HEINRICH BÖLL STIFTUNG
Die grüne politische Stiftung

Policy Brief

Intersektionale feministische Perspektiven auf die Gesetzgebung zur Bekämpfung von Cyberkriminalität

VON VIVIENNE KOBEL UND PAVLINA PAVLOWA

Herausgegeben vom Gunda-Werner-Institut und der Globalen Einheit für Menschliche Sicherheit in der Heinrich-Böll-Stiftung, Oktober 2025

Intersektionale feministische Perspektiven auf die Gesetzgebung zur Bekämpfung von Cyberkriminalität

Von Vivienne Kobel und Pavlina Pavlowa

Inhaltsverzeichnis

Liste der Abkürzungen

AHC	Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes/Ad-hoc-Ausschuss zur Ausarbeitung einer umfassenden internationalen Konvention zur Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien für kriminelle Zwecke
CFFP	Centre for Feminist Foreign Policy/Zentrum für feministische Außenpolitik
CSAM	Child Sexual Abusive Material/Abbildungen sexuellen Kindesmissbrauchs
EU	Europäische Union
IKT	Informations- und Kommunikationstechnologie
KI	Künstliche Intelligenz
NCIID	Non-Consensual Intimate Image Distribution/nicht einvernehmliche Verbreitung intimer Bilder
NCSII	Non-Consensual Dissemination of Intimate Images/nicht einvernehmliches Teilen intimer Bilder
NGO	Non-Governmental Organisation/Nichtregierungsorganisation
NISSA	National Authority for Information Security and Safety/Nationalen Behörde für Information und Sicherheit
TFGBV	Technology-Facilitated Gender-Based Violence/technologiegestützte geschlechtsspezifische Gewalt
UNCAC	United Nations Convention against Corruption/UN-Konvention gegen Korruption
UNTOC	United Nations Convention against Transnational Organized Crime and the Protocols thereto/UN-Konvention gegen die grenzüberschreitende organisierte Kriminalität

Vorwort

Die internationale Strafverfolgung von organisiertem Verbrechen und Kriminalität war bis zu dieser Publikation noch Neuland für die außen- und sicherheitspolitische Arbeit der Heinrich-Böll-Stiftung. Mit unserer im Jahr 2023 gestarteten Globalen Einheit für Menschliche Sicherheit in Wien, am Sitz des Büros der Vereinten Nationen für Drogen- und Verbrechensbekämpfung (UNODC), besteht nunmehr die Chance, sich diesem Thema aus grüner Perspektive anzunehmen.

Cyberkriminalität und organisiertes Verbrechen im Internet nehmen besonders rasant zu und entwickeln sich dabei laufend weiter. Eine UN-Konvention zur Bekämpfung von Cyberkriminalität, die Ende Oktober 2025 feierlich in Hanoi unterzeichnet werden soll, verfolgt zwar das Ziel, transnationale digitale Bedrohungen einzudämmen, doch ihr weit gefasster Anwendungsbereich wirft ernsthafte Bedenken auf, denn zu groß sind die Möglichkeiten von Missbrauch und staatlicher Übergriffe. In einer Welt, in der die Handlungsräume für die Zivilgesellschaft immer enger werden und Populisten wie Donald Trump eine anti-feministische Agenda verfolgen, werden Social-Media-Plattformen oder Messengerdienste oft dazu genutzt, Aktivist*innen auszuspähen, Zugang zu Informationen zu sperren oder Desinformation zu streuen.

Aus Mangel an den nötigen Ressourcen spielen in vielen feministischen Bewegungen digitale Rechte und Freiheiten immer noch eine untergeordnete Rolle. Ein Grund für uns, dieses auf Englisch in Zusammenarbeit mit dem Centre for Feminist Foreign Policy (CFFP) erschienene Policy Brief zu übersetzen und einer breiteren Leser*innenschaft zugänglich zu machen. Denn wie immer bei neuen völkerrechtlichen Vereinbarungen wird es jetzt auf die Umsetzung der UN-Cybercrime-Konvention auf Ebene der EU und Nationalstaaten ankommen; eine fortlaufend kritische Begleitung durch die Zivilgesellschaft ist dabei entscheidend.

