel sind Online-Plattformen für Informationsfreiheit, die es ermöglichen, Anfragen nach internationalen Freiheitsgesetzen mit einfachen Mitteln zu stellen. Diese Plattformen haben das Recht auf Zugang zu Informationen in das digitale Zeitalter gebracht. Ein anderes Beispiel für die neue digitale Teilhabe ist der Afro-Zensus, eine freiwillige Initiative, die Daten über die Lebens- und Wirtschaftsbedingungen der schwarzen afrikanischen und afrodiasporischen Bevölkerungen in Deutschland sammelt. Die digitale Welt ermöglicht es Initiativen, selbst Daten zu ihrer Geschichte erheben. Ein Ziel davon ist, Rassismus in Deutschland nicht nur sichtbar zu machen, sondern auch besser zu verstehen, damit man das Problem möglicherweise lösen kann. Wir erkennen die Wichtigkeit solcher Daten auch in Bezug auf Gendergerechtigkeit, zum Beispiel bei Initiativen wie „50 Prozent“, die dokumentieren, wie stark Frauen als Rednerinnen bei Konferenzen und Talkshows unterrepräsentiert sind. Frauen sind besonders von technikbasierter Gewalt bedroht, wenn etwa persönliche Daten gegen den Willen der Betroffenen erhoben werden, durch Stalking oder durch Beleidigungen, die oft über soziale Medien verbreitet werden. Die Grenze zwischen Offline und Online wird immer unschärfer. Die Gesetze zum Schutz der Menschenrechte müssen angepasst werden, um diesen neuen Realitäten gerecht zu werden. Das digitale Zeitalter bietet aber auch die Möglichkeit, die Arbeit von Regierungen transparenter zu machen und die politische Beteiligung zu erhöhen. Die Digitalisierung bringt aber auch neue Herausforderungen mit sich, die den Zugang zu diesen Technologien, aber auch deren Missbrauch betreffen. Wenn man Menschenrechte im digitalen Zeitalter schützen, verteidigen und durchsetzen will, müssen bei der Umsetzung von Maßnahmen die Menschenrechte in den Mittelpunkt gestellt und die bestehenden sozialen Strukturen berücksichtigt werden. Vielen Dank.

Die **Vorsitzende**: Herzlichen Dank, Frau Rahmann. Als Nächste ist Lena Rohrbach, Referentin für Digitalisierung, Wirtschaft und Rüstungsexportkontrolle bei Amnesty International an der Reihe. Fünf Minuten Zeit stehen auch Ihnen zur Verfügung.

SVe **Lena Rohrbach** (Referentin für Digitalisierung, Wirtschaft und Rüstungsexportkontrolle, Amnesty International): Vielen Dank für die Möglichkeit, hier sprechen zu dürfen. Amnesty beobachtet die Entwicklung einer Art von Werkzeugkasten, von Methoden und Technologien, die weltweit von Regierungen für einen Angriff auf die Zivilgesellschaft eingesetzt werden. Das heißt, die sogenannten Shrinking Spaces gibt es auch im digitalen Raum. Dazu gehören Internet-Shutdowns, die Zensur von Webseiten oder Socialmedia-Plattformen, so genannte Cybercrime Laws, die legitime freie Meinungsäußerung online kriminalisieren, Massenüberwachung sowie das Kriminalisieren von Anonymisierungs- und Verschlüsselungswerkzeugen wie VPN oder TOR, Hoffentlich wird sich Deutschland mit dem Darknet-Paragrafen nicht in die Riege der Staaten einreihen, die solche Beschränkungen vornehmen. Auf zwei weitere Werkzeuge möchte ich kurz näher eingehen. Erstens auf Spionagesoftware und zweitens auf die Gesichtserkennungstechnologie. Immer häufiger werden Menschenrechtsverteidiger weltweit gezielt wegen ihres Engagements überwacht, indem man ihre Smartphones oder Computer mit Spionagesoftware infiziert. Die Angreifer können dann Dateien von der Festplatte lesen oder verändern, sie können Standortdaten abfragen oder die Kamera heimlich anschalten, um private

Räume auszuspähen und verschlüsselte Kommunikation mitzulesen. Dies setzt Menschenrechtsverteidigerinnen und auch ihre Familien und Kontaktpersonen einem großen Risiko aus. Die verwendete Technologie kommt auch aus Europa, zum Beispiel von der Münchener Firma Findfischer oder dem italienischen Hackingteam. Europäische Firmen rüsten somit Regierungen mit miserabler Menschenrechtsbilanz auf, um Menschenrechtsverteidigerinnen zu überwachen. Es gibt zurzeit eine Chance, diesen Missstand zu beseitigen. Die Dual Use-Verordnung der EU, die den Export von Überwachungstechnik reguliert, wird derzeit reformiert. Leider sind die Kompromissvorschläge, die zurzeit auf dem Tisch liegen, ungeeignet, die Probleme zu beheben. Der voraussichtliche Abschluss der Trilog-Verhandlungen fällt aber in die Zeit der deutschen EU-Ratspräsidentschaft. Wir möchten, dass die Bundesregierung diese Gelegenheit nutzt, um sich für effektive Exportkontrollen stark zu machen. Zur Gesichtserkennungstechnologie: Immer mehr Staaten setzen identifizierende Gesichtserkennungstechnologie anlasslos im öffentlichen Raum ein. Auch in Deutschland hat dies auf Vorschlag des BMI zur Debatte gestanden. Wir leben bereits in einer Zeit potentiell vollständiger Überwachung der elektronischen Kommunikation. In manchen Ländern müssen Menschenrechtverteidigerinnen zusätzlich mit verwanzten Wohnungen rechnen. Die Gesichtserkennung schließt den für viele Menschen letzten überwachungsfreien Rückzugsraum. In der sogenannten Überwachungsgesamtrechnung ist die Gesichtserkennung daher nochmal ein qualitativer Sprung. Obwohl es häufig um legitime Ziele geht, zum Beispiel darum, Straftäter zu finden, kann die automatisierte Gesichtserkennung im öffentlichen Raum nach Auffassung von Amnesty nicht verhältnismäßig eingesetzt werden, weil sie alle vorbeikommenden Menschen anlasslos und ohne einen individualisierten begründeten Verdacht erfasst und analysiert. Damit verletzt sie unseres Erachtens das Recht auf Privatsphäre. Gesichtserkennung wirkt außerdem durch sogenannte Chilling Effects lähmend auf die Versammlungsfreiheit und führt erwiesenermaßen zu Diskriminierung. Es bedarf deshalb dringend einer Regulierung. Gesichtserkennung wird nämlich immer präziser und auch immer billiger. Deshalb nimmt ihr Einsatz weltweit zu. Das geschieht aber in einem Regulierungsvakuum, da Entwicklung und Einsatz die Gesetzgebung überholt haben. So etwas passiert häufig beim Einsatz von Technik, übrigens auch in der EU. Eine Kontrolle des Handels findet ebenfalls praktisch nicht statt. Die bereits genannte Dual Use-Verordnung erfasst nämlich die biometrische Überwachung noch gar nicht. So könnte zum Beispiel identifizierende Gesichtserkennung aus der EU nach China exportiert werden, ohne dass die dortige Menschenrechtslage eine Rolle spielen würde. Nach Ansicht von Amnesty bedarf es dringend eines Verbotes der Verwendung, Entwicklung, Produktion, des Verkaufs und des Exports von Gesichtserkennung zu Identifikationszwecken im öffentlichen Raum. Es bedarf eines Verbotes in Deutschland und in der EU sowie einer weltweiten Ächtung. Ein kleines Gedankenexperiment zum Schluss: Das Schlimmste, was passieren kann, wenn wir uns zu diesem Schritt entschließen, ist, dass alles ungefähr so bleibt, wie es ist. Das Schlimmste, was passieren kann, wenn wir es unterlassen, ist, dass die Freiheit unbeobachteter Bewegung im öffentlichen Raum beendet wird und dass sich in manchen Staaten durch Kombination mit Informationen aus der Kommunikationsüberwachung ein vollständiges Bild des Alltags der Bürgerinnen ergibt. Das ist nicht der Weg, den wir in Deutschland oder in der EU oder die Menschheit insgesamt gehen sollten. Vielen Dank.

Die **Vorsitzende**: Vielen Dank, Frau Rohrbach. Dann hat als nächste Frau Dr. Kristin Shi-Kupfer vom Mercator Institute for China Studies das Wort, und zwar für fünf Minuten.

SVe Dr. **Kristin Shi-Kupfer** (Mercator Institute for China Studies): Vielen Dank für die Gelegenheit zum Austausch. Ich hoffe, Sie hören mich alle gut – kurzer Soundcheck – o.k., wunderbar. Das Beispiel China zeigt sehr gut, wie wichtig die Verknüpfung zwischen digitalen Technologien, Menschenrechten und politischer Teilhabe ist. Denn aus Sicht der chinesischen Regierung ist das Land eine Art digitales Labor. Für uns stellt es hingegen ein lehrreiches Schaufenster für all den

Missbrauch und für all die Bedrohungen dar, die von digitalen Technologien ausgehen können. Ich möchte nicht ausschließen, dass es auch in China positive Impulse geben kann, was soziale Entwicklung oder soziale Gleichheit angeht; aber ich sehe doch die Bedrohung als sehr massiv an, und deswegen möchte ich mich im Folgenden darauf konzentrieren. In China können wir beobachten, dass die Regierung in dem Maße, wie sie digitale Technologien einsetzt und entwickelt, an Selbstbewusstsein gewinnt und dieses auch nach außen zur Schau trägt. Zugleich weist sie die Universalität jener grundlegenden Werte zurück, die sie einmal mit unterschrieben hat, also auch die allgemeinen Menschenrechte. Das trägt sie zunehmend in der Form nach außen, dass sie die Überlegenheit des chinesischen Systems im Vergleich zu liberalen Demokratien proklamiert. Der Einsatz sowie der Entwicklungs- und Innovationsgrad von digitalen Technologien ist ein wichtiger Bestandteil dieses Narrativs. Das zeigt sich ganz aktuell am Beispiel des Einsatzes von datengetriebenen Technologien zur Bekämpfung von Covid-19. Grundsätzlich verwendet Peking das Argument, dass digitale Technologien ein effektives Instrument zur Aufrechterhaltung von Sicherheit und Ordnung darstellen. Auf Menschenrechtsverletzungen geht Peking hingegen kaum ein. Allenfalls werden kommerzielle Interessen von Unternehmen oder Verfehlungen von einzelnen lokalen Behörden als potentielle Ursache zum Beispiel für Datenleaks genannt. Lange Zeit fühlte sich die chinesische Regierung in dieser Haltung bestätigt – gerade auch im Zusammenhang mit Covid-19, weil sie für sich in Anspruch nahm, die Pandemie durch den Einsatz dieser Technologie erfolgreich bekämpft zu haben. Aber es zeigt sich interessanterweise ganz aktuell durch den neuen Corona-Ausbruch in Peking, dass der Einsatz digitaler Technologien allein eben nicht ausreicht. Ich möchte im Gegenteil betonen, dass auch hier eine transparente und wahrheitsgemäße Kommunikation mit der eigenen Bevölkerung und der internationalen Gemeinschaft das Wesentliche ist und dass digitale Technologien nur dann erfolgreich eingesetzt werden können. Die Auswirkungen, die der Einsatz digitaler Technologien für die Menschenrechtssituation und die politische Teilhabe in China hat, sind, denke ich, hinlänglich bekannt. Sie sind auch in anderen Zusammenhängen schon genannt worden. Ich erinnere an den Ausbau der Überwachungskapazitäten in Bezug auf kritische Köpfe wie Rechtsanwälte oder Journalisten, aber auch ganz generell im öffentlichen Raum – unter dem Stichwort Smart Citys. Im Zusammenhang mit Covid-19 wird jetzt auch die Überlegung angestellt, die speziell dafür erhobenen Datensätze zu verstetigen und möglicherweise mit anderen Datensätzen im Rahmen des sozialen Bonitätssystems zu verknüpfen. Was bedeutet das alles für uns im internationalen Kontext, wenn es um die Wahrung von Menschenrechten und Teilhabe geht? Ich denke, wir werden eine zunehmende systematische Beeinflussung und auch Manipulation der internationalen öffentlichen Meinung erleben – nicht nur durch einzelne chinesische Diplomaten – und auch einen wachsenden politischen Druck auf bzw. Anreize für ausländische Unternehmen, Zensuroptionen in ihre Technologie einzubauen. Das haben wir bei YouTube und auch bei Linkedin schon erlebt, und die ganze Debatte über Zoom ist natürlich auch allen ein Begriff. Ferner verweise ich auf den potentiellen Missbrauch von Daten chinesischer Bürger und aller Bürger außerhalb Chinas durch den aktiven Export von chinesischen Apps, von Datenspeicherungstechnologie und überhaupt von digitaler Infrastruktur in andere Länder. Was können bzw. müssen wir tun? Viele Dinge sind schon genannt worden, die Exportkontrolle zum Beispiel. Umgekehrt geht es, wenn wir etwa an die Beschaffung von Technologie durch die öffentliche Hand in Deutschland, zum Beispiel durch die Polizei, denken – auch darauf ist von den Kolleginnen und Kollegen schon hingewiesen worden –, darum zu prüfen, ob chinesische Unternehmen mit ihrer Technologie nicht bereits in China, aber dann durch den Export auch in anderen Ländern zu Menschenrechtsverletzungen beitragen. Für öffentliche Institutionen ist es, denke ich, auch wichtig, bei Projekten der digitalen Forschungskooperation oder auch bei der Medienkooperation genau zu prüfen, woher die Daten oder die Inhalte stammen. Ich denke, eine Zensur von auf China bezogenen Inhalten müssen wir in unseren liberalen Demokratien grundsätzlich und entschieden zurückweisen. Ich möchte abschließend Taiwan erwähnen. Ich denke, Taiwan ist eine hoch entwickelte und

effektive digitale Gesellschaft, die viel mehr Aufmerksamkeit und auch Anerkennung von unserer Seite verdient und mit der wir stärker kooperieren sollten. Vielen Dank.

Die **Vorsitzende**: Herzlichen Dank, Frau Dr. Shi-Kupfer. Als letzter in der Expertenrunde – last but not least – ist Joachim Nikolaus Steinhöfel an der Reihe. Sie haben das Wort für fünf Minuten.

SV **Joachim Nikolaus Steinhöfel** (Rechtsanwalt): Wenn man nur eine Handvoll Grundrechte aufzählt, die das Wesen einer freien, rechtsstaatlichen und demokratischen Gesellschaft in ihrem Kern ausmachen, gehört die Meinungsfreiheit dazu. Das Bundesverfassungsgericht bezeichnet sie in seiner Rechtsprechung immer wieder als schlechthin konstituierend für die freiheitlich-demokratische Ordnung. Ich habe tatsächlich kurz gezögert, ob ich, um die Reichweite dieses Grundrechts noch einmal vor Augen zu führen, tatsächlich aus einer Entscheidung des Bundesverfassungsgerichts zitieren sollte. Sie werden vielleicht gleich erkennen, warum. Juni 2018: „Das Anliegen, die Verhinderung verfassungsfeindlicher Ansichten zu verhindern, ist ebenso wenig ein Grund, Meinungen zu beschränken, wie deren Wertlosigkeit oder auch Gefährlichkeit.“ Oder, auch aus dem Jahr 2018: „Die mögliche Konfrontation mit beunruhigenden Meinungen, auch wenn sie in ihrer gedanklichen Konsequenz gefährlich und selbst wenn sie auf eine prinzipielle Umwälzung der geltenden Ordnung gerichtet sind, gehört zum freiheitlichen Staat. Der Schutz vor einer Vergiftung des geistigen Klimas ist ebenso wenig ein Eingriffsgrund wie der Schutz der Bevölkerung vor einer Kränkung ihres Rechtsbewusstseins durch totalitäre Ideologien oder eine offenkundig falsche Interpretation der Geschichte.“ Dass auch ich persönlich viele Äußerungen, die damit zulässig sind, als widerwärtig erachte, darf ich Ihnen versichern. Aber Abscheu und ideologische Verachtung sind keine relevanten Kriterien im Sinne der Verfassung. In einem von vagen und unbestimmten Rechtsbegriffen wie „Hassrede“ und „Hetze“ beschädigten Diskurs erachten wahrscheinlich auch viele ganz normale Bürger die Verfassungsrichter als Steigbügelhalter einer Verwahrlosung der Debatte, wenn sie diese Zitate ohne Fundstelle lesen würden. Ich erzähle Ihnen nichts Neues, wenn ich darauf hinweise, dass die sozialen Medien den politischen und sozialen Diskurs revolutioniert und teilweise sicherlich auch befreit haben. Der fast kostenlose Zugang von Milliarden Menschen zu einem Forum Romanum der Gegenwart begründet eine Zeitenwende. Vielleicht erzähle ich Ihnen aber etwas Neues, wenn Sie erfahren, dass Facebook nicht nur eine vom Petitionsausschuss des Bundestages gebilligte und auf der Webseite des Bundestages veröffentlichte Petition als „Hassrede“ gelöscht und dies auch noch vor Gericht verteidigt hat. Vielleicht überrascht es Sie, wenn Sie erfahren, dass dasselbe Unternehmen zugibt, automatisiert Links zu einem deutschen Nachrichtenmagazin zu löschen, gegen ein Verbot Rechtsmittel einlegt, in der Verhandlung aber nicht begründen kann, warum die Löschung massenhaft technisch erfolgt ist, oder dass YouTube zugibt, völlig legitime Videos ohne eigene Überprüfung nur deswegen zu löschen, weil sie massenhaft denunziert wurden, für die Korrektur der eigenen Fehler aber Wochen braucht. Die YouTube-Chefin erklärte kürzlich bei CNN, sie werde alles löschen, was sich gegen die Verlautbarungen und Empfehlungen der Weltgesundheitsorganisation richte. Pressefreiheit, Meinungsfreiheit und Wissenschaftsfreiheit stehen jetzt also unter dem Vorbehalt der Billigung durch eine nichtdemokratisch legitimierte Institution. Erst kürzlich wurde vom Oberlandesgericht Karlsruhe ein als Faktencheck getarnter Eingriff in die Meinungsfreiheit durch die auch mit Steuergeldern subventionierte Organisation CORREKTIV als rechtswidrig untersagt. Es steht hier die fundamentale Frage im Raum, wer in einer offenen Gesellschaft legitimer Weise über wahre und falsche Meldungen entscheiden soll. Die Gefährdung der Meinungsfreiheit rührt aber nicht nur von Seiten der sozialen Netzwerke her. Das Netzwerkdurchsetzungs-Gesetz wird von der großen Mehrheit der Juristen wegen Verletzung von Artikel 5 als eindeutig verfassungswidrig erachtet. Bei der Anhörung im Rechtsausschuss schon 2017 hieß es: Das Bundesverfassungsgericht wird seine Rechtsprechung zur Meinungsfreiheit nicht vom Netzwerkdurchsetzungs-Gesetz faktisch einebnen lassen. Es bedarf nur noch einer Klage in

diese Richtung. Das war nur eine von acht ähnlichen, deutlich vernehmbaren Einschätzungen der Sachverständigen. Und es ist auch kein Ruhmesblatt für politische Verantwortungsträger, wenn ein Staatssekretär im Auswärtigen Amt einen Journalisten der Jerusalem Post bei Twitter blockiert und dies erst auf Abmahnung hin aufhebt, oder wenn eine Berliner Senatorin aus denselben Gründen eine Unterlassungserklärung unterschreiben muss, oder wenn ein Mitglied dieses Ausschusses einem normalen Nutzer auf Facebook droht – wörtlich: „Ja, dann werde ich Ihren Arbeitgeber mal fragen, ob das denn betriebstypisch ist, was Sie da absondern." Die Gewährleistung dieses Grundrechts in einer neuen digitalen Wirklichkeit ist eine schwierige und komplexe Herausforderung für den Gesetzgeber. Darum möchte ich mit einem ausdrücklichen Lob schließen. Die vorgesehene Änderung im § 5 Netzwerkdurchsetzungs-Gesetz zum Zustellbevollmächtigen wäre ein für die zahlreichen betroffenen Nutzer großer Schritt zur effizienteren Durchsetzung ihrer Rechte gegen die IT-Riesen. Denn dann können Abmahnungen, einstweilige Verfügungen und Klagen in Deutschland zugestellt werden. Und es wäre bei drastisch reduziertem Kostenrisiko und gleichzeitiger Entlastung der Justiz möglich, sich schneller und wirksamer gegen Sperrungen und Löschungen zu wehren. Vielen Dank.