Als feministische Zivilgesellschaft müssen wir auf das Recht auf Verschlüsselung und öffentlich, aber nicht staatlich kontrollierter Kommunikation im digitalen Raum pochen. Wir müssen voneinander lernen, was Kontrolle und Überwachung im Digitalen eigentlich meint und warum wir dieses Thema nicht getrennt von anderen feministischen Anliegen betrachten können. Digitalpolitik ist Gesellschaftspolitik, und diese Gesellschaft braucht feministische Akteur*innen, um gegen die Angriffe der autoritären Rechten bestehen zu können.

Berlin, im Oktober 2025

Katharina Klappheck
Gunda-Werner-Institut,
Heinrich-Böll-Stiftung

Simon Ilse
Globale Einheit Menschliche Sicherheit,
Heinrich-Böll-Stiftung

Zusammenfassung

Die zunehmende globale Abhängigkeit von digitalen Technologien macht Cyberkriminalität nicht bloß zu einer Bedrohung für technische Systeme, sondern kann sowohl Einzelnen als auch der Gesellschaft insgesamt schaden, wenn sie zum Ziel cyberkrimineller Aktivitäten werden. Frauen, LGBTQIA+, Journalist*innen, Menschenrechtler*innen und andere Gruppen, die aufgrund von Geschlecht, Race, Sexualität oder anderen (sich überschneidenden) Identitätsmarkern politisch und/oder historisch Marginalisierung erfahren, sind davon oft stärker und auf besondere Weise betroffen. Damit verschärft Cyberkriminalität bereits existierende soziale und systemische Ungleichheiten und patriarchale Strukturen. Zudem können jene Gruppen, die Cyberkriminalität am schutzlosesten ausgesetzt sind, unter dem Vorwand von Gesetzen zu deren Bekämpfung Ziel von staatlichem Machtmissbrauch werden. Vor diesem Hintergrund stellt dieses Positionspapier heraus, dass die nationale und internationale Gesetzgebung zur Bekämpfung von Cyberkriminalität einer aufmerksamen Prüfung aus intersektional feministischer Perspektive unterzogen werden sollte, um staatlichem Missbrauch vorzubeugen.

Während der Verhandlungen zur UN-Konvention gegen Cyberkriminalität haben verschiedene Interessengruppen wiederholt ähnliche Bedenken geäußert, insbesondere bezüglich der verstärkten internationalen Zusammenarbeit zur Bekämpfung von Straftaten, die mithilfe von Informations- und Kommunikationstechnologie (IKT) begangen werden, sowie zum Austausch elektronischer Beweismittel bei schweren Straftaten. Die UN-Konvention soll zwar der Bekämpfung transnationaler Cyberkriminalität dienen, kritisiert wurde aber ihr breit definierter Geltungsbereich, der autoritären Staaten Übergriffe ermöglicht und damit (digitale) Menschenrechte und Freiheit gefährden könnte. Dieses Positionspapier will die Grundlage für eine von einem intersektional feministischen Ansatz geprägte menschenrechtskonforme Umsetzung der UN-Konvention gegen Cyberkriminalität legen.

Zunächst sollen die unterschiedlichen und geschlechtsspezifischen Auswirkungen von Cyberkriminalität auf marginalisierte Individuen und Communitys untersucht werden, wobei ein Schwerpunkt auf dem notwendigen intersektional feministischen Ansatz liegt (Kapitel 2 und 3). Danach erfolgt eine Einschätzung, wie einzelne Staaten nationale Gesetzgebung zur Bekämpfung von Cyberkriminalität dazu genutzt haben, um (digitale) Menschenrechte und Freiheit zu beschränken, Meinungsfreiheit zu unterdrücken und eine autoritäre und antifeministische Agenda durchzusetzen (Kapitel 4). Mithilfe der Erkenntnisse aus nationalen Kontexten wird die UN-Cyberkriminalitätskonvention danach unter Aspekten der Geschlechtergerechtigkeit und Menschenrechte bewertet (Kapitel 5), wobei sowohl Hauptrisiken/-gefahren als auch Chancen herausgearbeitet werden.

Ergebnisse:

- Die UN-Konvention gegen Cyberkriminalität enthält in einigen Kapiteln Bestimmungen zu Geschlechtergerechtigkeit und betont die Bedeutung der Bekämpfung geschlechtsspezifischer Gewalt im digitalen Raum.
- Im Abkommen wird jedoch versäumt, breitere geschlechtersensible und -gerechte Ansätze aufzunehmen und eine aktive Förderung der Gleichstellung der Geschlechter in allen Bestimmungen festzuschreiben.
- Insbesondere in Bezug auf den internationalen Austausch elektronischer Beweismittel und verfahrensrechtliche Befugnisse birgt der breite Anwendungsbereich der UN-Konvention gegen Cyberkriminalität das Risiko, als allgemeines Abkommen über Datenzugriffe verwendet zu werden. Aufgrund unzureichender Maßnahmen zum Schutz von Menschenrechten und Daten umfassen mögliche Menschenrechtsverletzungen daher die gezielte Verfolgung marginalisierter Gruppen und vulnerabler Personen.
- Die weitreichenden Bestimmungen zur gegenseitigen Rechtshilfe des Abkommens bergen das Risiko, dass autoritäre Staaten die internationale Zusammenarbeit für repressive Ermittlungen missbrauchen, indem sie unter diesem Vorwand Schutzvorkehrungen gegen staatliche Übergriffe und geheime Erhebung von Daten abschwächen.
- Der im Abkommen festgelegte Kompetenzrahmen könnte die Tür für die Aufnahme inhaltsbezogener Vergehen öffnen, die z. B. mit Extremismus und Terrorismus oder der Verbreitung von Falschinformationen in Zusammenhang gestellt werden können. Diese hoch subjektiv auslegbaren Begriffe dienen autoritären Staaten häufig zur Rechtfertigung von Repressionen und der Verletzung von Meinungsfreiheit.
- Die UN-Konvention gegen Cyberkriminalität umfasst auch den Kampf gegen Abbildungen sexuellen Kindesmissbrauchs (CSAM – Child Sexual Abusive Material). Besonders angesichts der langfristigen, verheerenden Auswirkungen für die Überlebenden und der Häufigkeit dieses Verbrechens hat der Kampf gegen CSAM oberste Priorität. Dennoch könnten diese Maßnahmen unbeabsichtigte Konsequenzen nach sich ziehen, z. B. die Kriminalisierung von Minderjährigen aufgrund selbst erzeugter sexuell expliziter Inhalte.
- Die Berücksichtigung nicht einvernehmlich geteilter intimer Bilder (NCSII – Non-Consensual Dissemination of Intimate Images) markiert einen wichtigen Schritt im Kampf gegen geschlechtsspezifische Gewalt. Dadurch werden internationale Bemühungen zur Prävention, Ermittlung und Verfolgung von bildbasierter sexualisierter Gewalt gestärkt und gleichzeitig die internationale Zusammenarbeit zwischen Regierungen, Online-Plattformen und der Zivilgesellschaft gefördert, um Betroffene zu schützen und Täter*innen zur Verantwortung zu ziehen.

- Obwohl die UN-Konvention gegen Cyberkriminalität die Schutzbedürftigkeit von Betroffenen und Zeug*innen berücksichtigt, verweisen die entsprechenden Regelungen auf innerstaatliche Gesetze, die möglicherweise keine effektiven Schutzmaßnahmen vorsehen, so dass vor allem Betroffene mit erschwertem Rechtszugang keine juristischen Garantien auf Unterstützung, Schutz oder Zufluchtsorte erhalten.
- Die zukünftige Wirkung der UN-Konvention gegen Cyberkriminalität wird davon abhängen, wie Staaten das Abkommen umsetzen bzw. die Bestimmungen in den nationalen Rahmen übertragen. Das Abkommen wird aber nicht nur die nationale Gesetzgebung zur Bekämpfung von Cyberkriminalität beeinflussen, sondern auch die internationale Strafverfolgung, Verfahrensbefugnisse und die allgemeine staatenübergreifende Zusammenarbeit zur Prävention und Bekämpfung von Cyberkriminalität.
- Zivilgesellschaft und Menschenrechtsorganisationen müssen die transparente, inklusive und menschenrechtskonforme Umsetzung und deren Ergebnisse gezielt kontrollieren und bewerten.