Die **Vorsitzende**: Herzlichen Dank, Herr Steinhöfel. Dann kommen wir jetzt zur ersten Fraktionsrunde. Ich erläutere noch einmal ganz kurz das Verfahren. Die Union hat jetzt gleich als erste Fraktion die Möglichkeit, bis zu zwei Sachverständige zu befragen. Herr Brand nickt schon, er kennt das Prozedere. Ich weise Sie auch noch einmal darauf hin, dass Sie zwei Minuten Zeit für die Fragen haben und die befragten Sachverständigen vier Minuten für die Beantwortung, die sich dann anschließt. Herr Brand, Sie haben das Wort.

Abg. **Michael Brand** (Fulda) (CDU/CSU): Herzlichen Dank – der aufgrund der Zeit kurz ausfällt – für Ihre schriftliche und mündliche Stellungnahme. Meine erste Frage richtet sich an den Sachverständigen Dr. Kettemann. Im Anschluss an Ihre Ausführungen möchte ich erfahren, wie Deutschland auf globaler Ebene für Menschenrechte und digitale Teilhabe eintreten und den Internet Governance Process, der – wie von Ihnen geschildert – eine hohe Legitimität besitzt, durch die Einbindung und Beteiligung der Akteure Staat, Privatsektor, Unternehmen und Zivilgesellschaft fördern kann. Meine zweite Frage richtet sich … Wo sieht man eigentlich die Zeit, man wird ja gehetzt …

Die **Vorsitzende**: Sie haben bis jetzt 40 Sekunden gebraucht, ich weise Sie darauf hin.

Abg. **Michael Brand** (Fulda) (CDU/CSU): Frau Shi-Kupfer, anknüpfend an ihre schriftlichen Ausführungen zu unserer entsprechenden Frage haben sie hier über die Totalüberwachung und die Kontrolle der gesamten Bevölkerung in China gesprochen. Mich würde interessieren, welche Gegenreaktionen diese Strategie regional zum Beispiel in Hongkong, Taiwan, Indien, Japan, Korea, Vietnam oder Australien und international in Afrika, Südosteuropa, Osteuropa, Mitteleuropa – auch im digitalen Bereich – ausgelöst hat. Zudem haben Sie China als digitales Labor bezeichnet. Daher meine Frage: Besteht die Gefahr, dass dieses digitale Labor sich vor allem in autoritären Staaten ausbreiten könnte wie ein Krebsgeschwür?

Die **Vorsitzende**: Herzlichen Dank, Herr Brand. Dann würde ich jetzt in der Reihenfolge der angesprochenen Sachverständigen zunächst Herrn Dr. Kettemann für vier Minuten das Wort geben.

SV Dr. **Matthias C. Kettemann**: Vielen herzlichen Dank für die Fragen. Ich führe dazu gern etwas aus. Bei der Internet Governance geht es um die Regulierung des Internets und den Aufbau der zentralen Strukturen, in denen entschieden wird, welche Standards im Netz gelten sollen, ob neue Technologien eingesetzt werden und wie die Adressierung funktioniert. Darüber wird in ganz verschiedenen Gremien verhandelt, zum Beispiel in der Internationalen Telekommunikationsunion, aber auch in anderen UNO-Gremien. Hier ist jetzt die Möglichkeit gegeben, die internationalen Räume, über die debattiert wird, neu zu gestalten.

Im letzten Jahr, 2019, hat in Berlin das Internet Governance Forum stattgefunden. Das ist das weltweit größte Forum, in dem über Internetregulierung diskutiert wird. Frau Merkel hat das Forum gemeinsam mit dem UN-Generalsekretär eröffnet. Dieses Forum soll einen neuen Charakter bekommen, es soll entschiedener auftreten und vielleicht sogar Normen entwickeln können. Ganz bemerkenswert ist ein Prozess, der gerade abläuft. Deutschland ist, wie erwähnt, mitverantwortlich dafür, dem Generalsekretär Vorschläge zur besseren Aufstellung des Internet Governance Forums zu machen. Dazu führen das Wirtschaftsministerium und das Außenministerium mit Hilfe von Projektpartnern zurzeit eine globale Befragung durch und fassen die Weltmeinung zu diesem Thema zusammen. Die Projektpartner interviewen über das Internet Vertreter der Zivilgesellschaft, Vertreter anderer Staaten sowie Vertreterinnen und Vertreter von Nichtregierungsorganisationen und Unternehmen. Dabei versuchen sie herauszufinden, wie diese Akteure die verschiedenen Vorschläge für eine Verbesserung bzw. für eine Verfestigung der Rolle des Internet Governance Forums beurteilen. Ich sehe in diesem globalen Bürgerinnen-Dialog ein besonders effektives Mittel zur Entfaltung von deliberativen Demokratiepotentialen. Ich sehe darin ein sehr positives Zeichen, und ich denke, eine solche Befragung könnte man in anderen Internet-bezogenen Menschenrechtskontexten – zum Beispiel bei der Ausarbeitung neuer Gesetze – auf jeden Fall auch durchführen. Es wäre zum Beispiel daran zu denken, bei manchen Gesetzen, wie einem Netzwerkdurchsetzungs-Gesetz, einmal eine globale Bürgerinnen-Befragung durchzuführen, weil der Impact dieses Gesetzes – das hat auch eine andere Kollegin hier schon gezeigt – weit über die Grenzen Deutschlands hinaus zu spüren war. Vielen Dank.

Die **Vorsitzende**: Herzlichen Dank, Herr Dr. Kettemann. Dann hat als Nächste Frau Dr. Shi-Kupfer bis zu vier Minuten das Wort.

SVe Dr. **Kristin Shi-Kupfer**: Ja, ganz herzlichen Dank für die Frage. Mit den Ergebnissen und den regionalen und internationalen Gegenreaktionen sprechen Sie ein sehr wichtiges Thema an. Man sieht das aktuell besonders deutlich am Beispiel Hongkongs und Taiwans. Ich möchte die Frage mit einem Blick nach vorn beantworten. Ich denke, in Hongkong könnte die chinesische Regierung durch Störung und Infiltration von digitalen Netzwerken und Plattformen die Kommunikations- und damit auch die Organisationsfähigkeit der demokratischen Gruppierungen und der Protestbewegung noch viel stärker einschränken. Je nach Auslegung und Umsetzung des geplanten nationalen Sicherheitsgesetzes könnte die chinesische Regierung auch versuchen, die gesamte ihr suspekt oder gefährlich erscheinende digitale Kommunikation im Interesse der nationalen Sicherheit zu kriminalisieren. In Bezug auf Taiwan ist zu erwarten, dass die chinesische Regierung ihre Desinformationsstrategie, die sie bereits im Vorfeld der taiwanesischen Wahlen verfolgt hat, noch intensiviert und zugleich versuchen wird, durch die gezielte Lancierung von Falschinformationen die internationale Reputation Taiwans weiter zu schädigen. Ähnliche Mechanismen sind auch in Australien zu beobachten. Dort kam das gesamte Spektrum von Instrumenten der Einflussnahme zur Geltung; das heißt, neben der politischen auch die wirtschaftliche Einflussnahme; und dafür dienen digitale Technologien gerade auch im öffentlichen Raum letztlich als Träger. In Osteuropa, Südosteuropa und Afrika ist es ähnlich. Hier geht von dem Ausbau der digitalen Infrastruktur und damit dem Import des digitalen Labors, das Sie gerade sehr gut beschrieben haben, eine große Bedrohung aus, weil sie den Zugriff auf sensible Daten ermöglicht. Den chinesischen Unternehmen wird deutlich gemacht, dass sie in einem Rechtsraum agieren, in dem die chinesische Kommunistische Partei sie zwingen kann, Daten herauszugeben, die die Partei als wichtig für die nationale Sicherheit oder als anderweitig relevant erachtet. Daher halte ich den Ausbau und auch den Aufbau von digitaler Infrastruktur in Europa durch chinesische Unternehmen unter Datenschutzaspekten für nicht angemessen. Ganz herzlichen Dank.

Die **Vorsitzende**: Herzlichen Dank. Dann gehen wir weiter in der Runde. Herr Braun hat das Wort für die AfD-Fraktion. Zwei Minuten.

Abg. **Jürgen Braun** (AfD): Danke schön, Frau Vorsitzende. Liebe Kollegen, meine sehr verehrten Damen und Herren, zunächst einmal vielen Dank an die Experten, die wir eingeladen haben. Es war schon erkennbar, dass hier eine hohe Kompetenz vertreten ist. Dafür noch einmal vielen Dank. Ich finde es sehr bemerkenswert, was Frau Kurz über die positiven Seiten des Darknet gesagt hat, die man wohl zur Kenntnis nehmen muss, weil das Darknet eben auch Chancen für die Menschenrechte eröffnet und Bürgern die Möglichkeit gibt, sich zu entfalten – gerade auch in kritischen Situationen. Bemerkenswert ist auch die schriftliche Äußerung von Frau Nighat Dad zur Auswirkung des deutschen Netwerkdurchsetzungs-Gesetzes auf die Regierungen in Südostasien, die sich offenbar durch dieses sehr problematische – um nicht zu sagen eindeutig negative – Gesetz ermuntert gefühlt haben, die digitale Freiheit ihrer Bürger einzuschränken. Herr Rechtsanwalt Steinhöfel, Sie sind international bekannt als Experte auf diesem Gebiet, und sie haben auch die Aufmerksamkeit der Öffentlichkeit auf sich gezogen, insbesondere durch Ihre Auseinandersetzung mit Facebook und anderen Internet-Giganten. Wie beurteilen Sie die Auswirkung des Netzwerkdurchsetzungs-Gesetzes – das ist meine erste Frage – auf die Meinungsfreiheit? Meine zweite Frage betrifft die immer wieder sehr beliebten Begriffe Hass und Hetze, die seltsamerweise immer gemeinsam benutzt werden; Begriffe, die in der Vergangenheit von ganz anderen Regimen verwendet wurden, die mit Demokratie nichts am Hut hatten. Welche historischen Zusammenhänge sehen Sie bei den permanent benutzten Begriffen Hass und Hetze? Und welche Probleme sehen Sie bei der Verwendung des Begriffs Hassrede in rechtsstaatlichen Normen und für die Meinungsfreiheit?

Die **Vorsitzende**: Herzlichen Dank, Herr Braun. Herr Steinhöfel, Sie haben vier Minuten Zeit.

SV **Joachim Nikolaus Steinhöfel**: Das Netzwerkdurchsetzungs-Gesetz war ja von Anfang an einer vehementen verfassungsrechtlichen Kritik ausgesetzt. Ich war als Zuschauer bei einer öffentlichen Anhörung des Rechtsausschusses des Bundestages im Jahr 2017 und habe zugehört und mitgeschrieben. Da werden ja – Sie wissen das – Sachverständige von allen Parteien benannt – es waren sieben oder acht, das weiß ich nicht mehr so genau. Sie wurden gefragt, wie sie das Gesetz verfassungsrechtlich beurteilen. Alle, die gefragt wurden – bis auf den Kollegen vom Jugendschutz, der kein Verfassungsrechtler ist und der sich etwas bedeckt gehalten hat –, haben sich klipp und klar geäußert. Das gilt auch für sämtliche Oppositionsfraktionen im Deutschen Bundestag. Es besteht hier eine unglaublich weitgehende Übereinstimmung – manchmal sind die Beschlusslagen fast wortgleich – in der Ablehnung dieses Gesetzes. Jetzt ist fast schon eine Minute um, ich muss mich etwas sputen. David Kay, der Meinungsfreiheitsbeauftragte der UN, hat schon 2017 an die Bundesregierung geschrieben und sie daran erinnert, dass Zensurmaßnahmen nicht an private Rechtsträger delegiert werden dürfen. Das Hauptproblem des Gesetzes – das übrigens zur Folge hat, dass Artikel aus dem Postillion und Smileys und Gemälde von Bruegel dem Älteren gelöscht werden – ist die drohende Geldstrafe von bis zu 50 Millionen Euro. Das ist das Zweihundertfache dessen, was bei einem maximalen Verstoß gegen eine einstweilige Verfügung als Strafe verhängt werden kann. Das heißt, wenn die Bild-Zeitung auf der Titelseite das Schlimmste tut, was man überhaupt bei einem Verstoß gegen ein gerichtliches Verbot tun kann, dann drohen ihr 250.000 Euro Geldstrafe. Das Zweihundertfache dessen droht nun den Netzwerken, und zwar auch deren leitendem Personal. Wenn Sie dort leitender Manager sind und müssen an der Grenze der Meinungsfreiheit entscheiden, ob Sie einen Inhalt löschen oder nicht, dann ist die Entscheidung doch völlig klar: Sie löschen. Das Ziel ist völlig legitim, nämlich strafbare Inhalte aus dem Netz zu entfernen. Wer könnte dagegen sein? Jeder ist dafür, dass das, was rechtswidrig ist – und was da teilweise eingestellt wird, ist wirklich widerlich – gelöscht wird. Aber nicht so. Aus meiner Sicht wäre die Lösung – und ich habe damit nun wirklich viel zu tun – ganz einfach, nämlich – und das wurde in einem anderen Kontext schon erwähnt – eine bessere Ausstattung der Justiz für die Strafverfolgung. Der Fall Claudia Roth, bei dem ein Arbeitsloser, der sie beleidigt hat, zu 5.000 Euro Geldstrafe verurteilt wurde, hat dies

schon vor dem Netz-DG deutlich gemacht. Die andere Option wären bessere zivilprozessuale Möglichkeiten für die Nutzer, zum Beispiel ein pauschalierter Schadensersatz für jeden Tag unberechtigter Sperre. Das würde richtig Druck ausüben. Hass und Hate Speech: Ich frage jeden, der diese Begriffe benutzt: Was meinen Sie eigentlich damit? Meinen Sie mit Hass und Hetze das, was strafrechtlich untersagt ist, oder meinen Sie damit auch etwas anderes? Wenn Sie nämlich auch etwas anderes meinen, greift dies unmittelbar in Artikel 5 ein. Und wenn Sie das nicht meinen, warum sprechen Sie dann nicht statt von Hass und Hetze von strafbaren Inhalten. Das Strafgesetzbuch kann man ändern, wenn es Regelungsbedarf gibt. Aber dort ist klar definiert, was alles verboten ist, nämlich Verleumdung, üble Nachrede, Volksverhetzung, Verwendung verfassungsfeindlicher Symbole und so weiter. Darum sollte man diese Begriffe benutzen. Die diffusen, schwammigen Begriffe Hetze und Hass verunsichern den Nutzer, weil er nicht mehr genau weiß, wo die Grenze zwischen strafbarem und legalem Handeln verläuft; und das führt automatisch zu einer Art von Selbstzensur. Denn sehr oft werden zulässige Äußerungen mit diesen Begriffen belegt. Ich will im Folgenden keine Gleichsetzung vornehmen, das möchte ich unterstreichen. Aber wenn wir in die DDR zurückschauen, dann erinnern wir uns daran, dass es dort den Straftatbestand der staatsfeindlichen Hetze gegeben hat, der dafür verwendet wurde, Regimekritiker zu kriminalisieren und sie massenhaft ins Gefängnis zu bringen. Und im Jahr 1934 wurde in dem sogenannten Heimtücke-Gesetz ein noch weit üblerer Gesetzestatbestand verankert: Wer vorsätzlich eine unwahre oder gröblich entstellte … ich sage ja, ich habe zu Beginn ausdrücklich betont – die paar Sekunden müssen Sie mir jetzt zusätzlich zugestehen –, dass ich keinerlei Gleichsetzung dieser Regimes mit unserem freiheitlich-demokratischen Rechtsstaat vornehmen will, sondern nur auf terminologische Ähnlichkeiten hinweisen möchte, die uns zu besonderer Vorsicht mahnen sollten. Das Zivilrecht definiert durch die §§ 823 ff. und das Strafgesetzbuch durch die entsprechenden Strafrechtsvorschriften hinreichend und präzise die Bereiche strafbaren Handelns, die wiederum durch die Rechtsprechung konkretisiert worden sind. Auf diese Bereiche sollten wir uns konzentrieren und die diffusen schwammigen Begriffe, die Gefahren für die Meinungsfreiheit darstellen, möglichst nicht verwenden.

Die **Vorsitzende**: Herzlichen Dank. Dann hat jetzt für die SPD-Fraktion Frank Schwabe das Wort für zwei Minuten.

Abg. **Frank Schwabe** (SPD): Vielen Dank, Frau Vorsitzende. Ich würde meine Fragen gern an Frau Dr. Kurz und an Frau Rohrbach richten. Meine erste Frage bezieht sich auf das Netzwerkdurchsetzungs-Gesetz. Sicherlich ist es nicht unbedenklich, in diesen Bereich einzugreifen. Würden Sie sagen, dass man genau definieren kann, in welchen Fällen das gut ist und Sinn hat und in welchen Fällen es problematisch ist, oder sind Sie der Meinung, dass die Antwort auf diese Frage von den Ländern oder den Regierungen abhängt bzw. davon, ob die Länder autoritär oder nicht autoritär geführt werden. Die Frage ist also, woran man möglicherweise erkennen kann, ob der Eingriff gerechtfertigt oder nicht gerechtfertigt ist? Oder sind Sie der Meinung, dass jedes Gesetz, das reglementiert, schlecht ist? Die Art der Kommunikation ändert sich ja ständig. Wir sprechen hier gerade miteinander über ein bestimmtes Thema, aber im nächsten Moment schon wieder über irgendein anderes. Ist es eigentlich angemessen, dass private Organisationen die moderne Kommunikation organisieren, oder wäre es besser, wenn das staatlich organisiert und reglementiert würde? Im letzten Fall würde eben nicht YouTube oder wer auch immer, sondern irgendeine staatliche Behörde entscheiden, ob etwas gelöscht wird oder nicht. Und zum Thema Darknet: Kann man dafür irgendwelche Regeln finden, die sinnvoll wären? Ich denke, wenn man an bestimmte Länder denkt, da würde es ohne Darknet nicht funktionieren. Das ist wie im realen Leben. Da geht man auch manchmal nachts im Dunkeln raus. Nur wenn man darauf verzichten würden rauszugehen, könnte man verhindern, überfallen zu werden oder umgekehrt selbst jemanden zu überfallen. Dennoch muss es Regeln geben für den Fall, dass man nachts im Dunkeln rausgeht. Also wo könnte das stattfinden? Ich habe noch eine letzte Frage zu den internationalen Konventionen. Im Europarat

wird über bestimmte Konventionen zu diesem Thema diskutiert. Sehen Sie hier Regelungsbedarf?

Die **Vorsitzende**: Herzlichen Dank Herr Schwabe. Dann hat zunächst Frau Dr. Kurz das Wort, und ich habe es so verstanden, dass alle drei Fragen an jeweils die beiden Sachverständigen gerichtet waren. Frau Dr. Kurz, bitte.

SVe Dr. **Constanze Kurz**: Ich beginne mal mit dem Netz-DG. Wir haben in unserer schriftlichen Stellungnahme dazu nichts geschrieben, außer einer Passage, die sich darauf bezieht, dass auf den großen kommerziellen Plattformen – zumindest auf einigen von ihnen – bezahlte Akteure gut dokumentierte Desinformationskampagnen durchgeführt haben, die problematisch für die Meinungsfreiheit sind. Ich gehöre zu denen, die das Gesetz von Anfang an kritisiert haben; aber ich habe mir die Stellungnahmen, obwohl ich keine Juristin bin, damals im Justizausschuss durchgelesen. Ich denke, dass der Anreiz, der von dem Gesetz ausgeht, gegen die Freiheit der Rede vorzugehen, recht groß ist. Aber ich würde erst einmal die Entscheidung, die in Karlsruhe mit Sicherheit gefällt wird, abwarten wollen. Der Vorteil hier in Deutschland ist ja, dass wir solche Entscheidungen herbeiführen können. In manchen Ländern, die sich das Netz-DG zum Vorbild genommen haben, verfügen die davon Betroffenen sicher über weniger Möglichkeiten, sich dagegen juristisch zu wehren. Das ist meines Erachtens das eigentlich Gefährliche an dem Netz-DG. Wir haben damit in manchen Rechtsfragen Neuland betreten, und andere machen das nach. Während wir das hier aber vielleicht irgendwann korrigieren können, ist es anderswo viel schwieriger. Das tieferliegende Problem besteht aus meiner Sicht darin, dass wir uns – auch dieses Haus hier und viele Regierungen – ganz freiwillig in die Abhängigkeit von kommerziellen Werbeplattformen begeben haben. Dass wir unseren gesellschaftlichen Diskurs auf einer – ich will es noch einmal sagen – kommerziellen Werbeplattform führen wollen, halte ich für grundlegend falsch. Aber in diese Abhängigkeit haben wir uns freiwillig begeben. Ich glaube, dass eine Befreiung aus dieser Abhängigkeit sehr lange dauern wird. Aus juristischer Sicht kann ich dazu nichts weiter sagen. Beim Darknet, auf das sich ihre zweite Frage bezieht, handelt es sich um einen Begriff, der ähnlich ungute Assoziationen weckt wie die Begriffe Hassrede oder Hetze. Wenn man den Begriff Darknet verwendet, denkt man nicht an Menschen, die den Schutz der Anonymität brauchen oder die gar keine andere Möglichkeit haben, als ihre Identität zu verbergen, wenn sie kommunizieren wollen. Ein Großteil des Darknet besteht faktisch aus Webseiten; hinzukommen in geringem Umfang noch E-Mails und Chats, aber im Wesentlichen sind es Webseiten. Es gibt also diesen Begriff, der in den Medien im Wesentlichen verwendet wird, wenn es um Plattformen für Betäubungsmittelhandel geht. Aber das ist eben nur ein minimaler Teil. Da die Strafverfolgung hier durchaus eingreift, ist dieser Teil des Darknets sogar kleiner geworden. Die Tatsache, dass Menschen aus dem Darknet Informationen beziehen – zum Beispiel bei der Deutschen Welle, bei der BBC, bei Medienhäusern und vielen internationalen Zeitungen, die diese Informationen dort mittlerweile in Wort, Text und Bild anbieten –, ist sehr viel wichtiger geworden. Man wird aber die Ambivalenz des Darknet letztlich nicht auflösen können. Denn Anonymität kann auch bedeuten, dass Menschen mit kriminellen Absichten diese Technik benutzen. Aber diese Technik bietet sehr viel mehr Chancen, als sie Gefahren birgt. Und die letzte Frage … habe ich noch Zeit? Bei der letzten Frage ging es Ihnen um den Export, richtig?