In diesem Positionspapier werden eine Reihe zentraler Empfehlungen für Staaten formuliert, die vor allem im Kontext der UN-Konvention gegen Cyberkriminalität sicherstellen sollen, dass entsprechende Gesetze die Menschenrechte wahren, marginalisierte Communitys und vulnerable Individuen schützen sowie freie und gerechte digitale Gesellschaften befördern (Details s. S. 50–57):

1. Verschiedene Interessengruppen aktiv in Diskussionen und Beratungsprozesse zur Unterzeichnung und Verabschiedung der UN-Konvention gegen Cyberkriminalität einbinden und an entsprechender Stelle in Gespräche zur zukünftigen Umsetzung des Abkommens beteiligen.
2. Überprüfen, ob die Unterzeichnung der UN-Konvention gegen Cyberkriminalität mit der Verpflichtung zur Wahrung von Menschenrechten, Grundfreiheiten und anderen (politischen) Verpflichtungen vereinbar ist.
3. Bestehende Richtlinien und Maßnahmen zum Schutz von Menschenrechten bei der Umsetzung der Konvention einhalten. Ihre engmaschige Kontrolle sollte u. a. auf Grundlage von angemessenen, effektiven und inklusiven Bewertungsmechanismen und anderen Maßnahmen zum Schutz von Menschenrechten durchgeführt werden, die gemeinsam mit den relevanten Interessengruppen ausgearbeitet werden.
4. Eine intersektional feministische Perspektive auf Cyberkriminalitätsgesetze in (zukünftigen) nationalen und internationalen Standardisierungsprozessen und Diskussionsforen befördern, bei Inkrafttreten vor allem im Rahmen der Vertragsstaatenkonferenz der UN-Konvention gegen Cyberkriminalität.
5. In der Umsetzung der UN-Konvention gegen Cyberkriminalität auf nationaler Ebene und bei der entsprechenden Ausarbeitung/Anpassung der nationalen Gesetzgebung

zu Cyberkriminalität durchgängig Geschlechtergerechtigkeit berücksichtigen und nach intersektional feministischen Gesichtspunkten auch in Zusammenarbeit mit der (feministischen) Zivilgesellschaft und anderen Interessengruppen bewerten.

6. Den Ausbau von Kompetenzen, Zugang zum Recht und geschlechtssensible, betroffenenorientierte Unterstützung für Betroffene von Cyberkriminalität und staatlicher Willkür fördern und finanziell unterstützen.

7. Unabhängige und interdisziplinäre Forschung unterstützen, insbesondere feministische Wissenschaftler*innen und zivilgesellschaftliche (feministische) Arbeiten zu Cyberkriminalität und diesbezüglicher Gesetzgebung.

1 Einleitung

Laut Präambel der UN-Konvention gegen Cyberkriminalität «birgt Informations- und Kommunikationstechnik zwar ein enormes Potenzial für gesellschaftliche Entwicklungen, gleichzeitig eröffnet sie Kriminellen jedoch neue Möglichkeiten und könnte durch eine Steigerung und Ausdifferenzierung krimineller Aktivitäten einen schädlichen Einfluss auf Staaten [und Gesellschaften] haben» (United Nations General Assembly 2024a).

Mit zunehmender Abhängigkeit von digitalen Technologien hat auch **Cyberkriminalität immer größeren Einfluss auf das Wohlergehen von Individuum und Gesellschaft.** Während aber jede*r Einzelne zum Ziel cyberkrimineller Aktivitäten werden kann, **sind nicht alle gleichermaßen davon betroffen:** Einzelpersonen, Gruppen und Communitys, die politisch und/oder historisch aufgrund von Geschlecht, Race, Sexualität, sozioökonomischem Status usw. marginalisiert werden, trifft Cyberkriminalität meist häufiger und auf besondere Weise. Darüber hinaus können **Gesetze gegen Cyberkriminalität zur Durchsetzung einer repressiven antifeministischen Agenda missbraucht** werden. Unter dem Vorwand der Cyberkriminalitätsbekämpfung haben autoritäre Regime sowie schwache Demokratien **Gesetze gegen Cyberkriminalität dazu genutzt, Menschenrechte zu untergraben, Kritik zu unterdrücken und kritische Berichterstattung zu verhindern.** Meist sind für Cyberkriminalität besonders vulnerable Gruppen auch am härtesten von staatlichen Übergriffen auf Basis von Cyberkriminalitätsgesetzen betroffen. Durch diese doppelte Belastung wird ihnen der Zugang zu Menschenrechten, Grundfreiheiten sowie gesellschaftlicher und politischer Teilhabe verwehrt, mit weitreichenden Folgen für die Demokratie.