Abg. **Frank Schwabe** (SPD): Es ging mir um internationale Konventionen und um die Frage, ob Sie denken, dass es einen überstaatlichen Regelungsbedarf geben könnte.

SVe **Dr. Constanze Kurz**: Da die neuen Technologien mittlerweile eine ganze Reihe von Problemen aufgeworfen haben, könnten wir internationale Abkommen gut gebrauchen. Ich erinnere zum Beispiel daran, dass der UN-Menschenrechtsrat, als es nach zwei, drei Jahren Snowden-Diskussion um das Thema der massenhaften Überwachung ging, sich auch schon einmal dazu geäußert hat. Meiner Meinung nach sind solche Konventionen aber nur dann sinnvoll, wenn es sich um ratifizierte Verträge handelt, wie

etwa im Fall der Menschenrechtskonventionen. Wenn man nur Lippenbekenntnisse ablegt oder nicht bindende Erklärungen abgibt, ist das aus heutiger Sicht nicht mehr genug. Ich denke, damit verschließen wir die Augen vor den Realitäten und auch davor, dass wir die Verantwortung tragen. Denn bei uns im Westen befinden sich die Hersteller von Software, und damit können wir auch Regeln setzen und somit mehr tun, als unseren guten Willen in solchen Gremien kund zu tun. Außerdem kann man auch ganz praktisch etwas tun; wir zum Beispiel haben eine ganze Liste erstellt. Außerdem könnten wir den Verkauf von Software, die mit EU-Mitteln gefördert worden ist, an bestimmte Lizenzen binden, zum Beispiel an solche, die Überwachungssysteme ausschließen. Wir könnten auch generell restriktiver umgehen mit dem Export. Ich verweise hier gern noch einmal auf unsere schriftliche Stellungnahme. Wir haben die Möglichkeiten. Ich glaube, Grüß-August-Nachrichten helfen uns da wenig weiter.

Die **Vorsitzende**: Herzlichen Dank. Dann hat jetzt Frau Rohrbach für vier Minuten das Wort.

SVe **Lena Rohrbach**: Vielen Dank. Zu der ersten Frage nach dem Netz-DG und dem Kontext, in dem solche Regelungen in Deutschland und in anderen Ländern stehen: Zunächst einmal muss man, denke ich, anerkennen, dass es eine sehr große Herausforderung darstellt, die Meinungsfreiheit mit den Persönlichkeitsrechten online in die richtige Balance zu bringen, und zwar insbesondere angesichts der Tatsache, wie stark die Debatte von privaten Akteuren wie den großen Plattformen bestimmt wird. In diese Situation hätte man sich niemals bringen dürfen, darin stimme ich Constanze Kurz zu. Aber jetzt stehen wir ihr nun einmal gegenüber. Nach einer Zählung der Vereinten Nationen gibt es insgesamt ungefähr 154 sogenannte Cyber Laws, also Gesetzeswerke, welche Straftatbestände, die mit Äußerungen im Internet zu tun haben, definieren. Diese Gesetze sind natürlich qualitativ unterschiedlich; es sind völlig legitime, aber auch sehr problematische Gesetze dabei. Insofern darf man nicht alle Regelungen über einen Kamm scheren, auch wenn das Netz-DG problematische Nachahmungseffekte gehabt hat, vor denen ja im Vorfeld gewarnt wurde. Diese problematischen Aspekte hätte man sicherlich minimieren können, wenn man der Debatte mehr Raum gegeben und die Warnungen aus der Zivilgesellschaft ernster genommen hätte. Einige positiv zu bewertende Regelungen, die voraussichtlich demnächst implementiert werden – wie zum Beispiel das Wiedervorstellungsverfahren, das einem Betroffenen die Option einräumt, zu Unrecht gelöschte Inhalte wiederherstellen zu lassen –, hätte man dann vielleicht von Anfang an mit aufnehmen können. Dann wäre das gesamte Gesetz von Anfang an schlüssiger gewesen, und auch die Gefahr des Overblockings wäre geringer gewesen; denn es ist immer problematisch, wenn private Akteure – nach denen Sie gefragt hatten – für die Rechtsdurchsetzung in die Pflicht genommen werden. Das birgt nämlich immer die Gefahr, dass legitime Inhalte gelöscht werden. Gleichzeitig halten wir es für eine große Herausforderung, dass allein bei YouTube – ich habe die genauen Zahlen nicht mehr im Kopf – schätzungsweise hunderte von Stunden an Videomaterial pro Minute hochgeladen werden. Natürlich bedeutet dies, dass private Plattformen irgendeine Art von Verpflichtung haben, damit umzugehen. Ich denke, eine wichtige Aufgabe wäre, so genannte menschenrechtliche Sorgfaltspflichten umzusetzen, sich also entlang der UN-Leitlinien für Wirtschaft und Menschenrechte Gedanken darüber machen, welche menschenrechtlichen Herausforderungen mit der eigenen Tätigkeit verbunden sind, sodann Risikoanalysen durchzuführen und entsprechende Gegenmaßnahmen zu ergreifen. Im Übrigen halte ich es nicht für Zufall, dass die Begriffe Hass und Hetze im Internet in der Debatte häufig gemeinsam genannt werden. Denn es gibt ja diesen Begriff des Incitement to Hatred als Bezeichnung dafür, was völkerrechtlich von den Staaten sogar verboten werden sollte. In dieser Debatte liegt der Fokus auf der Frage nach den Verboten. Ich denke aber, dass wir uns stärker auf die positiven oder Komplementärmaßnahmen konzentrieren sollten. So hat Herr Kettemann auf das Beispiel von Behörden verwiesen, die nicht nur im Interesse der Antidiskriminierung tätig werden, sondern auch darin geschult sind, am Tatort Internetstraftaten zu verfolgen, professionell mit Anzeigen umzugehen, und der Diskriminierung vorzubeugen. Ich verweise in

diesem Zusammenhang auch noch auf die Antidiskriminierungsgesetzgebung und die Rassismus-Schulung. Das alles können wir effektiv betreiben, ohne dass wir uns auf die relativ schwierige Frage nach den Löschungen einlassen müssen. Nun möchte ich noch kurz auf die Frage eingehen, ob es ein Kriterium gibt, mit dem sich gute und schlechte Gesetze dieser Art unterscheiden lassen. Meines Erachtens zeichnet sich ein gutes Gesetz dadurch aus, dass es Straftaten klar definiert und sich an dem Grundsatz der Verhältnismäßigkeit orientiert. Für problematische Cyber Crime Laws ist hingegen charakteristisch, dass sie vage formuliert sind und zum Beispiel die Verbreitung von Terrorismus oder von Fake News unter Strafe stellen, ohne genau zu definieren, was das ist. So etwas trägt dann zur Kriminalisierung von legitimen Meinungsäußerungen, etwa von Bloggern, bei. Dieser Einwand gilt allerdings nicht für das deutsche Netz-DG, weil es auf klar definierte Straftaten verweist. Zu der Frage, ob es im Darknet klare Grenzen gibt …

Die **Vorsitzende**: Kommen Sie bitte zum Schluss. Ich muss Sie leider unterbrechen, es sei denn, die Frage kann schnell beantwortet werden. Dann würde ich ein Auge zudrücken.

SVe **Lena Rohrbach**: Es gibt keine klaren Grenzen, jedenfalls nicht, was die Verwendung des TOR-Browsers anbelangt, weil dieser nun einmal zum Guten wie zum Schlechten verwendet werden kann. Das lässt sich nicht unterscheiden. Jedenfalls verwenden auch wir das Darknet für unsere Recherchen.

Die **Vorsitzende**: Herzlichen Dank, Frau Rohrbach. Ich werde wieder ins Englische umschalten. Nighat, ich möchte Ihnen ein paar Fragen zu Pakistan aus dem Kreis der FDP-Fraktion stellen. Wir haben ein wenig darüber gesprochen, wie Regierungen in die Rede- und Meinungsfreiheit eingreifen können. Was ließe sich da tun? Die erste Frage betrifft vielleicht Ihre Arbeit und die dabei gewonnene Erfahrung: Wie wäre es möglich, die digitale Kluft zwischen den Geschlechtern weltweit zu schließen? Sie haben in Ihrer Erklärung die digitale Kluft zwischen den Geschlechtern in Pakistan angesprochen. Könnten Sie uns etwas mehr Einblick in Ihre Arbeit und Ihre bewährten Praktiken geben? Die zweite Frage, und damit können wir gut an die Ausführungen von Frau Rohrbach von eben anknüpfen: Inwieweit könnten oder sollten Regierungen nach Ihrer Ansicht in die Meinungsfreiheit eingreifen, um digitale Räume sicherer zu gestalten und Minderheiten, etwa Frauen, aber auch Menschenrechtsverteidiger und andere Gruppen, vor Diskriminierung und Cyberkriminalität zu schützen? Sehen Sie für den Schutz dieser Minderheiten eine Alternative zu Regulierung und Zensur, etwa die Netz-DG, wie wir sie hier in Deutschland haben, die auch im Menschenrechtsrat von der Volksrepublik China als positives Beispiel erwähnt wurde? Gerade habe ich gelesen, dass Sie erst unlängst in das Aufsichtsgremium berufen wurden, das bei Facebook Online-Inhalte prüft. Vielleicht können Sie Ihre Arbeit dort näher beleuchten? Vielen Dank. Sie haben vier Minuten Zeit, um diese Fragen zu beantworten.

SVe **Nighat Dad**: Vielen Dank. Also, um auf die erste Frage zurückzukommen, bei der es darum ging, die digitale Kluft zwischen den Geschlechtern genauer zu untersuchen: Ich habe das bereits kurz angesprochen, denke jedoch, dass es wichtig ist, die tieferen systemischen Probleme anzugehen, die dieser Kluft zugrunde liegen. Wenn ich mir den pakistanischen Kontext, aber auch den Kontext des Globalen Südens anschaue, reicht es nicht aus, Frauen Mobiltelefone und ähnliche Geräte zu geben und zu erwarten, dass die Kluft überbrückt wird. Wenn nicht am eigentlichen Grund für die Missbilligung in der Familie angesetzt wird, kann die Nutzung von Online-Räumen durch Frauen oft dazu führen, dass ihre Aktivitäten stärker überwacht werden, und jede als Übertretung wahrgenommene Handlung, selbst wenn sie so harmlos ist wie ein Telefonat mit einem Angehörigen des anderen Geschlechts, kann in Pakistan Gewalt und im Extremfall Ehrenmorde zur Folge haben. Bei der Bewältigung dieser Probleme müssen staatliche und gemeindebasierte Lösungen Hand in Hand gehen. Meine Organisation, die Digital-Rights-Foundation, bei der ich seit zehn Jahren tätig bin, arbeitet an Kampagnen, die von den Gemeinschaften getragen werden. Unter anderem

leiten wir die Kampagne Hamara Internet, was so viel heißt wie „Unser Internet“. Dabei besuchen wir Gemeinden, Schulen und Hochschulen im ganzen Land und sensibilisieren für digitale Sicherheit und Instrumente gegen Belästigung. Gleichzeitig haben wir von den Gemeinschaften erfahren, dass wir unter Berücksichtigung des Kontexts von Frauen Strategien bereitstellen, mit denen sie über ihre Freiheiten verhandeln können. Um diese Kluft zu überwinden, sollten daher stärker makroökonomisch orientierte Ansätze durch die Einbeziehung von Frauen in einem Entwicklungskontext und die Erarbeitung spezifischer Programme ergänzt werden. Wichtig ist meiner Ansicht nach auch, dass wir uns mit dieser digitalen Kluft zwischen den Geschlechtern nicht nur auf nationaler Ebene befassen, sondern auch betrachten, wie Unternehmen im Bereich der sozialen Medien diese Frage vor dem Hintergrund unterschiedlicher Gegebenheiten und Gesellschaften angehen. Meistens nämlich werden die Instrumente, etwa für die digitale Sicherheit, im Globalen Norden und in der Annahme erstellt, dass sie in aller Welt genutzt werden, ohne dass die Bedürfnisse und Anforderungen der Gemeinschaften in einem bestimmten lokalen Umfeld überhaupt bekannt sind. Bei ihrer zweiten Frage ging es darum, inwieweit Regierungen in die Meinungsfreiheit eingreifen sollten, um digitale Räume sicherer zu gestalten und Minderheiten zu schützen. Für mich besteht der derzeitige Ansatz der Regierungen darin, Gesetze zu Straftaten wie Online-Belästigung und Hassreden zu erlassen. In unserem eigenen Kontext habe ich beobachtet, dass diese Gesetze im Namen des Schutzes von Frauen und Mädchen angenommen werden. Diese Gesetze zur Cyberkriminalität sind wirklich sehr drakonisch und oft Bestandteil eines größeren Pakets, das die staatlichen Befugnisse so bündelt, dass sie regulierend und sanktionierend in die Meinungsfreiheit eingreifen. Gruppen in aller Welt, die für digitale Rechte eintreten, sehen diese Gesetze seit Langem als ein zweischneidiges Schwert an, und häufig enthalten die Gesetze nur geringe zusätzliche Schutzvorkehrungen für Frauen sowie sexuelle und religiöse Minderheiten, selbst wenn es um ihre Umsetzung geht. Wenn diese Gesetze im Namen des Schutzes dieser Minderheiten erlassen werden, ist der haft- und strafbewehrte Ansatz für den Umgang mit einigen der genannten Probleme oft unzulänglich, da viele Frauen das Strafjustizsystem dort, wo es schwach ausgeprägt ist und der systemischen Natur von so weitverbreiteten Erscheinungen wie Hassreden nicht gerecht wird, nicht in Anspruch nehmen wollen. Meiner Ansicht nach benötigen wir allgemein gehaltene und weit gefasste Rechtsvorschriften zur Regulierung des Internets. Gefragt sind flexiblere und opferorientierte Lösungskonzepte, die bereits im Rechtssystem vorhanden sind, rasch greifen und das Opfer für den verursachten Schaden entschädigen, auch wenn man dabei über das Strafjustizsystem hinausgehen muss. *

Die **Vorsitzende**: Nighat, leider ist Ihre Zeit abgelaufen. Vielleicht können wir uns später noch mit der letzten Frage zur Facebook-Lücke befassen. Leider müssen wir die Zeit wirklich streng einhalten. Ich hoffe, das ist für Sie in Ordnung. Jetzt hat Frau Nastic das Wort für die Fraktion DIE LINKE. Sie haben zwei Minuten Zeit.

Abg. **Zaklin Nastic** (DIE LINKE.): Vielen Dank auch von meiner Seite. Viele von Ihnen sprachen über die Vor-, vor allem aber auch über die Nachteile des digitalen Zeitalters, und sie haben dabei auf die wichtige Rolle von Menschenrechtsverteidigerinnen verwiesen. Zu den bekanntesten Menschenrechtsverteidigerinnen und Whistleblowern unserer Zeit zählen Julian Assange, Chelsea Manning und Edward Snowden. Zwei von ihnen sitzen im Gefängnis und einer lebt im Exil. Es stellt einer Demokratie kein gutes Zeugnis aus, wenn Menschen, die Kriegsverbrechen aufdecken, oder – wie im Falle von Edward Snowden – die Öffentlichkeit über die massenhafte Überwachung von Menschen in der ganzen Welt im Dienste der Geheimdienste informieren, so behandelt werden. Daran zeigt sich, wie wichtig die Rolle von Whistleblowerinnen – auch zur Stärkung der Demokratie – ist. Auch in Deutschland gibt es zahlreiche Whistleblowerinnen und Whistleblower. Im vergangenen Jahr hat die EU eine Richtlinie zum Umgang mit Whistleblowern geschaffen. Diese Richtlinie, die an das EU-Recht gekoppelt wird, überlässt es den einzelnen

Mitgliedstaaten, ob sie Verstöße im nationalen Kontext melden oder nicht. Nun verfolgen Herr Altmaier und das Wirtschaftsministerium das Ziel, dass diese Richtlinie nur auf EU-Ebene, aber nicht auf Bundesebene angewendet wird. Meine Fragen richten sich an Frau Rahmann und Frau Kurz. Reicht nach ihrer Einschätzung der Schutz von Menschenrechtsverteidigerinnen, also von Whistleblowerinnen, im digitalen Bereich in Deutschland aus? Wie verhält sich die deutsche Rechtslage zur Rechtslage in anderen Staaten? Könnte man sich an anderen Staaten, die ein positives Beispiel abgeben, orientieren? Und welche Schritte sollte der Gesetzgeber in Deutschland unternehmen, um Whistleblowern den bestmöglichen Schutz zu gewähren? Vielen Dank.

Die **Vorsitzende**: Herzlichen Dank, Frau Nastic. Dann würde ich zuerst Frau Rahmann für vier Minuten das Wort geben, und dann Frau Dr. Kurz.

SVe **Zara Rahmann**: Vielen Dank für die Frage. Zunächst muss man sagen, dass das, was Chelsea Manning zugestoßen ist, ganz schrecklich ist. Ich glaube, es zeigt, dass der Schutz von Whistleblowern in vielen Ländern nicht ausreicht. Meiner Meinung nach ist der Schutz von Whistleblowern auch hier in Deutschland nicht ausreichend. Aber, wie bereits gesagt, haben wir jetzt die Möglichkeit, das durch die Verabschiedung der neuen EU-Whistleblower-Richtlinie zu ändern. Die EU-Richtlinie verfolgt ehrenwerte Ziele, zum Beispiel den Schutz der Whistleblower vor Kündigung, Degradierung, Mobbing und anderen Formen von schlechter Behandlung. Die Verabschiedung der Richtlinie ist ein wichtiger Schritt, er bezieht sich aber nur auf Verstöße gegen EU-Recht und nicht auf Verstöße gegen nationales Recht. Ich würde es daher begrüßen, wenn Deutschland die Richtlinie übernehmen und auch auf Verstöße gegen Bundesrecht anwenden würde. Andernfalls würde der Schutz von Whistleblowern in Deutschland weit hinter das Schutzniveau in anderen EU-Ländern zurückfallen, die sich freiwillig entschieden haben, die Richtlinie in nationales Recht zu übernehmen. Ich finde es außerdem wichtig, daran zu arbeiten, dass die Richtlinie, sobald sie adaptiert ist, auch durchgesetzt wird. Man kann schon bei den internationalen Organisationen, zum Beispiel bei den Vereinten Nationen, erkennen, dass die Durchsetzung manchmal Probleme bereitet. Das System der Vereinten Nationen trägt in seiner derzeitigen Form wenig zum Schutz von Whistleblowern bei, weil dort viele Menschen nur als Auftragnehmer arbeiten. Das Problem hat also weniger mit der Richtlinie als solcher, als vielmehr mit der Naivität im Hinblick auf deren Durchsetzung zu tun. Ich denke, es kommt auf beides an, auf die Richtlinie ebenso wie auf die Durchsetzung. Beides ist wichtig und könnte stark verbessert werden, auch in Deutschland.