Diese und andere Überlegungen zu Menschenrechtsaspekten kamen während der Verhandlungen der **UN-Konvention zur Bekämpfung von Cyberkriminalität zur Sprache, die sich im Untertitel der entsprechenden Resolution der «Stärkung der internationalen Zusammenarbeit zur Bekämpfung bestimmter Straftaten, die mithilfe von Informations- und Kommunikationssystemen begangen werden, sowie de[m] Austausch elektronischer Beweismittel in schweren Strafsachen» verschreibt.**[1] Das erste UN-Abkommen zu Cyberkriminalität hält in der Präambel fest, «dass der Gebrauch von Informations- und Kommunikationssystemen einen beträchtlichen Einfluss auf die Schwere, die Geschwindigkeit und die Reichweite von kriminellen Vergehen haben kann» (United Nations General Assembly 2024a). Außerdem wird in der Konvention «die wachsende Zahl von Betroffenen und die Dringlichkeit, mit der diesen Betroffenen Gerechtigkeit widerfahren soll, ebenso anerkannt wie die Notwendigkeit, bei Maßnahmen zur Prävention und Bekämpfung von [Cyberkriminalitäts-]Delikten die Bedürfnisse vulnerabler Personen zu berücksichtigen» (ebd.). Ein weiteres Ziel ist die «Stärkung der internationalen Zusammenarbeit für die

1 Der vollständige Text findet sich im Anhang der Resolution der UN-Generalversammlung *A/RES/79/243*.

effizientere Prävention und Bekämpfung solcher Aktivitäten auf nationaler, regionaler und internationaler Ebene» (ebd.). Während der Verhandlungen haben Menschenrechtsorganisationen, die Zivilgesellschaft, die Privatwirtschaft, die Wissenschaft und Technologie-Expert*innen ebenso wie viele Staaten den Vertragstext scharf kritisiert, u. a. aufgrund des starken Fokus auf Kriminalisierung. Trotz der zahlreichen Einwände[2] wurde die UN-Konvention gegen Cyberkriminalität am 8. August 2024 durch eine Konsensentscheidung des AHC[3] verabschiedet und am 24. Dezember 2024 von der Generalversammlung der Vereinten Nationen bestätigt (UN News 2024).

Aufbauend auf der Kritik zahlreicher zivilgesellschaftlicher Organisationen, darunter auch des CFFP (Centre for Feminist Foreign Policy/Zentrum für feministische Außenpolitik), sollte eine Diskussion unter Berücksichtigung intersektional feministischer Aspekte und Grundätze angeregt werden, die einer menschenrechtskonformen Umsetzung der UN-Konvention gegen Cyberkriminalität den Weg ebnet. Dieses Positionspapier soll dazu ein erster Schritt sein. Die darin vorgelegte Analyse umfasst drei Stufen: Zunächst werden geschlechtsspezifische und gesellschaftliche Auswirkungen von Cyberkriminalität analysiert. Danach wird untersucht, wie nationale Gesetzgebung zur Bekämpfung von Cyberkriminalität missbraucht wird. Im letzten Abschnitt werden Erkenntnisse und Empfehlungen für die Ausarbeitung zukünftiger Gesetze gegen Cyberkriminalität und besonders für die Umsetzung der UN-Konventionen abgeleitet. In diesem Bericht:

- werden **geschlechtsspezifische und gesellschaftliche Auswirkungen von Cyberkriminalität** auf vulnerable und marginalisierte Individuen und Gruppen im Fokus von Cyberattacken untersucht, um die Notwendigkeit einer intersektional feministischen Gesetzgebung herauszuarbeiten (Kapitel 2),
- werden die **wichtigsten Aspekte einer intersektional feministischen Perspektive auf Cyberkriminalitätsgesetze** vorgestellt (Kapitel 3),
- werden die **Risiken, die mit Cyberkriminalitätsgesetzen einzelner Staaten einhergehen, analysiert** und **die Rolle bewertet, die antifeministischen und autoritären Kräften dabei zukommt** (Kapitel 4),