Die **Vorsitzende**: Herzlichen Dank. Dann hat Frau Dr. Kurz das Wort, für vier Minuten.

SVe Dr. **Constanze Kurz**: Auch ich möchte mich für die Frage bedanken. Ich kann die Frage sicherlich nicht vollumfänglich juristisch beantworten, aber ich will es aus einer Perspektive versuchen, die mir enorm wichtig erscheint – auch vor dem Hintergrund all dessen, was heute bereits gesagt wurde. Die Whistleblower – gerade die prominenten Fälle, die Sie erwähnten – haben im Wesentlichen Techniken angewandt, die wir hier im Westen entwickeln. Ich empfehle jedem das aktuelle Buch von Barton Gellman, der für die Washington Post schreibt und der jahrelang aus den Papieren von Snowden veröffentlicht hat. Es ist bemerkenswert, mit welcher technischen Expertise er zu Werke gehen musste, um im Westen eine Publikation über diese Veröffentlichungen herausbringen zu können. Er beschreibt im Detail, welche Techniken er dabei benutzt hat. Diese Techniken und insbesondere die Infrastruktur für die Anonymisierung- und Verschlüsselungstechniken werden hier bei uns entwickelt. Wenn wir beschließen sollten, diese Technik zu durchlöchern, dann nehmen wir künftigen Whistleblowern die Möglichkeit zu veröffentlichen. Daher kann ich nur jedem empfehlen, dieses Buch zu lesen. Sie haben WikiLeaks angesprochen. Ich möchte hier darauf verweisen, dass sich – unabhängig davon, was Sie heute von dem inhaftierten Julian Assange denken – ein großer Teil der Publikation von WikiLeaks auf Asien und vor allem auf Afrika bezogen hat.

Dazu wurden viele Dokumente von internationalen Whistleblower veröffentlicht, bevor es zu dem langen Streit über das Colateral Murder-Video kam. WikiLeaks hat eine sehr viel größere Spannweite an Informationen veröffentlicht, als es während dieses Streits den Anschein hatte. Ich denke, dass wir in Deutschland, aber auch in der EU ein starkes Augenmerk auf diese umstrittene Verhandlung in Großbritannien werfen sollten. Im Übrigen hat sich der Bundestag in Bezug auf den Whistleblower des Jahrzehnts, als den man Edward Snowden wohl bezeichnen kann, nicht mit Ruhm bekleckert, da sich der Bundestag nicht einmal entschließen konnte, ihn im Rahmen des NSA-BND-Untersuchungsausschusses anzuhören. Es ist also schon formal bzw. juristisch Einiges nachzuholen in Bezug auf die Richtlinie, die gerade erwähnt wurde. Vor allem aber gilt es, darauf zu achten, diesen Menschen weiterhin die nötigen technischen Mittel zur Verfügung zu stellen, damit sie die Informationen, die sie aus Gewissensgründen veröffentlichen wollen, auch weiterhin an die Öffentlichkeit bringen können. Insofern schließe ich mich den Forderungen des deutschen Whistleblower-Netzwerkes in Bezug auf die EU-Richtlinie an. Vielleicht zum Abschluss noch: Die angesprochenen Fälle haben in der Mehrzahl einen politischen Hintergrund und erregen große öffentliche Aufmerksamkeit. In vielen, auch repressiven Regimen ist Whistleblowing nicht mit solchen großen international bekannten Fällen verbunden, und es ist daher viel schwerer, die Öffentlichkeit zu erreichen – etwa, wenn es um Informationen geht, die sich gegen Arbeitgeber oder Behörden im eigenen Lande richten. Ich will daran erinnern, dass es oft nicht um Prominente geht, die aufgrund ihrer Bekanntheit halbwegs durch die Öffentlichkeit geschützt sind, sondern meistens um kleinere Fälle.

Die **Vorsitzende**: Herzlichen Dank, Frau Dr. Kurz. Dann hat jetzt Frau Bause für die GRÜNEN das Wort für zwei Minuten.

Abg. **Margarete Bause** (BÜNDNIS 90/DIE GRÜNEN): Dankeschön für Ihre Stellungnahmen. In verschiedenen Stellungnahmen ist auf die Gefährdung durch den Einsatz von Gesichtserkennungssoftware eingegangen worden. Dazu habe ich zunächst zwei Fragen an Lena Rohrbach. Der VN-Sonderberichterstatter für das Recht auf Meinungsfreiheit, David Kaye, hat sich für ein weltweites Moratorium für Überwachungstechnologie ausgesprochen, insbesondere für Gesichtserkennungstechnologie. Halten sie es für wahrscheinlich, dass sich ein solches Moratorium durchsetzen lässt, und was müsste eigentlich in der Zeit dieses Moratoriums getan werden? Meine zweite Frage bezieht sich auf das TOR-Netzwerk, also auf das Darknet. Haben Sie Hinweise auf geheimdienstliche Angriffe auch in Deutschland auf dieses TOR-Netzwerk, und welche Gefahr geht von diesem Netzwerk für die Menschenrechte und die Menschenrechtsverteidigerinnen aus? Diese Frage richtet sich an Frau Dr. Kurz. Vergangene Woche haben Amazon, Microsoft und IBM erklärt, dass sie Gesichtserkennungssoftware so lange nicht mehr an die Polizeibehörden in den USA verkaufen werden, bis ein Regulierungsgesetz vorliegt. Ferner haben sie den Polizeibehörden die Nutzung bereits eingekaufter Software untersagt. Ist die Situation in Deutschland ähnlich, oder halten Sie die hier existierenden Regeln für ausreichend? Meine zweite Frage an Sie lautet wie folgt: In den vergangenen Wochen hat ein weiteres US-Unternehmen Schlagzeilen gemacht, nämlich Clearview, ein Start-up-Unternehmen, das drei Milliarden Portraitfotos gesammelt und den Strafverfolgungsbehörden zur Verfügung gestellt hat. Es ermöglicht seinen Kunden mittels Fotos einer Person alle anderen im Internet verfügbaren Fotos dieser Person zu finden. Welche Gefahren ergeben sich aus Ihrer Sicht aus diesem Geschäftsmodell für die Menschenrechtsverteidiger, und können Sie beurteilen, ob die Bereitstellung dieses Angebotes in Deutschland legal wäre?

Die **Vorsitzende**: Herzlichen Dank. Sie haben das Wort, Frau Rohrbach, für vier Minuten.

SVe **Lena Rohrbach**: Wir unterstützen das von Ihnen erwähnte Moratorium von David Kaye, das tatsächlich recht umfassend ist, gemeinsam mit anderen zivilgesellschaftlichen Organisationen. Es handelt sich um ein allgemeines Moratorium für die Anwendung von Überwachungssystemen, den

Handel mit ihnen und auch ihre Entwicklung – und dies mit dem Ziel, wie David Kaye sagen würde, als Menschheit einmal innezuhalten. Ich denke, dieses Moratorium ist etwas, das wir unterstützen sollten. Ob ein solches generelles Moratorium kommen wird – da bin ich eher skeptisch. Das hält uns aber nicht davon ab zu sagen, dass es auf jeden Fall sinnvoll wäre. In der Zwischenzeit muss man eben schauen, was man tun kann. Da wäre zum einen das von mir schon erwähnte Verbot von Überwachungstechnologie, die offensichtlich immer unverhältnismäßig und deswegen auch immer menschenrechtswidrig ist, wie zum Beispiel die anlasslose automatisierte Gesichtserkennung im öffentlichen Raum. Für andere Fälle, die verhältnismäßig sein könnten, müsste man dann angemessene Regeln schaffen. Im Übrigen dürften anlasslose Technologien zur Identifizierung auch nicht exportiert werden, da es unseres Erachtens keine legitimen Anwendungsfälle im öffentlichen Raum gibt. In Bezug auf alle anderen Arten von Überwachungstechnologie sollte sich die Bundesregierung dringend für eine effektive Kontrolle des Exports aus der Europäischen Union einsetzen. Eine Reform ist unbedingt notwendig – unter anderem deshalb, weil die Überwachungstechnologie, wie etwa die Gesichtserkennung, von den gelten Regelungen gar nicht erfasst wird bzw. viel zu langsam wirkt. Es dauert regelmäßig mehrere Jahre, bis neue Technologien auf die Liste für die Exportkontrolle gesetzt werden. Der Innovationszyklus im technischen Bereich ist natürlich viel schneller. In der Zwischenzeit, bis zu einer Neuregelung, können die Technologien, die weiterhin exportiert werden, schon viel Schaden angerichtet haben. Wir haben dazu sechs konkrete Vorschläge. Erstens muss Europa umfassend definieren, was überhaupt der Exportkontrolle unterworfen werden soll, damit zum Beispiel Gesichtserkennung oder Systeme zur Vorratsdatenspeicherung mit erfasst sind. Ferner bedarf es der Einführung von menschenrechtlichen Sorgfaltspflichten für die exportierenden Unternehmen. Sie sollen dazu verpflichtet werden, in Form einer Eigenanalyse zu prüfen, ob ein von ihnen exportiertes System in dem importierenden Land dazu verwendet werden könnte, Menschenrechtsverletzungen zu begehen. Umgekehrt könnten sich diese Unternehmen auch entlasten, wenn sie eine solche Prüfung vorgenommen haben und es dann zu Menschenrechtsverletzungen kommt, die nicht vorhersehbar waren. Dies erfordert schnelle und effektive Verfahren, die es ermöglichen, neue Technologien der Exportkontrolle zu unterwerfen, also in den Anhang der Dual Use-Verordnung aufzunehmen. Eine Möglichkeit dafür wäre die so genannte EU-autonome Liste, aber die Regierungen könnten sich auch was anderes einfallen lassen. Ferner bedarf es einer so genannten Catch all-Klausel, also eines Verfahrens, um den Export von Gütern auch dann zu verbieten, wenn sie nicht von der bestehenden Kontrollliste erfasst werden, aber ein Risiko für die Menschenrechte darstellen. Wir brauchen auch mehr Transparenz in Bezug darauf, welche Exporte genehmigt und welche nicht genehmigt worden sind. Zudem müssten Menschenrechtsaspekte ein entscheidendes normatives Kriterium bei der Exportregulierung sein. Das heißt, einfach gesagt, Staaten dürften keine Genehmigungen erteilen, wenn ein signifikantes Risiko besteht, dass der Export zu Menschenrechtsverletzungen beitragen würde. Analog fordern wir so etwas zum Beispiel auch für die Kontrolle des Exports von konventionellen Waffen. Zu etwaigen geheimdienstlichen Angriffen auf TOR-Netzwerke in Deutschland liegen Amnesty keine Informationen vor. Ich erinnere mich aber an geleakte Dokumente, in denen behauptet worden ist, dass der BND ein System zur Überwachung des TOR-Netzwerkes entwickelt hätte. Diese Behauptung konnten wir mit unseren Mitteln nicht überprüfen. Ich erinnere mich ferner daran, dass es für manche Geheimdienste, beispielsweise für die NSA, ausreicht, einen TOR-Knoten zu betreiben, um in die Kategorie der überwachungswürdigen Personen eingeordnet zu werden. Wie der BND das handhabt, weiß ich nicht. Das ist natürlich problematisch, weil auch die Organisation Reporter ohne Grenzen einen TOR-Knoten betreibt, was an sich menschenrechtlich unproblematisch bzw. sogar förderlich ist.

Die **Vorsitzende**: Herzlichen Dank. Das war eine Punktlandung, die Zeit hat genau gereicht. Dann hat jetzt Frau Dr. Kurz für vier Minuten das Wort.

SVe Dr. **Constanze Kurz**: Soll ich zu der gerade beantworteten Frage nach den Eingriffen von Militärs und Geheimdiensten in das TOR-Netzwerk noch etwas sagen, auch wenn ich nicht persönlich gefragt wurde? Dann verweise ich auf unsere schriftliche Stellungnahme, denn das TOR-Project betreibt ein eigenes Safety Board, das darüber forscht. Grundsätzlich hat es solche Angriffe gegeben, die sind teilweise belegt, teilweise nur vermutet. Wir haben in den Fußnoten zwei Hinweise dazu gegeben. Dort kann man sich über das Projekt als solches informieren. Im Übrigen will ich etwas zu der Frage nach der Gesichtserkennung sagen. Ich stimme in jedem Punkt mit Frau Rohrbach überein. Wir forschen im CCC seit 15 Jahren zum Thema Gesichtserkennung, und wir treten auch schon lange dafür ein, zu einem Verbot zu kommen, vor allem zu einem Verbot der automatisierten Gesichtserkennung. Aber ich muss die Frage auf ein größeres Feld ausdehnen. Die Gesichtserkennung bildet nur einen Teil in einem größeren Puzzle. Die heute verfügbaren Techniken beziehen sich längst nicht mehr nur auf das Körpermerkmal Gesicht – das sehr einfach zu registrieren ist, weil wir es in der Regel exponieren –, sondern längst auch auf Verhaltensmerkmale. Diese Technik wurde übrigens auch schon getestet, und zwar hier in Berlin im Rahmen des Südkreuz-Projekts. Sie bezieht sich auf biometrische Merkmale wie die Stimme und die Mimik; dabei geht es vor allem darum, wie wir Emotionen ausdrücken und wie man diese automatisiert auswerten kann. Wir sprechen zurzeit zwar nur über automatisierte Gesichtserkennung, aber eigentlich geht es um sehr viel mehr, nämlich um verschiedene Arten der Aufzeichnung von Körpermerkmalen, die in Zukunft möglich sein werden. Auch darüber sollten wir sprechen, wenn wir uns mit der automatisierten Körpermerkmalsauswertung befassen. Wir dürfen vor dieser Realität nicht die Augen verschließen. Die Staaten der Welt sind die Geldgeber für diese biometrischen Systeme, auch Deutschland gehört seit 15 Jahren dazu. Kaum jemand hat zur Kenntnis genommen, was der Bundestag vor wenigen Tagen beschlossen hat, nämlich dass die Zwangsbiometrie eingeführt wird, der zufolge die Gesichtsbilder, die wir abgeben, jetzt überwiegend in den Ämtern aufgenommen werden. Und kaum jemand hat in Deutschland darüber diskutiert, dass es im Jahr 2007 eine Novelle gegeben hat – zu der es auch eine Sachverständigenanhörung gab –, die den automatisierten Zugriff auf die Biometrie-Bilder erlaubt, die in den letzten zehn Jahren entstanden sind. Deutschland und viele andere europäische und nichteuropäische Länder haben sich daran beteiligt; sie sind noch heute die größten Geldgeber und sind auch die wichtigsten Betreiber von Gesichtsdatenbanken. Sie haben außerdem das Unternehmen Clearview erwähnt. Das ist ein kommerzielles Unternehmen, das sich Bilder im Wesentlichen bei Facebook illegal angeeignet hat, und dafür wird es sicherlich eine hohe Strafe erhalten. Ich denke, Clearview wird sein Geschäftsmodell nicht in dieser Form fortführen können. Aber über die wirklich qualitativ guten Bilder verfügen die staatlichen Datenbanken rund um die Welt, die sich mit jedem Jahr vergrößern und die wir finanzieren. Ich sehe also Europa in der Verantwortung, sein Handeln in Bezug auf die Körpermerkmalmessung der eigenen Bürger zu verbessern, auch um zum Vorbild für andere Länder zu werden. Wir haben in unserer schriftlichen Stellungnahme ferner ein paar Beispiele dafür aufgeführt, wie die Corona-Pandemie in einigen anderen Ländern zur Ausbreitung der automatisierten Gesichtserkennung geführt hat – übrigens bis hin zur Identifizierung von ethnischen Merkmalen –, und dies ohne jede Diskussion, weil die Angst der Bevölkerung vor dem Virus so groß ist. Wir sehen hier also ein riesiges Problemfeld. Davor sollten sich weder die deutsche Regierung noch andere EU-Länder wegducken – auch in Anbetracht ihrer eigenen Praxis. Ich rede mich schon wieder in Rage.

Die **Vorsitzende**: Sie hätten noch eine halbe Minute gehabt, aber jetzt ist es zu spät. Prima, herzlichen Dank. Das war die erste Runde. Wir können jetzt nahtlos zur zweiten Fraktionsrunde übergehen. Ich schaue einmal zur Union. Frank Heinrich hat das Wort für zwei Minuten, das übliche Prozedere.

Abg. **Frank Heinrich** (Chemnitz) (CDU/CSU): Dankeschön. Ich lerne viel dazu, auch wenn ich nicht sagen würde, dass dieses Thema für mich völliges Neuland ist. Aber ich möchte an zwei von

Ihnen noch einmal Fragen stellen, zum einen an Dr. Kettemann. Sie sagten ganz am Anfang Ihres Statements, dass wir im nächsten halben Jahr gute Chancen haben, politisch Einfluss zu nehmen, weil wir bei den Vereinten Nationen und in der EU jetzt eine stärkere Position haben als sonst. Da stimme ich mit Ihnen überein. Aber was könnte das Ihrer Meinung nach sein? Wenn Sie eine Priorisierung vornehmen könnten, in welcher Reihenfolge würden Sie dann die Themen setzen und an welchen Punkten sollten wir uns mit besonderem Nachdruck engagieren. Dann habe ich noch eine weitere Frage. Herr Schwabe hat – glaube ich – Frau Dr. Kurz die Frage gestellt, ob es sinnvoll wäre, Konventionen zu vereinbaren. Dazu würde ich gern Ihre Meinung hören – insbesondere ob Sie glauben, dass solche Vereinbarungen in diesem Bereich überhaupt greifen würde. Ferner habe ich von einem Geschäftsmodell gehört, eine Art Facebook unabhängig von der Werbewirtschaft auf europäischer oder nationaler Ebene zu etablieren. Es stellt sich die Frage, wie man das finanziert. Was halten Sie davon, und worauf müsste man Wert legen? Dann habe ich noch eine Frage an Frau Dr. Shi-Kupfer. Wir hatten Ihnen in dem schriftlichen Katalog die Frage gestellt, welche Strategie die kommunistische Führung Chinas als digitale Supermacht verfolgt. Ich würde die Frage gern einmal umkehren. Welche Strategie raten Sie uns im Umgang mit China angesichts der starken Position, die das Land auf dem digitalen Weltmarkt nun einmal hat? Wie sollten wir uns dazu stellen bzw. wie sollten wir uns davon abgrenzen? Und wie könnten wir auf China politisch einwirken? Da kommen wir wieder auf diese Konventionen zu sprechen. Hat das Sinn, hören die Chinesen überhaupt auf uns, oder sind sie in diesem Feld bereits so überlegen, dass sie das nicht für nötig halten. Dankeschön.

Die **Vorsitzende**: Herzlichen Dank, Herr Heinrich. Jetzt hat zunächst Herr Dr. Kettemann für vier Minuten das Wort. Dann geht es weiter.

SV Dr. **Matthias C. Kettemann**: Vielen herzlichen Dank Herr Abgeordneter Heinrich für die Fragen. Zu den Prioritäten würde ich Folgendes vorschlagen: Zuallererst würde ich gemeinsam mit dem Wirtschaftsministerium und dem Außenministerium dafür sorgen, dass der Bericht an den UNO-Generalsekretär zur Reform der Internet Governance möglichst viele effektive Vorschläge enthält – insbesondere eine Verstärkung der Beteiligung der Parlamente. Beim letzten Internet Governance Forum in Berlin gab es zum ersten Mal einen Parlamentarier-Track, bei dem Mitglieder auch dieses Hauses mit Mitgliedern des Internet Governance Forums zusammengearbeitet und sich gemeinsam über Modelle Gedanken gemacht haben, welche politischen Weichenstellungen man vornehmen könnte. Das heißt, erste Priorität sollte sein, die Parlamente als Vehikel der demokratischen Legitimation in die globalen Prozesse einzubringen. Dieser Aspekt sollte über das Außen- und das Wirtschaftsministerium noch in den Bericht zur Internet Governance Eingang finden. Zweitens: Im Sicherheitsrat, der wegen der Corona-Pandemie gerade ein bisschen zurückhaltender agiert, sollte ein Mainstreaming der digitalen Rechte durchgeführt werden. In den Menschenrechtsrat in Genf hat Deutschland schon in den letzten Jahren wichtige Vorlagen eingebracht. Man denke nur an die Einbringung der berühmten Resolution zur Privatsphäre im Internet durch Brasilien und Deutschland nach den Snowden-Enthüllungen. Es wäre jetzt an der Zeit, erneut die Initiative zu ergreifen und die Notwendigkeit, die Privatsphäre zu schützen, durch eine neue Resolution zu betonen. Wir brauchen weder eine neue UNO-Konvention zum Internet als solchem noch zu den Menschenrechten im Internet. Es gibt bereits sehr gute Dokumente, sie müssen nur effektiv umgesetzt werden. Mein Vorschlag lautet also, keine neuen Konventionen zu schaffen, sondern die bestehenden umzusetzen – allerdings mit einer Ausnahme: Der Generalsekretär der Vereinten Nationen bereitet zurzeit ein Statement zu Vertrauen und Sicherheit im Internet vor. Dies soll nicht die Rolle bestehender Komitees in der UNO ersetzen, sondern es soll in eine neue Richtung zeigen. Deutschland sollte sich an der Initiative beteiligen und über die UNO-Mission in New York dem Statement für Vertrauen und Sicherheit im Internet Unterstützung gewähren und sich dafür einsetzen, dass den Menschenrechten ein hoher Stellenwert eingeräumt wird. Im Übrigen sehe ich in der Schaffung eines europäischen oder eines

deutschen alternativen sozialen Netzwerks kein erfolgversprechendes Geschäftsmodell. Klüger wäre es, die positiven Aspekte der europäischen und deutschen digitalen Souveränität zu verstärken und zum Beispiel eine bereits erprobte deutsche und europäische Cloud-Infrastruktur auf- bzw. auszubauen. Denn der Versuch eines künstlichen Nachbaus von Facebook wäre ebenso zum Scheitern verurteilt wie die Entwicklung einer europäischen Suchmaschine. Daher sollte man eher auf die bestehenden Modelle einzuwirken versuchen und zugleich kleine kompetitive Start-ups in Deutschland und Europa entschieden unterstützen. Dasselbe gilt für gute Beispiele wie etwa die Hessenbox. Dies waren, glaube ich, die wichtigsten Aspekte. Vielen Dank.

Die **Vorsitzende**: Herzlichen Dank, Herr Dr. Kettemann. Dann geht es weiter, vier Minuten für Frau Dr. Shi-Kupfer.

SVe Dr. **Kristin Shi-Kupfer**: Ganz herzlichen Dank für die Frage. Was können wir tun bzw. hört uns die chinesische Regierung überhaupt noch zu? Damit möchte ich anfangen. Ich glaube, die Kommunikationsstrategie ist hier ein ganz wichtiges Stichwort; das klingt zwar schwammig, ist es aber nicht. Ich denke, da können wir ganz viel tun, und da ist auch schon viel passiert, vor allem auf politischer Ebene. Man sollte nicht wie ein Kaninchen auf die Schlange starren und China blinde Bewunderung für seine grandiosen digitalen Technologien entgegenbringen, bei denen die Chinesen uns meilenweit voraus sind. Im Grunde sind wir in Europa zwischen China und den USA eingeklemmt. Sicher müssen wir hier einiges nachholen; aber ich glaube, wir müssen auch wegkommen von dieser Schockstarre bzw. einer blinden Zuversicht, dass der Technologieeinsatz in China alle Probleme löst. Dies gilt es auch im Austausch insbesondere mit dem offiziellen China klarzumachen. Ein zweiter Aspekt, der kommunikationsstrategisch von Bedeutung ist, besteht darin, zur Kenntnis zu nehmen, dass es trotz Zensur auch in China kontroverse Debatten über Privatheit und Datenschutz gibt. Das ist ein Punkt, an den man gerade bei offiziellen Gesprächen anknüpfen kann, indem man darauf verweist, dass auch Chinas Bürgern der Schutz ihrer privaten Daten nicht einerlei ist. Gerade im Zusammenhang mit der Covid-19-Pandemie ist diese Debatte in China wieder hochgekocht. Ich denke, von diesem Argument sollte man sehr viel stärker Gebrauch machen – auch als Entgegnung auf den Einwand aus Peking, das seien ja „westliche“ Prinzipien, auf denen man da beharre. Ein zweiter Aspekt ist die Frage der Reziprozität im Hinblick auf Zugang und politische Teilhabe. Chinesische Akteure können die volle Bandbreite unseres öffentlichen Raumes und unserer öffentlichen Meinung nutzen. Selbstverständlich können sie das tun, solange sie keine strafrechtlichen Normen verletzen. Aber man sollte die chinesische Seite auch darauf hinweisen und das auch immer wieder ansprechen, dass unsere Akteure dies im chinesischen Raum eben nicht dürfen, dass wir nicht die entsprechenden Möglichkeiten haben, mit der chinesischen Gesellschaft zu kommunizieren und ins Gespräch zu kommen. Und nun ein letzter Punkt, der nach wie vor sehr wichtig ist und über den auch diskutiert wird: Aus meiner Sicht sollten wir in Europa von einem Ausbau der digitalen Infrastruktur mit Hilfe chinesischer Unternehmen nach wie vor Abstand nehmen, und zwar nicht primär wegen der technischen Aspekte – wenngleich das sicherlich auch ein relevanter Bereich ist –, sondern vor allem wegen der politischen und rechtlichen Rahmenbedingungen und wegen des politischen Drucks, der auf die chinesischen Unternehmen ausgeübt wird. Ich denke, es ist ganz wichtig, hier weiterhin ganz klar zu bleiben und – das ist ja auch schon angesprochen worden – auf europäische Lösungen zu setzen bzw. in diesen Fragen stärker mit Partnern aus liberalen Demokratien zusammenzuarbeiten. Außerdem sollte man Taiwan generell stärker in den Blick nehmen und zum Beispiel würdigen, was dieses Land im Zusammenhang mit der Covid-19-Pandemie geleistet hat; auch weil dies unterstreicht, dass digitale Technologien auch in einer offenen und transparenten Kommunikationsgesellschaft wirkungsvoll eingesetzt werden können. Dankeschön.

Die **Vorsitzende**: Herzlichen Dank. Dann hat jetzt für die AfD-Fraktion Herr Braun das Wort. Zwei Minuten.

Abg. **Jürgen Braun** (AfD): Vielen Dank, Frau Vorsitzende. Ich habe zwei Fragen, die ich an Herrn Steinhöfel richten möchte. Der erste Punkt ist, welche technisch implementierten Eingriffe in die Meinungsfreiheit es bei den sozialen Medien gibt. Was ist da zum Beispiel automatisiert bzw. was ist rein technischer Art. Zweiter Punkt: Es hat allgemeines Aufsehen, auch in Deutschland, erregt, dass Donald Trump am 28. Mai 2020 eine Durchführungsanordnung erlassen hat, die Zensur im Internet – genauer: in den sozialen Medien – verhindern soll. Das ist insofern ein spannendes Thema, als Amerika der Hauptsitz dieser sozialen Medien ist, die quasi eine Monopolstellung besitzen. Hier geht es darum, ob Meinungen falsch oder richtig bewertet werden. Twitter hat – das ist ein entscheidender Hintergrund dabei – die Chinesin Pfeifer-Li in den Bord of Directors übernommen. Diese Dame war vorher in China für Google tätig und hat sich der Kommunistischen Partei Chinas mit einer regimekonformen Version für Google in China angedient. Das heißt, Twitter ist auf einem Weg, der gerade nicht in Richtung Demokratie, sondern in Richtung Unterdrückung der Meinungsfreiheit führt. Daher habe ich an Sie die Frage, wie Sie das so genannte „Fakten checken“ oder „Fakten finden“, das zurzeit stark in Mode ist, bewerten, und das beinhaltet, dass Leute, die oft gar keine Ahnung von dem jeweiligen Gebiet haben, behaupten, sie könnten beurteilen, was richtig und was falsch ist.

Die **Vorsitzende**: Herr Steinhöfel, Sie haben das Wort für vier Minuten.

SV **Joachim Nikolaus Steinhöfel**: Ich habe Gott sei Dank eine Stoppuhr dabei, denn das ist viel. Ich fange mal mit Donald Trump an. Was da geschehen ist, hat viel Applaus gefunden, nämlich dass ein Fakten-Check bei Twitter erstmals durchgeführt wurde, als es um einem Post von Donald Trump ging. Dagegen ist grundsätzlich nichts einzuwenden. Nur besteht in den USA das rechtliche Problem, dass die Netzwerke keine Publisher im Sinne der New York Times oder der Washington Post sind. Wenn die großen sozialen Netzwerke damit anfangen, redaktionell zu arbeiten, dann verlieren sie ein Haftungsprivileg, und dann ist praktisch ihre gesamte Existenz in den USA gefährdet. Mark Zuckerberg hat noch am selben Tag oder innerhalb von 24 Stunden klipp und klar gesagt, dass die Netzwerke nicht diejenigen sein sollten, die zwischen richtig und falsch unterscheiden. Was wir in Deutschland tun können, nämlich als Bürger bzw. als Nutzer Klage einreichen, ist in den USA nicht möglich, weil die Rechtsprechung dort die Ansicht vertritt, dass es sich bei den Netzwerken um Non-governmental Actors handelt und dass gemäß dem 1. Zusatzartikel zur Verfassung der Vereinigten Staaten von Amerika (First Amendment) die Meinungsfreiheit in den USA nicht von Bürgern geltend gemacht werden kann. Section 230 – das ist die einschlägige Regelung – besagt Folgendes: Wenn Twitter Fakten-Checks durchführt, dann ist das Unternehmen ein Publisher und verliert das Haftungsprivileg. Deswegen wird das wahrscheinlich nicht realisiert werden können. Der zweite Aspekt ist: Wenn sie den Fakten-Check bei einer Nachricht von Trump durchführen – wogegen ich nichts einzuwenden habe –, dann sollten sie es auch bei Chamenei tun, wenn der dazu aufruft, Israel dem Erdboden gleich zu machen. Wenn Fakten-Check, dann bitte in allen Fällen, auch bei der chinesischen KP und so weiter und nicht nur bei Donald Trump, weil Twitter den nun einmal nicht mag. Das wäre nämlich eine Diskriminierung, und die ist nicht zulässig; also entweder alle oder keiner. Automatisches Löschen: Ich habe mich gefragt, ob ich weinen oder lachen soll, als ich erfahren habe, dass Facebook jemanden 30 Tage lang gesperrt hat, weil er ein Smiley gepostet hat oder ein Gemälde von Bruegel dem Älteren, den „Bauerntanz“ – ein Gemälde, das in Wien im Museum hängt und auf dem nicht einmal ein nacktes Bein zu sehen ist – oder vielleicht doch gerade eben so. Wenn ein menschliches Wesen eine solche Sperrung vornimmt, wird man die Hände über den Kopf zusammenschlagen, aber wenn das von künstlicher Intelligenz gemacht wird, dann zeigt sich, dass das überhaupt nicht funktionieren kann. Wie ich eingangs schon kurz erwähnt hatte, ist im Rahmen von Gerichtsverfahren nachgewiesen worden, dass beispielsweise Links zur Zeitschrift Fokus automatisiert gelöscht worden sind und dass bei YouTube – aufgrund bloßer Denunziation und ohne Prüfung des Inhalts – Löschungen vorgenommen wurden und der Fehler erst nachträglich korrigiert wurde. Damit macht der

politisch jeweils anders Positionierte von der Möglichkeit Gebrauch, Inhalte aus den Netzwerken zu entfernen, ohne vorher zu prüfen, ob das überhaupt begründet ist. Es ist ein Jahr her, dass ich im Rechtsausschuss davon berichtet habe, dass wir gerade einen Prozess gegen die Fakten-Checker führen. Ein Jahr später lag dann das Urteil des OLG Karlsruhe vor, das – glaube ich – eine Zeitenwende für die Fakten-Checker eingeläutet hat. Grundsätzlich ist der Fakten-Chekck eine wunderbare Idee. Niemand hat ein rechtliches oder sonstiges Interesse daran, unwahre Tatsachen zu publizieren und zu verbreiten; das versteht sich von selbst. Die Frage ist nur, wer in unserer Gesellschaft darüber entscheiden soll, was richtig und was falsch ist. Wenn die Fakten-Checker selbst keinerlei Kontrolle unterliegen, sind sie dafür sicherlich nicht die Richtigen. Das ganze Instrumentarium des Fakten-Checks ist diskreditiert, weil man bislang für den Fall, dass man dagegen vorgehen wollte, faktisch keine strukturierte Widerspruchsmöglichkeit hatte. Die Folgen waren ebenfalls weitreichend – das ist wichtig zu betonen. Denn wenn ein Beitrag getagged wurde, verlor er 80 Prozent seiner Reichweite, und Werbung war auch nicht mehr möglich. Außerdem drohte die Löschung der Inhalte des Profils und damit eine Diskreditierung, weil der Fakten-Checker ja zum Ausdruck gebracht hatte, dass es falsch ist, was man gesagt hatte. Das OLG Karlsruhe hat das für grundsätzlich problematisch erklärt und in seinem Urteil von einer nicht mehr hinzunehmenden Herabsetzung der journalistischen Leistung der Klägerin gesprochen. Dieses Oberlandesgericht ist eines der renommiertesten in Deutschland. Die Zeitenwende, die das Urteil eingeläutet hat, besteht darin, dass jetzt jeder Fakten-Check einer wettbewerbsrechtlichen Kontrolle unterliegt. In dem besagten Fall ging es ganz konkret sogar um die Meinung der Beklagten, was vor dem Hintergrund von Artikel 5 Grundgesetz vollkommen absurd ist. Man kann Tatsachen überprüfen, aber niemals eine Meinung. In diesem Fall wurde eine Meinung durch einen Fakten-Check abgewertet, und damit hat es jetzt ein Ende. Danke.

Die **Vorsitzende**: Vielen Dank. Dann hat Herr Schwabe nun für die SPD-Fraktion das Wort für zwei Minuten.

Abg. **Frank Schwabe** (SPD): Vielen Dank, Frau Vorsitzende. Ich möchte noch einmal Frau Dr. Kurz und Frau Rohrbach befragen. Ganz kurz: Das Thema Schutz von Whistleblowern ist schon angesprochen worden. Welchen Regulierungsbedarf sehen Sie da eigentlich? Was müsste man tun? Auch da möchte ich wieder wissen, was auf internationaler Ebene nötig wäre. Es gibt ja durchaus die eine oder andere Bestimmung dazu, etwa beim Europarat. Welche gesetzliche Regelung zum Schutz von Whistleblowern brauchen wir, und wie müssen wir da im Bundestag agieren? Auch die Themen Gesichtserkennung, Spionagesoftware und andere sind schon vielfach angesprochen worden. Ich überlege die ganze Zeit, wie man die möglichen Anwendungen voneinander abgrenzen und dann auch organisieren kann. Wenn man zum Beispiel ein Haus baut, dann könnte man es schon heute mit einem System zur Gesichtserkennung bzw. so ausstatten, dass es einen an den Augen oder am Gang erkennt und sich dann die Tür öffnet. Natürlich kann man eine solche Technik für alles Mögliche verwenden – für gute wie für weniger gute Zwecke. Wo liegt eigentlich die Grenze zwischen dem einen und dem anderen und wie zieht man die? Wie kann man schon bei der Entwicklung solcher Techniken verhindern, dass sie missbraucht werden. Und könnten Sie uns vielleicht erklären, welche Unternehmen, die im deutschen oder auch im internationalen Kontext agieren, hier besonders wichtig sind und welche Praktiken, etwa beim Export, wir kritisch beleuchten sollten?

Die **Vorsitzende**: Herzlichen Dank. Dann würde ich jetzt mit Frau Dr. Kurz anfangen und dann zu Frau Rohrbach übergeben. Vier Minuten.

SVe Dr. **Constanze Kurz**: Ich fange mal bei der letzten Frage, also bei der Gesichtserkennung, an. Ich denke, der Fall Clearview, über den international viel gesprochen wurde, wäre so in Europa nicht möglich gewesen. Da greifen schon die Regelungen der Datenschutzgrundverordnung. Ich glaube, so ein Geschäftsmodell könnte man hier schlicht nicht aufbauen. Die Nachfrage auf

dem großen Markt, der sich in den letzten ca. 15 Jahren bei den Gesichtserkennungssystemen entwickelt hat und an dem auch europäische Hersteller beteiligt sind, geht zum Großteil von staatlichen Stellen und insbesondere von Flughäfen aus. Hier sind sozusagen die wesentlichen Marktakteure im Bereich Gesichtserkennung zu finden. Da am Anfang die Fehlerquote relativ hoch war, hat sich erst nach einigen Jahren ein profitabler kommerzieller Markt gebildet – allerdings weniger im Bereich Sicherheit als vielmehr im Bereich Convenience. Das erkennen wir heute an unseren Smartphones, wo es nicht primär um Sicherheit, sondern darum geht, dass man sein Handy bequem entsperren kann. Diese beiden Bereiche würde ich schon einmal voneinander unterscheiden. Ob man jemanden im Interesse einer staatlichen Entität in einer Masse von Passanten mit einem bestimmten System identifizieren kann oder ob man auf seinen privaten informationstechnischen Geräten ein Gesichtserkennungssystem installiert hat, das macht qualitativ einen großen Unterschied. Man erkennt ja in dem kommerziellen oder Convenience-Bereich, dass die Firmen, die entsprechende Hardware für Mobiltelefone anbieten, dafür nicht mehr unter dem Gesichtspunkt der Sicherheit, sondern eher unter dem der Bequemlichkeit werben. So würde ich es einmal ausdrücken. Ich habe vorhin so stark betont, dass der Markt für die Gesichtserkennungstechnologie durch die staatliche Nachfrage bestimmt wird, weil verschiedene europäische Staaten, aber mittlerweile auch Staaten in der ganzen Welt so viel Geld in diesen Bereich investieren. Der gesamte Bereich hat sich lange Zeit nicht wirklich entwickeln können, weil die Ergebnisse der Software für automatische Gesichtserkennung verhältnismäßig schlecht waren. Eine Metastudie, in deren Rahmen an die 200 Gesichtserkennungs-Softwaresysteme getestet worden sind, hat ergeben, dass die Resultate immer noch verhältnismäßig schlecht sind. (Auf diese Studie haben wir auch in unserer schriftlichen Stellungnahme hingewiesen.) Vor allem aber macht die Studie auf einen Aspekt aufmerksam, der für die Menschenrechte relevant ist, nämlich auf die diesen Systemen inhärente Diskriminierung. Denn die Gesichtserkennungssysteme wirken für bestimmte Menschengruppen immer diskriminierend. Dies wird bei einer automatisierten Gesichtserkennung insofern zu einem Problem, als manche Menschen dann beispielsweise jeden zweiten Tag herausgefiltert werden, nur weil Sie über einen bestimmten Bahnhof laufen, einer bestimmten Ethnie oder einer bestimmten Altersgruppe angehören. Die Betroffenen erfahren so eine permanente Diskriminierung. Dieser Effekt tritt bei den Tests im Rahmen der besagten Studie, die ein amerikanisches technisches Standardisierungsinstitut durchgeführt hat, leider immer wieder zutage. Das liegt an der Art, wie diese Software heute konzipiert wird. Ich habe aber vorhin schon darauf hingewiesen, dass die Gesichtserkennung nur einen Teil des Problems darstellt, weil künftig auch andere Körpermerkmale erfasst werden können. Es gibt mittlerweile Systeme, die sich nicht nur auf ein biometrisches Körpermerkmal, sondern auf zwei oder mehrere beziehen, oder die weitere Daten, wie etwa von dem Telefon, das man in der Tasche hat, mit auswerten. Wiederum andere Systeme führen nicht nur eine Gesichtserkennung zum Zweck der biometrischen Wiedererkennung und Identifizierung durch, sondern zielen darüber hinaus darauf ab, Emotionen vom Gesicht abzulesen, also zum Beispiel herauszufinden, ob jemand entspannt und fröhlich oder vielleicht nervös und gestresst ist. Solche Formen der Erkennung halte ich für ethisch sehr fragwürdig, sie sind aber mittlerweile technisch machbar. Die Fehlerquote ist zwar immer noch hoch – und daher wird auch viel über die Funktionsfähigkeit dieser Systeme diskutiert –, sie sind aber technisch immerhin so weit ausgereift, dass sie eine Bedrohung für normale Passanten darstellen. Daher würden wir es sehr begrüßen, wenn die EU das Moratorium beschließen bzw. wenn sie auf Initiative Deutschlands ein Verbot der automatisierten massenhaften Gesichtserkennung aussprechen würde. Wie schon von anderen angeregt, würde auch ich mir wünschen, dass das Verbot auf den Export von automatisierter Gesichtserkennung ausgedehnt würde.

Die **Vorsitzende**: Herzlichen Dank. Frau Rohrbach, jetzt haben Sie das Wort für vier Minuten.