2 Siehe beispielsweise die folgenden Stellungnahmen, in denen UN-Mitgliedstaaten aufgefordert werden, das UN-Übereinkommen gegen Cyberkriminalität in der UN-Generalversammlung abzulehnen und/oder nicht zu ratifizieren: 29 NGOs verfassten einen *gemeinsamen Brief an die EU*; AI Sur, ein Verband zivilgesellschaftlicher Organisationen und wissenschaftlicher Einrichtungen, veröffentlichte einen *offenen Brief an lateinamerikanische Staaten*; der Beirat der Freedom Online Coalition (FOC) sprach proaktiv *Empfehlungen an die FOC-Mitgliedstaaten* aus; und die Internationale Handelskammer veröffentlichte eine *Stellungnahme an Regierungen*.

3 AHC steht für Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (Ad-hoc-Ausschuss zur Ausarbeitung einer umfassenden internationalen Konvention zur Bekämpfung der Nutzung von IKT für kriminelle Zwecke).

- wird die **UN-Konvention gegen Cyberkriminalität** aus einem feministischen und geschlechtergerechten Blickwinkel auf potenzielle Risiken und Chancen untersucht (Kapitel 5),
- und es werden **Empfehlungen zur rechtsverbindlichen Umsetzung** einer menschenrechtskonformen UN-Konvention gegen Cyberkriminalität sowie für eine Gesetzgebung auf nationaler Ebene ausgesprochen, die menschenrechtskonform und nach geschlechtersensiblen Punkten erarbeitet und umgesetzt wird (Kapitel 6).

In diesem Positionspapier werden verschiedene negative Auswirkungen von sowohl Cyberkriminalität als auch von nationaler Gesetzgebung zu ihrer Bekämpfung erörtert. Wenn möglich, werden zur Veranschaulichung der Analysen und Ergebnisse ein oder mehrere Beispiele aus unterschiedlichen Ländern herangezogen. Diese haben keinen Anspruch auf Vollständigkeit, sondern sind vielmehr als Schlaglichter zu verstehen. Die Auswahl der Fälle erfolgte nicht aufgrund geografischer Präferenz (und/oder anderer Formen von Bias).

Dieses Positionspapier hat die Auswirkungen von Gesetzten gegen Cyberkriminalität und deren staatlichen Missbrauch zum Thema (vor allem in autoritären Staaten und schwachen Demokratien). Nicht zu vernachlässigen ist aber, dass sowohl in autoritären als auch demokratischen Staaten die Achtung vor Menschenrechten on- und offline alarmierend schnell abnimmt (Amnesty International 2024a). Außerdem wird die Internetfreiheit weltweit zunehmend beschnitten (Freedom House 2024). Es ist davon auszugehen, dass dieser anhaltende Trend der Polarisierung, des Demokratieabbaus und der Autokratisierung (Nord et al. 2024) in Kombination mit technischem Fortschritt die Folgen von Cyberkriminalität und repressiven/missbräuchlichen Gesetzen gegen Cyberkriminalität noch verschärfen wird – vor allem für marginalisierte Personen sowie für demokratische Strukturen und die allgemeinen Rahmenbedingungen für Menschenrechte.

2 Zu differenzierende Folgen von Cyberkriminalität und Gesetzen zu ihrer Bekämpfung

Zunächst werden Fachbegriffe definiert, bevor die verschiedenen Folgen von Cyberkriminalität und den Gesetzen zu ihrer Bekämpfung zusammengefasst werden, worauf aufbauend in Kapitel 3 eine intersektional feministische Perspektive auf die Gesetzgebung gegen Cyberkriminalität entwickelt wird. Genauere Definitionen werden in den jeweiligen Infoboxen zur Verfügung gestellt.

Was ist Cyberkriminalität?