SVe **Lena Rohrbach**: Eine wichtige Unterscheidung, die Constanze Kurz vorgenommen hat, würde ich gern noch näher erläutern. Es ist richtig, dass es viele – ich sehe gerade, ich habe mein Video nicht an. Das mache ich noch schnell – und auch legitime Anwendungen von Gesichtserkennungstechnologie gibt. Deswegen habe ich mich im Vorfeld gefragt, ob ich in der knappen Zeit, die mir für mein Eingangsstatement zur Verfügung steht, wirklich jedes Mal von einer identifizierenden automatisierten Gesichtserkennung im öffentlichen Raum sprechen soll. Ich habe mich dann dafür entschieden, um eben diese Differenzierung deutlich zu machen. Grob gesagt, kann man Gesichtserkennung in zwei verschiedene Funktionen unterteilen. Zum einen gibt es die authentifizierende oder verifizierende Funktion, die im Grunde die Frage beantwortet, ob eine Person wirklich die ist, die sie vorgibt zu sein. So funktioniert zum Beispiel ein Smartphone, das mit einem sogenannten Gesichtslogg arbeitet oder die Grenzkontrolle am Flughafen, wenn man dort seinen Personalausweis nicht einer Person, sondern einer Maschine vorlegt, die dann für dieses Gesicht nach einem exakten Treffer sucht. Davon sind normalerweise keine weiteren Personen betroffen. Zudem lässt sich in den meisten Fällen der Kontext, in dem man zu dieser Art von Gesichtskontrolle aufgefordert wird, umgehen. Und offensichtlich wird davon auch Gebrauch gemacht. Deswegen halten wir diese Systeme für menschenrechtlich weniger problematisch. Andere Gesichtserkennungssysteme können hingegen verdeckt eingesetzt werden. Ich würde daher sagen, dass für die authentifizierende oder verifizierende Gesichtserkennung keine Exportkontrolle und ganz sicher kein Verbot in Betracht gezogen werden muss. Die identifizierende Gesichtserkennung beantwortet die Frage, wer eine Person ist; sie kann anlasslos im öffentlichen Raum eingesetzt werden, um die Gesichter von allen Menschen zu scannen, die an dem Gerät vorbeigehen. Diese Technik ermöglicht es zu prüfen, ob unter den erfassten Personen solche sind, die in einer Liste von Fotos von gesuchten Kriminellen oder auch von gesuchten Oppositionellen – je nach Kontext – geführt werden. Diese Technik ist problematisch wegen der Anlasslosigkeit der Erfassung, weil sie dazu führt, dass viele Personen, die sich nur zufällig im öffentlichen Raum aufhalten, herausgefiltert bzw. analysiert werden können. Denn es ist nun einmal ein konstituierendes Merkmal öffentlicher Räume, dass dort viele Leute vorbeigehen. Dazu hat das Bundesverfassungsgericht in seinem Urteil zum Kfz-Scanning Folgendes festgestellt: Selbst wenn ein Kfz-Kennzeichen – also etwas noch vergleichsweise Harmloses im Vergleich zu einem Gesicht – nur durch ein Scanning-System durchläuft, dort analysiert und dann gleich wieder gelöscht wird, handelt es sich hier um einen Eingriff. Das gleiche gilt für unsere Gesichter. Auch wenn wir quasi nur durchlaufen, analysiert werden und dann aufgrund der Entscheidungen des Algorithmus – der lernt ja – wieder gelöscht werden, ist das trotzdem ein Eingriff und hat Auswirkungen, wie beispielsweise den Chilling Effect. Die Hersteller nehmen selbst solche Unterscheidungen vor. Im Zusammenhang mit der Thales Group zum Beispiel, einem sehr großer Hersteller, habe ich, glaube ich, zum ersten Mal von dieser Unterscheidung gehört. Die Hersteller sind in der Lage, ihre eigenen Technologien entsprechend zu kategorisieren. Deswegen bin ich sicher, dass es – auch wenn es eine Herausforderung darstellt – mit ein wenig Einsatz und durch entsprechende Informationen der Hersteller möglich sein müsste, Regularien so abzufassen, dass die eine Art der Gesichtserkennung einer Exportkontrolle unterworfen oder sogar verboten werden kann, während man die andere als harmlos einstuft. Constanze Kurz hatte gesagt, dass die Fehlerquote schon geringer geworden ist, und sie hatte über die diskriminierenden Effekte gesprochen. Das stimmt, die Fehlerquote vermindert sich rapide, weil die Algorithmen der Gesichtserkennung mittlerweile mit Hilfe immer diverserer Sets trainiert werden. Trotzdem muss man sagen, dass es einen Diskriminierungseffekt gibt, der dieser Technologie quasi inhärent ist und den man nicht eliminieren kann. Es besteht das Risiko, dass Gesichtserkennung gezielt gegen Menschen eingesetzt wird, die Merkmale aufweisen, welche durch die Antidiskriminierungsgesetzgebung geschützt sind, weil diese sich nun einmal vor allem im Gesicht niederschlagen, wie zum Beispiel Ethnie, Alter oder Geschlecht. Das sehen wir zum Beispiel in China, wo der Hersteller

Hikvision für seine Gesichtserkennungskameras gezielt mit dem Hinweis geworben hat, dass sie zwischen Uiguren und Han-Chinesen unterscheiden könnten. Das wurde dann später wieder von der Webseite gelöscht. Das ist auch relevant, weil …

Die **Vorsitzende**: Kommen Sie bitte zum Schluss!

SVe **Lena Rohrbach**: … Gesichtserkennung ein wesentlicher Baustein des Überwachungssystems ist, das gegen die Uiguren eingesetzt wird.

Die **Vorsitzende**: Vielen Dank, Frau Rohrbach. Als Nächster hat nun der Kollege Peter Heidt für die FDP das Wort für zwei Minuten.

Abg. **Peter Heidt** (FDP): Vielen Dank, Frau Vorsitzende. Ich würde mich auch gern an Frau Kurz und Frau Rohrbach wenden. Ich will ein wenig anknüpfen an den Kollegen Schwabe und auf dieses Spannungsfeld hinweisen, das es natürlich gibt. Wir müssen unterscheiden zwischen einem Rechtsstaat wie der Bundesrepublik auf der einen Seite und Unrechtsstaaten auf der anderen Seite. Neben China und der Bundesrepublik gibt es aber ein breites Feld von Ländern, die irgendwie dazwischen liegen. Die Künstliche Intelligenz, die immer mehr auf uns zukommt, schafft weitere Möglichkeiten. Ich sehe die Probleme, auf die Sie hingewiesen haben, genauso wie Sie. Zunächst schaue ich mir die Videoüberwachung an. In Hessen wird dieser Tage beschlossen, 200 Millionen Euro – soweit ich mich richtig erinnere – für flächendeckende Videoüberwachung auszugeben. Darauf bezieht sich meine Frage. Denn Sie haben zu Recht beschrieben, dass von den menschenrechtlichen Risiken durch Gesichtserkennung vor allem marginalisierte Gruppen betroffen sind. Wie können wir als demokratischer Rechtsstaat damit umgehen? Ein komplettes Verbot oder ein Stopp der Entwicklung dieser Technologien ist natürlich nicht einfach zu realisieren. Auch mit dem Darknet gibt es Probleme. Sie sagten zwar, dass die geringer geworden seien, ich habe aber in meiner eigenen beruflichen Praxis immer wieder festgestellt, dass sich vor allem im Bereich Betäubungsmittel nach wie vor Einiges abspielt. Deshalb würde ich gern von Ihnen noch ein paar Informationen bekommen, die uns helfen könnten, hier den richtigen Weg einzuschlagen. Und vielleicht noch eine Frage an Frau Rohrbach. Sie hatten gesagt, dass Internet-Shutdowns sehr problematisch sind, und auf die daraus resultierenden Menschenrechtsverletzungen verwiesen. Vielleicht könnten Sie ein bisschen näher ausführen, wie wir in Deutschland in diesem Bereich effektiver vorgehen und uns noch besser gegen solche Internet-Shutdowns wappnen könnten. Vielen Dank.

Die **Vorsitzende**: Herzlichen Dank, Herr Heidt. Dann machen wir jetzt Folgendes: Ich würde umgekehrt beginnen, und Sie wechseln sich ab. Frau Rohrbach, Sie haben das Wort für vier Minuten, und dann kommt Frau Dr. Kurz.

SVe **Lena Rohrbach**: Vielen Dank. Also die erste Frage war, was wir – abgesehen von einem Verbot – tun könnten, wenn es die Videoüberwachung und die Gesichtserkennung nun einmal gibt. Sie werden von mir natürlich nichts anderes hören, als dass eben diese … (*Ton abgebrochen*)

Die **Vorsitzende**: Frau Rohrbach, wir können Sie zurzeit nicht verstehen. Ich glaube, das Mikrophon ist ausgeschaltet. Vielleicht starten Sie einfach noch einmal. Jetzt sind Sie zu hören. Starten Sie einfach noch einmal von vorne.

SVe **Lena Rohrbach**: Vielen Dank. Was die anlasslose Überwachung bzw. die Gesichtserkennung oder auch die Videoüberwachung im öffentlichen Raum angeht, werden Sie von mir keine andere Empfehlung bekommen als die, diese Techniken generell nicht anzuwenden, weil dies unverhältnismäßig wäre und auch weil es das Problem der so genannten Mission Creeps gibt, wenn wir die Anwendung in manchen Fällen zulassen. Das haben wir zum Beispiel von der Vorratsdatenspeicherung gelernt. Da kommt dann sehr schnell der Wunsch auf, immer weitere Anwendungsfälle, die wirklich nicht mehr verhältnismäßig sind, zuzulassen. Gleichwohl gibt es legitime Anwendungen von Gesichtserkennung, bei denen es sich eben nicht

um eine identifizierende anlasslose Gesichtserkennung im öffentlichen Raum handelt. In der Tat können wir hier etwas tun, um die Diskriminierungseffekte, die ich erwähnt habe, zu verringern. So habe ich Ihre Frage verstanden. Die Gesichtserkennung wirkt ja diskriminierend wegen der so genannten Historic Bytes; das heißt, die Algorithmen sind trainiert durch die Daten, die sie eingespeist bekommen haben, und die sind eben wenig divers. Wenn man diese nun diverser gestaltet, dann wird der Algorithmus weniger diskriminierende Effekte zeigen. Das geschieht auch schon. Vor allem die teureren Systeme können das mittlerweile schon viel besser. Eine andere Möglichkeit bietet der sogenannte Computer Bias. Er knüpft an die Tatsache an, dass bei all denjenigen, die solche Systeme einsetzen – zum Beispiel bei Polizeibehörden, aber auch bei uns allen – der psychologische Effekt zu beobachten ist, dass man die Ergebnisse eines Computers für besonders objektiv und glaubwürdig hält, obwohl sie das nicht unbedingt sind; manchmal ist sogar das Gegenteil der Fall. Wenn man nun Menschen darüber aufklärt, dass es diesen Bias gibt, dann gibt man Ihnen – oder zum Beispiel einer Polizeibehörde – die Möglichkeit, das Ergebnis, das ihnen das System geliefert hat, noch einmal kritisch zu überprüfen. Ferner sollten öffentliche Stellen unseres Erachtens keine Algorithmen einsetzen, in die nicht hineingeschaut werden oder deren Ergebnis man nicht erklären kann. Denn die Opakheit beim Einsatz durch die öffentlichen Stellen führt zu vielen Problemen, zum Beispiel beim Recht auf ein faires Verfahren. Wir sind daher der Meinung, dass die Hersteller der Technologien, die zum Beispiel von Polizeibehörden verwendet werden, zu einer Transparenzanzeige verpflichtet werden sollten. Der Algorithmus sollte mit einer Art Warnzettel verknüpft werden, der offenlegt, wie der Algorithmus trainiert wurde, wie er funktioniert und welche Fehler er möglicherweise produzieren könnte. Wenn das der Fall wäre, würde das diejenigen, die solche Systeme einsetzen, in die Lage versetzen, anders mit den Systemen umzugehen. Eine weitere Frage bezog sich auf die Shutdowns. Wir können sie natürlich von Deutschland aus nicht verbieten, weil wir sie ja erfreulicherweise nicht durchführen. Wir können uns aber international, zum Beispiel auf UN-Ebene, in Form von den von Herrn Kettemann angesprochenen Resolutionen dagegen aussprechen und auch versuchen, diesbezüglich Verhandlungen über ein Vertragswerk in Gang zu bringen. Eine andere Frage ist, wie die Menschen vor Ort mit Shutdowns oder auch mit partiellen Sperren umgehen können. Da spielt auch TOR wieder eine Rolle, und damit sind wir wieder beim Darknet-Paragraphen angelangt. Deutschland ist das Land mit den meisten Menschen, die sich für TOR engagieren und wo die meisten TOR-Knoten betrieben werden. Das heißt, wenn Deutschland als das Land, das die meiste Infrastruktur dafür weltweit zur Verfügung stellt, TOR kriminalisieren würde, hätte dies weltweite Auswirkungen.

Die **Vorsitzende**: Herzlichen Dank. Da kann, glaube ich, Frau Dr. Kurz nahtlos anschließen. Vier Minuten.

SVe Dr. **Constanze Kurz**: Nein, die Frage nach TOR war gar nicht an mich gerichtet, aber ich stimme Frau Rohrbach natürlich zu. Tatsächlich sind die Deutschen mit Abstand die Aktivsten in diesem TOR-Netzwerk; das gilt übrigens auch für den CCC, und darauf sind wir nicht wenig stolz. Ich will etwas zur Gesichtserkennung sagen. Frau Rohrbach hatte vor allem auf die identifizierenden Verfahren abgehoben. Mir geht es um einen anderen Aspekt, den ich vorhin schon zu betonen versucht habe, nämlich darum – und Sie haben das in ihrer Frage bereits kurz angesprochen –, dass mit diesem System automatisierte Entscheidungen getroffen werden. Zum Beispiel landet das Gesicht eines bestimmten Menschen, der erfasst wird, wenn Passanten anlasslos gefilmt und die Aufnahmen dann ausgewertet werden, in einer Datenbank. Außerdem ist es an Flughäfen so, dass unmittelbar eine Reaktion erfolgt, dass also eine automatisierte Entscheidung getroffen wird. Das war für uns das qualifizierende Kriterium dafür, ein Verbot zu fordern. Aus meiner Sicht wäre ein Verbot aber nicht das Einzige. Ich möchte selbstverständlich keine anlasslose Massenüberwachung von Gesichtern in Deutschland oder in Europa haben. Vielmehr fordern wir von den europäischen Staaten und vor allem von Deutschland, sich dafür einzusetzen, dass diese Technik in den Ländern, in denen sie bereits eingesetzt wird – und zwar

flächendeckend und ohne Diskussion, weil es diese Form von öffentlicher Diskussion wie bei uns dort gar nicht gibt –, zurückgebaut wird und die Geräte, die dafür aus dem Westen eingeführt worden sind, nicht mehr verwendet werden dürfen. Wenn man zum Beispiel nach China blickt, stellt man allerdings fest, dass manche Länder ihre eigenen Hersteller haben. Sie müssen also nicht unbedingt auf westliche Softwareprodukte zurückgreifen. Aber sofern dies der Fall ist, würde ich auf jeden Fall an unserer Forderung festhalten wollen. Somit wäre ein Verbot der massenhaften automatisierten Gesichtserkennung die eine und das Engagement dafür, dass diese Technik anderswo nicht noch weiter ausgebaut oder ihr Einsatz sogar rückgefahren wird, die andere Sache. Ich möchte außerdem Frau Rohrbach darin beipflichten, was sie zu der Stellungnahme sagte, die der Deutsche Anwaltsverein zu der automatisierten Gesichtserkennung abgegeben hat. Ich denke, der Verein hat sich die relevanten Urteile aus der Rechtsprechung des Bundesverfassungsgerichts genau angeschaut und sehr klar die Ansicht vertreten, dass wir hier von einer anlasslosen Überwachung sprechen müssen, gegen die man sich nicht wehren kann, weil die wenigsten von uns – wenn man einmal von Pandemiezeiten absieht – ihr Gesicht verdecken. Und selbst daran passen sich – wie wir gelernt haben – die Softwarehersteller schon an, indem sie dies zu kompensieren versuchen und jetzt nur noch bestimmte Bereiche des Gesichts, die Augen, in die Softwareanalyse einbeziehen. Ich will abschließend noch auf einen weiteren Bereich zu sprechen kommen, der hier noch keine große Rolle gespielt hat, der aber mit der automatisierten Gesichtserkennung eng zusammenhängt, nämlich das sogenannte Predictive Policing. Es gibt eine ganze Reihe von großen Testprojekten kommerzieller Art, die an die Polizei in großen Städten verkauft werden. Diese sind jedoch teilweise schon wieder zurückgerollt worden, etwa in den USA. Aber dort ist diese automatisierte Erkennung in andere Analyseprodukte im Rahmen des sogenannten Predictive Policing eingebaut worden. Das wird vor allem von der Firma Palantir angeboten. Auch in Hessen soll ein Teil dieser Software Verwendung finden. Wir müssen uns also dessen bewusst sein, dass sich die Überwachungstechnik in ihrer Gesamtheit nicht auf die Erfassung von Körpermerkmalen beschränkt, sondern dass hier weitere Daten hinzukommen, wie etwa Äußerungen in den Social Media, Daten von Mobiltelefonen oder Informationen aus Polizeidatenbanken samt der Historie der Daten, die dort gespeichert ist. Wir haben es also mit einem großen Problemfeld zu tun, bei dem es nicht allein um Gesichtserkennungssyteme, sondern auch um alltägliche Äußerungen geht, die dann in größere Überwachungs- und Kontrollsysteme inkorporiert werden.

Die **Vorsitzende**: Herzlichen Dank. Dann hat jetzt der Kollege Brandt für DIE LINKE. das Wort. Zwei Minuten.

Abg. **Michel Brandt** (DIE LINKE.): Erst einmal auch von mir vielen Dank für Ihre Stellungnahmen und für die sehr interessante Debatte, die sich hier jetzt gerade daraus entspinnt. Ich habe noch einige kleinere Fragen an Frau Rahman. Wir haben zwar gerade schon über den Schutz von Whistleblowern gesprochen. Mir geht es aber darüber hinaus um Menschenrechtsverteidigerinnen generell, die Repressionen oder einer Überwachung ausgesetzt sind, weil mittlerweile die technologischen Methoden dafür vorhanden sind. Was wäre denn für uns im Ausschuss der Arbeitsauftrag bzw. was wäre generell zu tun, um Menschenrechtsverteidigerinnen international besser schützen zu können? Wie könnte man von politischer Seite, auch von Seiten der Bundesregierung, effektiver agieren und reagieren? Außerdem habe ich an Frau Rohrbach folgende Frage: Denken Sie, dass ein Lieferkettengesetz, das den Unternehmen bestimmte Sorgfaltspflichten vorschreibt, eine Option bieten würde, um dem Export von Sicherheitstechnik, die woanders missbraucht werden kann, vorzubeugen? Würden Sie sagen, dass darin eine Chance liegt? Ich habe noch eine weitere Frage, die sich an beide Sachverständige richtet. Wir haben viel über die Gefahren gesprochen, die diese Technologien mit sich bringen. Ich würde jetzt gern zumindest noch einmal kurz auch auf die Chancen zu sprechen kommen und Ihnen die Möglichkeit geben wollen auszuführen, inwieweit die neuen Technologien

und ihre Anwendungsmöglichkeiten Menschenrechtsverteidigerinnen oder auch marginalisierten Gruppen eine Chance bieten, Menschenrechte durchzusetzen, sich besser zu vernetzen und mehr zu kommunizieren. Dankeschön.

Die **Vorsitzende**: Herzlichen Dank. Frau Rahman, jetzt haben Sie für vier Minuten das Wort.

SVe **Zara Rahman**: Vielen Dank für die Fragen. Zunächst zu der ersten Frage: Was können wir tun, um Menschenrechtsverteidiger besser zu schützen? Ich denke, wir brauchen eine Kombination von Lösungen auf verschiedenen Ebenen. Ich halte es zunächst einmal für wichtig, dass die politische Ebene nicht zur Verstärkung des Problems der digitalen Überwachung in Deutschland beiträgt, zum Beispiel – wie die beiden Kolleginnen schon ausgeführt haben – durch die Entwicklung oder den Verkauf von Überwachungstechnologie durch deutsche Unternehmen. Ich denke, wir sollten ein striktes Exportverbot oder eine strikte Exportkontrolle für Überwachungstechnologie einführen. Außerdem sollten wir – das ist auch schon angesprochen worden – mehr Unterstützung für die Entwicklung von Verschlüsselungssoftware leisten, die es Menschen ermöglicht, sich gegen Überwachung zu schützen, wie zum Beispiel der TOR-Browser oder andere Verschlüsselungstechnologien. Ich glaube, auch Nighat hat schon gesagt, dass Deutschland von anderen Ländern oft zum Vorbild genommen wird. Ich denke, das ist sehr wichtig, und daher sollte die Politik sich nicht verleiten lassen, das Urheberrecht zum Vorwand für die Zensur von Informationen zu nehmen, sondern sollte sich die Stärkung von Transparenz und Informationsfreiheit zum Ziel setzen. Dann zu den marginalisierten Gruppen: Ich denke, es ist wichtig, diesen Menschen erst einmal zuzuhören, um zu erfahren, was sie wollen und was sie brauchen. Man kann nicht über marginalisierte Gruppen sprechen, bevor man verstanden hat, was die Hindernisse für ihre Teilhabe sind. Zum Beispiel stellen, wie ich bereits gesagt habe, die strukturelle Diskriminierung und der strukturelle Rassismus ein gravierendes Problem in der deutschen Gesellschaft dar. Ich finde es wichtig, erst einmal zuzuhören, was diese Menschen wollen und brauchen. Es gibt so viele potentielle Gründe dafür, weshalb die Teilhabe für diese Gruppen so schwer zu realisieren ist. Das hängt zum Beispiel mit der Infrastruktur, dem Internetzugang – wie Nighat schon gesagt hat – dem Digital Gender Gap oder auch mit den Erfahrungen zusammen, die diese Gruppen auf den digitalen Plattformen machen. Ich tue mich schwer mit konkreten Empfehlungen, aber ich würde sagen, man sollte erst einmal richtig zuhören, was diese Gruppen wollen und was sie brauchen, und ihnen dann die Chance geben, selbst zu entscheiden. Danke.

Die **Vorsitzende**: Herzlichen Dank. Dann hat Frau Rohrbach das Wort. Vier Minuten.

SVe **Lena Rohrbach**: Danke schön. Ich glaube tatsächlich, dass das, was wir im Moment unter dem Stichwort Lieferkettengesetz diskutieren, eine stark unterschätzte positive Auswirkung auf den gesamten Bereich Digitalisierung und Menschenrechte hätte. Deswegen bin ich nicht ganz glücklich mit dem Begriff Lieferkettengesetz und würde den Begriff Sorgfaltspflichtengesetz bevorzugen, weil er zeigt, dass die Regelung über das Problem der Lieferketten hinausgeht. Tatsächlich sind im Bereich Digitalisierung und Menschenrechte bzw. Risiken und Chancen fast immer private Unternehmen beteiligt. Dadurch zeichnet sich dieser Bereich aus. Wenn man von den seltenen Ausnahmefällen absieht, in denen Staaten ein System vollständig selbst entwickelt haben – was manchmal bei sehr kritischen Technologien oder Infrastrukturen vorkommt –, ist hier eigentlich immer ein privates Unternehmen beteiligt. Und wenn diese privaten Unternehmen angehalten wären, gemäß den UN-Leitlinien ihre Sorgfaltspflichten zu erfüllen, dann hätte man damit, glaube ich, „viele Fliegen mit einer Klappe geschlagen“, wie man das so sagt. Das reicht von der Hassrede im Internet über die typischen Risiken für Social Media-Plattformen bis hin zur KI. Alle Unternehmen sind ja angehalten, sich Gedanken darüber zu machen, welche spezifischen menschenrechtlichen Risiken mit ihrer Arbeit verbunden sind, und gegebenenfalls Gegenmaßnahmen zu ergreifen. Deswegen hatten wir den Vorschlag gemacht, den

Unternehmen im Rahmen der Dual Use-Reform für den Export von Überwachungstechnik Sorgfaltspflichten aufzuerlegen und darüber hinaus ein allgemeines Sorgfaltspflichtengesetz zu verabschieden, damit am Ende alle technischen Unternehmen ab einer gewissen Größe mit erfasst werden. Eine solche Regelung hat in der EU schon einmal ernsthaft zur Debatte gestanden, sie ist aber in dem aktuellen Kommissionsvorschlag leider nicht mehr enthalten. Im Übrigen gibt es positive Beispiele, die zeigen, wie Unternehmen Menschenrechte schützen können. Das könnten Sie als Parlamentarier vielleicht auch erreichen, wenn Sie die besagten Regelungen zu den Sorgfaltspflichten einführen würden. Die Unternehmen Google und Facebook werden zwar oft mit guten Gründen gescholten, aber auch sie liefern zum Teil positive Beispiele. So haben uns ägyptische Menschenrechtsverteidiger Screenshots von einer Warnmeldung gezeigt, die sie von ihrem Anbieter GMail bekommen haben und mit der sie darauf aufmerksam gemacht wurden, dass bestimmte Personen versucht haben, ihre Konten zu hacken. Der Anbieter GMail hat seinen Kunden sogar mitgeteilt, dass er die Vermutung hat, der Angriff sei von der Regierung gesteuert gewesen. Dadurch hätten die Menschenrechtsverteidiger die Chance bekommen, ihr Verhalten entsprechend anzupassen. Außerdem hat man ihnen das Angebot gemacht, in das Social Protection Program aufgenommen zu werden. Ferner hat Facebook kürzlich mitgeteilt, dass man mit Hilfe von Metadatenanalysen die Möglichkeit erhalten habe, gegen das sogenannte Cyber-Grooming vorzugehen, also gegen Menschen, die sich auf Facebook an Kinder heranmachen. Nicht alle, aber viele dieser Mechanismen, die Facebook da verwendet hat, wären auch gut geeignet, um Menschenrechtsverteidigerinnen oder Journalistinnen vor Angriffen wie dem Social Engineering auf Facebook zu schützen, also vor Menschen, die auf Facebook vorgeben, Freundinnen und Freunde oder Aktivisten zu sein, um sich das Vertrauen der Menschenrechtsverteidigerinnen und Journalistinnen zu erschleichen, ihnen dann eine E-Mail mit einem Link zu schicken, der beim Öffnen zur Installation einer Spionagesoftware führen würde. Ich glaube, in diesem Bereich gibt es noch viel Gutes, was Unternehmen tun könnten. Im Übrigen hat Frau Rahman gerade schon Einiges genannt, was man tun kann, um die Chancen der digitalen Technologien besser zu nutzen, wie zum Beispiel Ende zu Ende-Verschlüsselungen, die Förderung von VPN oder TOR- und Whistleblower-Plattformen.

Die **Vorsitzende**: Herzlichen Dank, Frau Rohrbach. Dann hat nun der Kollege Gehring zwei Minuten lang das Wort für die GRÜNEN.

Abg. **Kai Gehring** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank. Ich hoffe, ich bin zu verstehen. Ihre Antwort baut eine Brücke zu der Frage, die ich an Constanze Kurz stellen möchte. Jetzt noch einmal zusammenfassend: Mit welchen Instrumenten und Mitteln kann die BRD Ihrer Einschätzung nach am besten dazu beitragen, digitale Schutzräume für Menschenrechtsverteidigerinnen und Menschenrechtsverteidiger zu erhalten bzw. neue zu schaffen? Es wäre mir wichtig, von Ihnen zusammenfassend etwas über die gesetzgeberischen Möglichkeiten zu erfahren. Meine zweite Frage richtet sich an Frau Rohrbach. Sie hatten schon einzelne Beispiele für die zusätzlichen Diskriminierungsrisiken von Minderheiten und marginalisierten Gruppen durch staatliche oder private automatisierte biometrische Erkennungstechnologien genannt. Ich denke, das wäre sehr wichtig, und deshalb möchte ich Sie fragen, ob Sie noch weitere Beispiele oder Belege dafür anführen können, einfach um das Problembewusstsein des Bundesgesetzgebers für die verschiedenen Dimensionen weiter zu schärfen. Denn das ist ja ein Problem, das es auch in liberalen Demokratien gibt. Ihre diesbezüglichen Regulierungsvorschläge teile ich ausdrücklich. Eine weitere Frage richtet sich an Sie beide. Uns ist es wichtig, hier interdisziplinär zu denken, und der Forschung kommt ja auch eine große Bedeutung zu. Inwieweit werden Sie als Menschenrechtsverteidigerinnen und -verteidiger von Forschungseinrichtungen und Forschungsförderorganisationen systematisch in interdisziplinäre Forschungsvorhaben einbezogen, wenn es um die digitalen Technologien geht? Denn aus meiner Sicht sind menschenrechtliche und ethische Perspektiven in der Technikfolgenabschätzung, in der

Begleitforschung oder auch schon beim Forschungsdesign sehr wichtig. Könnten Sie hierzu noch Ausführungen machen? Danke.

Die **Vorsitzende**: Herzlichen Dank. Frau Dr. Kurz, Sie haben das Wort für vier Minuten.

SVe Dr. **Constanze Kurz**: Ich bedanke mich für die Frage. Natürlich könnte man dazu jetzt noch endlos weitere Vorschläge machen, aber ich will mich auf die wichtigsten beschränken. Ich denke, für viele dieser Fragen bildet die IT-Sicherheit gewissermaßen die Basis, und das ist der Bereich, auf den Deutschland und andere europäische Länder ihren Fokus richten könnten. Es geht darum, digitale Systeme zu schaffen, die anonymisierte Kommunikation ermöglichen, die aber auch sicher sind, also frei von Hintertüren, und deren Verschlüsselungssoftware nicht absichtlich abgeschwächt wurde. Wir haben in Europa ohnehin eine strukturelle IT-Sicherheitskrise. Mit einer Regelung in diesem Bereich würde man also zwei Fliegen mit einer Klappe schlagen. Gleichzeitig müsste man natürlich auch überlegen, wie man garantieren kann, dass auch Menschen in repressiven Regimen diese Technologien sicher nutzen können. Dafür müssten dann Verschlüsselungs- und Anonymisierungslösungen korrekt eingesetzt werden. Das heißt aber, man muss die Nutzer schulen. Dafür haben wir ein paar Vorschläge gemacht. Wenn man sich Beispiele aus der Vergangenheit ansieht – wir haben eines genannt –, dann stößt man auf die Firma Blackberry. Generell gilt: Wenn man erstmal die Tür geöffnet hat, egal für welche Art von Regimen, um an Inhalte zu kommen, dann tritt sehr schnell der Fall ein, dass auch andere Staaten und vor allem nicht demokratische Staaten diese Zugänge haben wollen. Bei Blackberry war das zum Beispiel mal der Fall, die sind aber heute im Mobiltelefonmarkt nicht mehr so wichtig. Die Frage, wem man unter welchen Bedingungen Zweitschlüssel oder Drittschlüssel für verschlüsselte Kommunikation überlässt, ist eine eminent politische Frage – insbesondere wenn man an Länder denkt, die nicht solche demokratischen Standards haben. Alles, was man tun kann, um die IT-Sicherheit zu erhöhen und die Hintertürenfreiheit zu garantieren, hat mit Transparenz zu tun. Daher ist es auf jeden Fall zu befürworten, dass man in Europa vor allem solche Verschlüsselungs- und Anonymisierungslösungen fördert, die Open Source sind – also die man sich ansehen und deren Sicherheit man garantieren kann –, dass man aber auch die wissenschaftliche Forschung stärkt und die Möglichkeiten zu testen ausweitet. Wie wir schon gehört haben, sind die Turonian Services die zentrale Software für solcherart Kommunikation und Anonymisierung, und da fließen natürlich auch europäische und US-amerikanische Gelder hinein, nicht nur um die Software zu erstellen, sondern auch um sie zu erhalten, um Löcher darin zu finden und so weiter. Es geht auch darum, die Leute zu schulen, die die Technik benutzen. Auf all diese Dinge würden wir den Fokus legen. Vielleicht abschließend noch: Damit helfen wir nicht nur den von Repressionen bedrohten Benutzern irgendwo auf der Welt, sondern letztlich auch uns selbst. Denn wir sind genauso angreifbar; und das gilt übrigens nicht nur für Privatleute, sondern natürlich auch für die Wirtschaft und die Behörden, die diese Software benutzen– gerade wenn wir über verschlüsselte Kommunikationswege nachdenken. Wir tun also nicht nur anderen einen Gefallen, sondern letztlich auch uns selbst. Für die Politik heißt das, dass man gesetzgeberische Hintertüren auf jeden Fall vermeiden sollte. Vielen Dank.

Die **Vorsitzende**: Herzlichen Dank. Frau Rohrbach, dann haben Sie jetzt für vier Minuten das Wort.

SVe **Lena Rohrbach**: Vielen Dank. Das waren im Grunde zwei Fragen; die erste bezog sich auf die höheren Fehlerraten und die diskriminierenden Effekte. Zu den People of Color zählen auch Frauen, und auch bei nichtbinären und genderfluiden Menschen treten besonders hohe Fehlerraten auf, was zur Folge hat, dass sie zum Beispiel häufiger von der Polizei angehalten werden. In manchen Ländern kann es sogar zu einer Inhaftierung oder zu Folterungen führen, wenn eine Gesichtserkennung fälschlicherweise gemeldet hat, dass eine Person kriminell ist und gesucht wird. Unzureichend untersucht ist die Fehleranfälligkeit bis jetzt in Bezug auf Menschen mit Behinderung. Nun zu den konkreten

Beispielen: Die American Civil Liberty Union hat einmal mit Hilfe der Amazon-Software Recognition Fotos der Mitglieder des US-Repräsentantenhauses mit einer Liste von Fotos von 25.000 Straftätern und Straftäterinnen verglichen. Das kostet übrigens gut 12 Dollar – soweit zu dem Punkt, dass es immer günstiger wird, solche Technik anzuwenden. Die Software hat dann tatsächlich 28 Repräsentantenhaus-Politiker als Kriminelle identifiziert, von denen 40 Prozent People of Color waren, obwohl diese nur 20 Prozent der Mitglieder des Kongresses stellen. Ein anderes Beispiel, an das sich vielleicht manche erinnern, ist der Fall, bei dem Google-Images Bilder von Afroamerikanern fälschlicherweise als Gorillas identifiziert hat. Zum Glück haben sich die Betroffenen über Social Media gewehrt, so dass Google schnell darauf aufmerksam geworden ist. Das ist ein Beispiel für eine wirklich gravierende Diskriminierung im Algorithmus. Auch bei der Gesichtserkennung kommt es zu intersektionalen Diskriminierungen. Das heißt, wer gleich mehrere Merkmale aufweist, ist besonders betroffen, zum Beispiel schwarze Frauen. Ein weiteres Beispiel aus den USA liefert gerade die Bewegung Black Lives Matter. Die beschriebene Diskriminierung wird dadurch weiter verstärkt, dass in den USA schwarze Menschen in den polizeilichen Fotodatenbanken nicht nur überrepräsentiert sind, sondern dass es darüber hinaus eher zu fehlerhaften Matches kommt, weil sie häufiger auf der Straße angehalten werden. Die Meldungen werden dann gegebenenfalls mit den polizeilichen Datenbanken abgeglichen, und das führt zu so genannten Over Policed Communities. Dort leben viele Menschen, die einer diskriminierten Gruppe angehören oder die sich für diese einsetzen, zum Beispiel aktuell für schwarze Menschen, die sich gegen Rassismus wehren. Da Menschenrechtsverteidiger in vielen Ländern darauf angewiesen sind, sich im öffentlichen Raum zu treffen, sind Aktivistinnen und Menschenrechtsverteidigerinnen eben auch in besonders hohem Maß von den beschriebenen Effekten betroffen. Zur Frage nach den Forschungszusammenhängen ist zu sagen, dass Amnesty International da in Deutschland nicht eingebunden wird. Ich kann nicht für die internationale Ebene sprechen, da müsste ich tatsächlich nachfragen. Aber auf jedem Fall kann man sagen, dass zivilgesellschaftliche Akteure in die Forschung und Entwicklung sowie in die Technikfolgenabschätzung nicht systematisch eingebunden werden, obwohl das sicherlich wünschenswert wäre.

Die **Vorsitzende**: Herzlichen Dank, Frau Rohrbach. Wir haben noch eine knappe halbe Stunde Zeit bis zum Ende der Anhörung und würden jetzt in die dritte Runde starten. Ich werde einfach bei den einzelnen Fraktionen schauen, ob es noch weitere Fragen gibt. An Sie alle gemeinsam, auch an die Sachverständigen, habe ich die Bitte, sich vielleicht etwas kürzer zu fassen, damit gegebenenfalls noch einmal alle Fraktionen die Möglichkeit haben, Fragen an Sie zu richten. Ich schaue Frank Heinrich von der Union an. Zwei Minuten, maximal.

Abg. **Frank Heinrich** (Chemnitz) (CDU/CSU): Ich werde den Zeitrahmen nicht ausschöpfen. Ich würde gern Frau Dr. Kurz vom Chaos Computer Club und auch Frau Rohrbach nach der Zusammenarbeit fragen. Hier kam gerade die Frage auf, inwieweit Sie in die Technikfolgenabschätzung eingebunden sind. Ich möchte hingegen wissen, inwiefern sich die NGOs und die Beteiligten der Zivilgesellschaft bei diesem Thema absprechen. Wir binden Sie ja heute hier ein, und ich finde es großartig, dass wir das auf dieser Ebene tun. Ich hatte mit Amnesty vor einem Jahr ein Gespräch, und da hatte ich den Eindruck, dass man selbst noch nicht weiß, welche Definitionen man verwenden will und wo die menschenrechtlichen Stolpersteine liegen. Auf all das konnte man mir noch keine hundertprozentige Antwort geben. Wo stehen Sie jetzt in dem Prozess der Zusammenarbeit der Organisationen?

Die **Vorsitzende**: Frau Dr. Kurz und dann Frau Rohrbach.

SVe Dr. **Constanze Kurz**: Ehrlich gesagt würde ich den Chaos Computer Club nicht mit Amnesty vergleichen wollen. Wir sind eine vollständig ehrenamtlich arbeitende Organisation. Es gibt keine Form von strukturierter Arbeit. Wir bestehen aus Arbeitsgruppen, die sich zusammenfinden, weil die Beteiligten ein

Interesse daran haben oder weil sie in diesem Bereich arbeiten oder früher gearbeitet haben. Zum Thema Biometrie gibt es bei uns schon sehr lange eine Gruppe; die besteht seit 15 Jahren. Aber sie ist, denke ich, nicht so gut strukturiert, wie dies bei Organisationen wie Amnesty oder anderen zivilgesellschaftlichen Organisationen der Fall ist, die daran regelmäßig arbeiten. Wir beraten ab und an Parlamentarier bzw. Ausschüsse im Land oder im Bund, und wir schreiben Stellungnahmen für solche Ausschüsse oder auch für das Bundesverfassungsgericht. Aber das ist nicht vergleichbar etwa mit einer konstanten wissenschaftlichen Arbeit. Wir arbeiten international mit anderen NGOs zusammen. Das ist aber eher punktuell und nicht auf eine Weise organisiert, die ich als permanent oder dauerhaft bezeichnen würde. Als eine technisch orientierte Organisation versuchen wir, ein bisschen in die Zukunft zu schauen, um zu erfahren, welche Probleme auf uns zukommen; und die Ergebnisse machen wir dann auch gern öffentlich. Das schafft man manchmal, und manchmal schafft man es nicht. Ich würde das aber nicht als irgendeine Form von strukturierter Zusammenarbeit bezeichnen wollen, wenn ich ehrlich bin.

Die **Vorsitzende**: Frau Rohrbach, Sie haben das Wort.

SVe **Lena Rohrbach**: Erst einmal vielen Dank für das Kompliment bzw. dafür, dass der Chaos Computer Club den Eindruck hat, wir seien strukturiert. Das freut mich. Ich bin nicht ganz sicher, was Sie, Herr Heinrich, meinten, als Sie sagten, dass wir vor einem Jahr noch nicht klar hätten benennen können, welche Stolpersteine es gibt. Aber unabhängig davon, um welche es genau geht, es ist natürlich auch bei uns so, dass sich die Meinungsbildung gerade zu aktuellen Fragen immer in Entwicklung befindet und wir tatsächlich manchmal heute mehr zu einer Sache sagen können als zum Beispiel vor einem Jahr. Außerdem arbeiten wir mit anderen NGOs zusammen, tauschen Argumente mit ihnen aus oder finden uns zu Bündnissen zusammen. Auch beim Thema Digitalisierung, das wir heute hier besprechen, gibt es NGO-Bündnisse, an denen Amnesty und andere beteiligt sind wie die … **???**, das sich für eine Ächtung von autonomen Waffensystemen einsetzt. Generell gibt es natürlich auch bei solchen NGOs wie Amnesty, die hauptamtliche Mitarbeiter haben, aber vollständig spendenfinanziert sind, manchmal Kapazitätsprobleme, die darüber entscheiden, wo man sich noch einbringen kann und wo nicht mehr.