Es gibt keine international anerkannte Definition von Cyberkriminalität. Tatsächlich haben die «politischen Erwägungen zur Abgrenzung des Konzepts [der Cyberkriminalität]» (Hansel & Silomon 2023: 9) auf nationaler und internationaler Ebene eine bedeutende Rolle in den Bemühungen gespielt, eine Gesetzgebung im Kampf gegen Cyberkriminalität zu etablieren. Sofern nicht anders vermerkt, wird in diesem Text eine breite Definition von Cyberkriminalität verwendet und daher länderspezifische Kontexte beleuchtet, die sich sowohl auf «computerabhängige»[4] als auch «computergestützte»[5] Straftaten beziehen (zu denen auch «content-related offences» zählen, also die Verbreitung rechtswidriger digitaler Inhalte, s. Kapitel 4). Außerdem werden die Begründung, Ausgestaltung und Umsetzung gesetzgeberischer Maßnahmen auf nationaler und internationaler Ebene untersucht. Vor allem aus einer intersektional feministischen Perspektive wäre eine engere Definition nicht zielführend, da «geschlechtsspezifische Cyberangriffe die von der Cybersicherheitscommunity definierten gängigen Unterscheidungen zwischen computerabhängigen und computergestützten Bedrohungen und Risiken überschreiten» (Shires, Hasib & Swali 2024: 8).

4 Cyber-dependent: Computerkriminalität im engeren Sinn, also Straftaten, bei denen Angriffe auf Datenbestände oder Computersysteme unter Ausnutzung von IKT begangen werden.

5 Cyber-enabled: Computerkriminalität im weiteren Sinn, also Straftaten, bei denen IKT zur Planung, Vorbereitung oder Ausführung eingesetzt wird.

Ein kurzer Überblick über verschiedene Definitionen von Cyberkriminalität

Von den über 160 Staaten, die Gesetze zur Bekämpfung von Cyberkriminalität verabschiedet haben (UNODC o. D.), verwenden manche eine enge Definition von **computerabhängigen Verbrechen**, also solche, die ausschließlich mittels Computern, Netzwerken oder anderen digitalen Technologien verübt werden (z. B. unerlaubter Zugang zu Systemen, Verbreitung von Ransomware, also Erpressungssoftware, oder Denial-of-Service-Angriffe (DoS), die es ohne Cybertechnologie nicht geben würde). Weiter gefasste Definitionen beinhalten auch **computergestützte Verbrechen**, also «herkömmliche» Verbrechen, bei denen digitale Technologie genutzt wird, um Reichweite, Umfang und Effizienz zu erhöhen, die aber nicht vollkommen vom digitalen Raum abhängig sind. Darunter fallen beispielsweise computergestützter Betrug, Online-Stalking und -Belästigung. Eine dritte Cybercrime-Kategorie, die viele Staaten unter computergestützter Kriminalität einordnen, sind sogenannte **«content-related offences»** (inhaltsbezogene Vergehen), also die Verbreitung rechtswidriger digitaler Inhalte. Dazu zählen die Herstellung, Verbreitung oder das Hosten illegaler oder schädlicher Inhalte im digitalen Raum, z. B. auf Online-Plattformen. Je nach Staat fällt darunter auch die Verbreitung von Abbildungen sexuellen Kindesmissbrauchs (CSAM), das nicht einvernehmliche Teilen intimer Bilder (NCSII), die Verbreitung von Hassrede oder der Aufruf zum Terrorismus sowie die «Beleidigung und Diffamierung von Religion oder religiösen Werten, die Gefährdung der Sitten und die Verbreitung von Fakenews/Falschinformationen» (Hakmeh & Saunders 2024).[6]

Die Online-Welt ist eine Erweiterung der Offline-Welt. In vielerlei Hinsicht verstärken Online-Räume bereits existierende Machtungleichheit, Bias, diskriminierendes Verhalten und missbräuchliche Strukturen (s. Bernarding & Kobel 2023). Die durch Cyberkriminalität verursachten Schäden können Überschneidungen mit patriarchalen und misogynen Strukturen aufweisen. Geschlecht[7] und intersektionale Identitätsmarker wie Race,

6 Dieser Infokasten wurde auf Basis von McGuire und Dowling (2013), UNODC Education for Justice (o. D.) und Sarre et al. (2018) erstellt. Eine ausführliche Übersicht über unterschiedliche Begriffe und Typen von Cyberkriminalität sowie deren digitale Beweismittel findet sich bei Kävrestad et al. (2024). Eine Literaturübersicht und Fallbeispiele zu insbesondere cyberabhängigen Straftaten bietet Maimon und Louderback (2019).