Die **Vorsitzende**: Vielen Dank, Frau Rohrbach. Dann hat der Kollege Braun das Wort. Zwei Minuten.

Abg. **Jürgen Braun** (AfD): Ich fasse mich jetzt kürzer, ich nehme Rücksicht auf alle, gar keine Frage. Mir geht es um Aktuelles, besonders darum, wie sich die sogenannte Corona-Pandemie auf die sozialen Medien ausgewirkt und was sie nach Ihrer Ansicht im Hinblick auf die Meinungsfreiheit verändert hat, was also auffällig ist im Bereich der sozialen Medien. Und dann die zweite Frage: Wie hat sich die Corona-Pandemie bzw. die Corona-Krise auf Entscheidungen des Gesetzgebers ausgewirkt? Denn wir befinden uns in der verfassungsrechtlich bedenklichen Lage, die auch von vielen Staatsrechtlern kritisiert wird, dass die Grundrechte ohne entsprechende gesetzliche Grundlage sehr stark eingeschränkt wurden, so dass manche Handlungen der Bundesregierung oder der Landesregierungen als verfassungswidrig einzustufen sind. Wie stehen Sie dazu?

Die **Vorsitzende**: Herr Steinhöfel, vier Minuten.

SV **Joachim Nikolaus Steinhöfel**: Fangen wir mal mit den sozialen Medien an. Natürlich sahen sich auch die sozialen Medien durch die Corona-Pandemie mit einer ganz außergewöhnlichen Situation konfrontiert. Ich hatte eingangs schon die Äußerung der YouTube-Chefin Susan Wojcicki bei CNN Ende April 2020 erwähnt, die gesagt hat – ich zitiere sie mal: „Alles, was sich gegen die Empfehlungen und Verlautbarungen der Weltgesundheitsorganisation richtet, werden wir entfernen.“ Man muss sich dabei vor Augen führen, dass die WHO keine demokratisch legitimierte Organisation ist und dass ihr Chef – dessen Abberufung das Repräsentantenhaus der

Vereinigten Staaten heute Morgen verlangt hat, in dem es eine Mehrheit der Demokraten gibt – unter starkem Einfluss Chinas steht und nur mit chinesischer Hilfe überhaupt in diese Position gekommen ist. Diese Mann ist zwei Wochen nach Ausbruch der Pandemie nach China gereist ist, um dort einen Anstandsbesuch zu machen und China für seine transparente Politik im Rahmen der Pandemie zu loben. Wenn diese Organisation dann sozusagen das letzte Wort hat, wenn es darum geht zu entscheiden, was bei YouTube zu medizinisch-wissenschaftlichen Themen veröffentlicht werden darf, dann erfolgt über diesen Weg quasi ein unmittelbarer Eingriff in die Meinungsfreiheit und damit eine Einschränkung dessen, was zu diesen Themen bei YouTube in Deutschland wie im Rest der Welt diskutiert werden darf, wenn der Eingriff weltweit erfolgt. Das ist eine unglaubliche Situation. Sicher werden auch in Deutschland zu dieser Frage jede Menge Verschwörungstheorien verbreitet, und ich habe in diesem Zusammenhang auch Mandatsanfragen bekommen. Sie wollen gar nicht wissen, was da alles als Heilmittel bezeichnet wird – das ist sagenhaft. Also wirklich, da sind die Alu-Hutträger der Welt geschlossen aufgetreten. Aber es gibt natürlich auch wissenschaftliche Dispute, wie etwa den zwischen Drosten und Streeck. Das haben wir alle mitbekommen. In diesem Kontext fällt mir ein, dass Streeck – ich glaube, in der Talkshow von Markus Lanz – gesagt hat, er hätte schon Sorge, seine wissenschaftliche Meinung zu sagen, weil dies einen Shitstorm auslösen könnte. Daraufhin hat der ehrenwerte Wolfgang Kubicki gesagt: „Wenn das so ist, dann haben wir nicht nur ein Meinungsbildungsproblem, sondern dann haben wir ein Demokratieproblem.“ Ich denke, damit hat er Recht. Was Eingriffe in die Grundrechte angeht, hat unser Rechtsstaat sehr gut funktioniert. Die Verfassungsgerichte haben erst eine Weile abgewartet, weil wir es ja mit einer hoch komplizierten, schwierigen Situation mit großen Herausforderungen für den Gesetz- und Verordnungsgeber zu tun hatten. Aber dann hat es Eingriffe des Verfassungsgerichts beim Demonstrationsverbot und Eingriffe verschiedener Landesverfassungsgerichte gegeben. Ich finde, das hat ganz gut funktioniert. Denn in einer solch schwierigen Situation muss man dem Gesetzgeber gegenüber auch ein wenig Nachsicht üben. Dies gilt allerdings nicht für die Regelung, die Ende März 2020 vom Bundestag verabschiedet worden ist, nämlich für § 5 des Infektionsschutzgesetzes, weil dieser Paragraph unzulässiger Weise in Länderkompetenzen eingreift. Damit wird eine Verordnungsbefugnis auf das Gesundheitsministerium übertragen. Das kann nun nach Gutsherrenart, das heißt ohne gesetzliche Kontrolle, und ohne hinreichende Zustimmung der Länder entscheiden, inwieweit hier Ausnahmeregelungen vorgenommen werden dürfen oder nicht. Dies steht meines Erachtens eindeutig im Widerspruch zu Artikel 80 Abs. 1 und 2 des Grundgesetzes. Danke.

Die **Vorsitzende**: Herzlichen Dank. Dann schaue ich Richtung SPD, die hat keine weiteren Fragen. Nighat, ich hoffe, Sie sind noch mit uns verbunden. Ich hätte nämlich noch eine letzte Frage an Sie, kann Sie aber im Moment nicht sehen. Schauen wir einmal, ja, die Verbindung steht noch. Wunderbar, die Verbindung ist gut. Wir haben also vorhin über schrumpfende Räume für Menschenrechtsverteidiger gesprochen. Da Sie jetzt die einzige Sachverständige sind, die nicht aus Deutschland kommt, sondern in einem Umfeld tätig ist, das stärker schrumpft als hier in Deutschland, möchte ich Sie bitten, etwas ausführlicher über die Voraussetzungen zu sprechen, die wir für die Schaffung eines sichereren digitalen Raums insbesondere für die Zivilgesellschaft und die Menschenrechtsverteidiger in Ländern wie Pakistan, aber auch in anderen, mit Pakistan vergleichbaren Ländern in Betracht ziehen müssen. Bitte, Sie haben vier Minuten Zeit für Ihre Antwort.

SVe **Nighat Dad**: Vielen Dank. Ich habe den Eindruck, dass die Gesetzgeber in Pakistan sich oft an europäischen Ländern als „Goldstandard“ und als Inbegriff bewährter Praktiken orientieren. Auch zivilgesellschaftliche Gruppen machen die Menschenrechte über internationale Instrumente wie den GSP+-Status geltend. Ich werde noch einmal auf den von mir bereits erwähnten Punkt zurückkommen, nämlich dass die Übernahme regressiver Gesetze im Globalen Norden eine verheerende Wirkung auf die Überzeugungsarbeit hier in meinem Land haben kann. In der

Vergangenheit haben wir oft erlebt, dass Gesetze in aller Welt gewissermaßen wörtlich aus anderen Gesetzen übernommen wurden. Was die digitalen Rechte betrifft, so hat die Regierung auf Bestimmungen wie den Schutz der Bürger vor Online-Schädigungen, die teilweise an die im Vereinigten Königreich vorgeschlagenen Bestimmungen angelehnt waren, verzichtet. Ich sehe hier einen sehr direkten Zusammenhang zwischen dem, was in Räumen wie diesem geschieht, und den digitalen Rechten weltweit. Ob es uns gefällt oder nicht: Als Erben der globalen Hegemonie und der Wirtschaftsmächte sind die Länder des Globalen Nordens gut dafür aufgestellt, eine weltweite Führungsrolle zu übernehmen und moralisch mit gutem Beispiel voranzugehen. So, wie ich die Auswirkungen auf Minderheiten einschätze, denke ich, dass wir eine Zunahme solcher Gesetze und Politikkonzepte zur Regulierung des Internets nicht nur zu den gewohnten Zeiten beobachten. Vielmehr glaube ich, dass, wenn die Regierungen, insbesondere die Regierungen in den Industrieländern, die fortschrittlichen Regierungen, die demokratischen Regierungen während der Pandemie Maßnahmen einleiten, egal mit welchem Ziel, ob sie damit Überwachungsbefugnisse verstärken oder sich selbst mehr Befugnisse geben, eine Kontrolle und Gegenkontrolle unterbleibt. Ich finde, dass damit sehr schlechte Präzedenzfälle für religiöse Minderheiten in Pakistan, für sexuelle Minderheiten in Pakistan, für Aktivisten, für Journalisten geschaffen werden. Dabei habe ich nicht nur Pakistan im Blick, sondern diesen Teil der Welt, wo der Rechtsstaat bekanntlich schwach ausgeprägt ist, das Justizsystem versagt, unsere Demokratien noch nicht konsolidiert sind. Als jedoch diese Gesetze kamen – ich spreche hier vor allem von Gesetzen, weil ich die Gesetze, die ich sehe, im Zusammenhang mit den Bemühungen um die Regulierung des Internets für sehr problematisch halte –, diese Gesetze, die Regierungen haben es sich zur Gewohnheit gemacht, neue Gesetze zum Schutz der Bürger im Namen der nationalen Sicherheit, des Kampfes gegen den Terrorismus und jetzt des Kampfes gegen die Pandemie zu erlassen. Für mich liegt das Problem auf der Hand: Minderheiten werden durch diese Gesetze nicht geschützt. Eher habe ich den Eindruck, dass sie Selbstzensur üben. Es gibt keine Schutzvorkehrungen, und daher ist die Angst vor Überwachung größer. In Europa haben Sie die Datenschutz-Grundverordnung. In Pakistan haben wir nicht einmal eine Grundnorm für den Datenschutz. Ich halte es also für sehr wichtig, dass die Menschen, die in den Europäischen Parlamenten, in Deutschland, Entscheidungspositionen einnehmen, denn ich wende mich hier an die jeweiligen Parlamentarier, dass Sie bei den Entscheidungen, die Sie treffen, selbst während der Pandemie, sehr aufmerksam prüfen, wie sich das auf die Entscheidungen in unseren Ländern auswirkt. Für Minderheiten ist die Lage schlimm, zumal keine digitale Kompetenz vorhanden ist. Die Menschen wissen nicht einmal, wie sie sich auf den Plattformen in Bezug auf die digitale Sicherheit schützen können: Für mich ist es sehr wichtig, dass wir uns bei der Debatte über die Zugänglichkeit des Internets und all diese Grundrechte im Online-Raum bewusst sind, dass die Allgemeinheit, die Bevölkerung an sich, nicht einmal weiß, was digitale Rechte bedeuten. *

Die **Vorsitzende**: Herzlichen Dank, ich schalte jetzt wieder auf Deutsch um. Jetzt schaue ich zur Fraktion DIE LINKE. Gibt es weitere Fragen? Das ist nicht der Fall. Dann Frau Bause, von Ihrer Seite? Ja, dann haben Sie zwei Minuten Zeit.

Abg. **Margarete Bause** (BÜNDNIS 90/DIE GRÜNEN): Ich habe eine Frage an Herrn Kettemann. Sie haben vorhin das Internet Governance Forum erwähnt, in das sich auch die Zivilgesellschaft einbringen kann. Wie können wir es erreichen, dass sich die Zivilgesellschaft bzw. zivilgesellschaftliche Akteure auch in andere Formate besser einbringen können, um digitale Technologien für den Schutz von zivilgesellschaftlicher Teilhabe nutzbar zu machen?

Die **Vorsitzende**: Herzlichen Dank. Herr Kettemann, Sie haben dann das Wort.

SV Dr. **Matthias C. Kettemann**: Die Zivilgesellschaft kann nur dann entsprechend gefördert werden, wenn alle Akteuren sich überhaupt dessen bewusst sind, dass sie sich hier engagieren können. Wenn wir ehrlich sind, dann

müssen wir zugeben, dass nicht sehr viele Menschen wissen – und zwar sogar nachdem im letzten Jahr das Internet Governance Forum in Berlin mit viel Geld unterstützt wurde –, dass es das Forum überhaupt gibt. Wie viele Ihrer Kolleginnen und Kollegen waren dort, wo es doch nur ein paar Meter von Ihnen entfernt an der Spree stattgefunden hat? In dem Forum geht es wirklich um die Grundfragen der Internetregulierung bzw. um die Grundfragen der Regulierung einer Technologie, die unsere Kommunikation für lange Zeit beeinflussen wird. Das heißt, was können wir wirklich tun? Schauen Sie sich an, wo jetzt gerade die Umstellung auf das digitale Leben ins Stocken geraten ist! Das ist zum Beispiel an den Schulen der Fall. Es ist ein Problem, dass Digitalisierung kein Querschnittsthema in allen Schulfächern ist. Es ist ein Problem, dass das hier noch nicht angekommen ist, auch nicht in der beruflichen Weiterbildung. Es gibt aber einzelne Initiativen; in Hamburg hat man zum Beispiel vor der Corona-Krise damit angefangen, berufsbildende Schulen stärker zu unterstützen. Auch wir vom Leibniz-Institut gehen in die Schulen und fördern die Bewusstseinsbildung bei jungen Menschen, denn hier ist ganz viel Bewusstseinsbildung nötig. Eine Initiative, die zum Beispiel sehr gut ankommt, ist das Youth IGF (Youth Internet Governance Forum), das die Gesellschaft für Informatik initiiert hat. Da werden junge Menschen an das Internet Governance Forum herangeführt. Es muss sich einfach – und das gilt nicht nur für den Bereich Internet – in der Gesellschaft ein Bewusstsein dafür herausbilden, dass man gemeinsam etwas erreichen kann, wenn man sich engagiert. Da man sich heute über das Internet so schnell in Entscheidungsprozesse einbringen kann, haben wir jetzt die Chance, dass dies jeder, der dies will, auch tun kann, sofern er die Unterstützung erhält, die er dafür benötigt. Dafür muss man natürlich auch etwas Geld in die Hand nehmen; aber wenn man das tut, dann kann man die Legitimation der politischen Entscheidungsbildung in Zukunft erhöhen. Danke sehr.

Die **Vorsitzende**: Herzlichen Dank. Sie haben Zeit für eine weitere Frage. Das Wort hat Herr Gehring. – Das ging jetzt wahrscheinlich zu schnell jetzt. Herr Gehring, sind Sie noch dabei? Sie hätten jetzt direkt das Wort. Wir verstehen Sie ganz schlecht, muss ich sagen, zumindest hier im Ausschussraum, als hätten Sie etwas vor dem Mikrophon. – Jetzt ist es besser.

Abg. **Kai Gehring** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank. Da Sie, Herr Kettemann, auch über den internationalen Kontext gut Bescheid wissen, hätte ich noch die Frage an Sie, welche Länder aus Ihrer Sicht beim Schutz von digitalen Bürgerrechten weltweit führend sind. Wir haben hier bis jetzt viel über die Regulierungsmechanismen gesprochen, die wir auf europäischer und internationaler Ebene anwenden sollten. Aber wir fragen uns natürlich immer wieder, welche Länder wir uns zumindest ein Stück weit für eine Regulierung hierzulande zum Vorbild nehmen könnten.

Die **Vorsitzende**: Herr Dr. Kettemann, Sie haben das Wort.

SV Dr. **Matthias C. Kettemann**: Wenn man sich die Bewertungen von internationalen NGOs wie Internet Freedom Watch anschaut, dann erkennt man, dass im Bereich der digitalen Grundrechte sozusagen die üblichen Verdächtigen sehr gut abschneiden. Dazu gehören die nordischen Staaten – sie rangieren immer recht weit oben –, aber auch Staaten wie Kanada. Ich denke nur, dass wir hier konkreter werden müssen. Deutschland und Frankreich sind zum Beispiel zwei Staaten mit einem guten Track Record im Bereich der Bürgerrechte. Gleichwohl werden sowohl Frankreich als auch Deutschland dafür kritisiert, dass sie mit dem Netz-DG im Falle Deutschlands bzw. mit dem aktuellen Avia-Gesetz im Falle Frankreichs einen Weg eingeschlagen haben, der im globalen Zusammenhang missinterpretiert werden kann. Das heißt, wir müssen uns einzelne Initiativen anschauen und jeweils überprüfen, ob sie geeignet sind. Und ich denke, das können wir tun, indem wir fragen, was wirklich funktioniert. So funktioniert etwa in der Schweiz die Integration der Zivilgesellschaft in die Internetregulierung phantastisch. Dort ist die Zusammenarbeit der Behörden mit der Zivilgesellschaft sehr gut. Die Integration der Wissenschaft in die Politikentwicklung im

Bereich Internet und Internetrechte funktioniert in Schweden sehr gut. Und Finnland zeichnet sich dadurch aus, dass dem Internet und der digitalen Welt schon in der schulischen Ausbildung breiter Raum eingeräumt wird. Aber auch in Deutschland gibt es großartige Initiativen, die Unterstützung verdienen. So beginnt zum Beispiel in ein paar Tagen eine Initiative, bei der sich die Bundesbeauftragte für Medien im Rahmen der europäischen Ratspräsidentschaft Deutschlands gemeinsam mit Wissenschaftlerinnen und Wissenschaftlern mit der Frage auseinandersetzt, welche neuen Wege in der Medienordnung beschritten werden müssen. Das hat auch ganz konkrete Auswirkungen auf das Internet. Das heißt, kein einzelner Staat macht alles richtig, aber viele Staaten haben gute Ideen; auch aus Deutschland stammen gute Ideen. Schauen wir uns an, welche funktionieren!

Die **Vorsitzende**: Herzlichen Dank, Herr Dr. Kettemann. Das war ein schöner Schlusssatz. Ich möchte ihn aufgreifen, um mich erst einmal bei Ihnen allen ganz herzlich für die Statements und ganz generell für die Arbeit, die Sie in Ihre Vorbereitung gesteckt haben, zu bedanken. Ich würde zusammenfassend sagen wollen, dass es zum Ende hin noch einmal besonders spannend geworden ist. Das ist bei unseren Anhörungen sehr häufig der Fall. Denn zu Beginn stellt jeder die Fragen, die vorbereitet worden sind, während zum Ende hin deutlich wird, wo tatsächlich der „Hase im Pfeffer liegt“. Was ich für mich mitnehme, ist die Botschaft – und ich hoffe, das gilt ein Stück weit auch für Sie alle –, wie wichtig Bildung ist und welch große Bedeutung sie für verschiedene Bereiche, auch für den Schutz von Menschenrechten besitzt und welch weitreichende Auswirkungen vor allem die digitale Bildung hat, nicht nur hier bei uns in Deutschland, sondern auch in vielen anderen Ländern. Umgekehrt zeigt sich, wie manche Staaten, vor allem repressive Regime, den Mangel an Bildung in diesem Bereich – dies hat ja auch Nighat Dad aus Pakistan berichtet – ausnutzen, um die Bevölkerung zu manipulieren. Ich denke, eine Erkenntnis können wir alle vielleicht von hier mitnehmen und in die weitere programmatische Arbeit und auch in unsere Anträge oder Stellungnahmen hier in diesem Ausschuss einfließen lassen, nämlich dass Bildung am Ende für die Frage, was Menschenrechtsbildung vor Ort bedeutet, ein sehr wichtiger Aspekt ist und einen hohen Stellenwert haben muss, wenn wir erfolgreich dazu beitragen wollen, dass Menschenrechte universell gelten. Ich möchte es dabei bewenden lassen und mich bei Ihnen hier im Saal, aber auch bei allen, die die Möglichkeit genutzt haben, sich über WebEx zuzuschalten, ganz herzlich bedanken. Vielen Dank auch an das Ausschusssekretariat für die sorgfältige Vorbereitung der etwas anderen Ausschussanhörung, die wie immer reibungslos abgelaufen ist. Es hat alles wunderbar geklappt, vielen Dank. Und ein ganz besonderes Dankeschön nach Pakistan. Nighat, haben Sie vielen Dank, dass Sie zu uns gestoßen sind. Vielleicht konnten Sie ein paar Worte Deutsch lernen, und es wäre schön, wenn wir uns bei anderer Gelegenheit persönlich kennenlernen würden. Vielen Dank an alle, und einen schönen Abend noch. Ich schließe die Sitzung.

***** *Die Wortbeiträge der Sachverständigen Nighat Dad wurden vom Sprachendienst des Deutschen Bundestages aus dem Englischen ins Deutsche übersetzt.*

Schluss der Sitzung: 16:54 Uhr

Gyde Jensen, MdB
Vorsitzende