7 In diesem Positionspapier wird Gender als soziales Konstrukt definiert, das ein nicht binäres Spektrum beschreibt und durch Politik, Medien, Familienstrukturen, Religion, Gesetze usw. bestimmt wird. Gender konzeptualisiert Vorstellungen, die sich auf gesellschaftlich erwartetes, akzeptiertes und sanktioniertes Verhalten bzw. soziale Normen auswirken. Gender als Mittel, um Machthierarchien und strukturelle Ungleichheit unter Menschen, Gemeinschaften und Staaten zu zementieren, bestimmt die individuelle gesellschaftliche Stellung und Rolle Einzelner (CFFP Glossary 2021). In diesem Positionspapier (und darüber hinaus) meint Gender niemals nur «Frauen», sondern auch Männer und alle anderen Personen.

Sexualität, sozioökonomischer Status und Beruf haben demnach einen entscheidenden Einfluss auf Charakter, Form, Schwere und Wirkungsdauer des zugefügten Schadens.

Der intersektionale und kontextuelle Charakter (geschlechtsspezifischer) Cyberangriffe und dessen verstärkende Folgewirkung

Geschlechtsspezifische Cyberangriffe sind nicht nur **intersektional**, sondern auch **kontextuell**. Wie Pavlova (2024) darlegt, «beeinflussen gesellschaftliche und rechtliche Rahmenbedingungen, Geschlechterrollen und -normen, die Gesellschaft und Staat auferlegen, der Zugang zu staatlichen Leistungen, die sozialen und Familienstrukturen und die Umgebung […] zusätzlich die Art, die Wahrscheinlichkeit und die Schwere des erlittenen Schadens.» Ein weiterer Mechanismus, der geschlechtsspezifische Angriffe im digitalen Raum verstärkt, ist die Wechselwirkung zwischen verschiedenen Arten von Schädigungen, wie sie Shires, Hassib und Swali (2024) anhand von Hassrede, Datenschutzverletzung und staatlichem Übergriff beschreiben. Letzteres meint geschlechtsspezifische Schädigungen im digitalen Raum, die «auf die staatliche Anwendung von Richtlinien und Gesetzen zurückgehen, mit denen bestimmte staatskonforme Geschlechternormen im digitalen Raum befördert und gefestigt werden» (ebd.). Dies geschieht u. a. durch die Ausnutzung von Cyberkriminalitätsgesetzen zur Kriminalisierung von Online-Inhalten auf Grundlage geschlechtsspezifischer sozialer Normen oder «Sitten» (Shires, Hassib & Swali 2024: 15). Wissenschaftler*innen der Denkfabrik Chatham House beobachteten dabei einen «Verstärkungs- und Kumulationseffekt»: Eine geschlechtsspezifische Schädigung durch Cyberkriminalität verursacht eine weitere oder steht mit dieser in Verbindung – und tritt so eine Art Schadensspirale los, die sich wiederum verstärkt auf die Betroffenen auswirkt (ebd.).

Die meisten der schätzungsweise 2,6 Milliarden Menschen ohne Internetzugang (International Telecommunication Union 2023) sind Frauen und Mädchen (International Telecommunication Union 2024: 3).[8] Folglich haben sie weniger Zugang zu digitaler Bildung, was erhöhte Vulnerabilität gegenüber Cyberkriminalität mitverursacht. Gleichzeitig verüben Männer häufiger Cyberverbrechen, darunter solche mit geschlechtsspezifischem Charakter, z. B. die Nutzung von Schadprogrammen zum Stalking von Intimpartner*innen (Bada et al. 2021). Mädchen und Frauen sind von diesen Verbrechen insbesondere in Form von Kontrolle oder innerfamiliärer bzw. partnerschaftlicher Gewalt betroffen.

8 Weltweit nutzen etwa 70 Prozent der Männer und 65 Prozent der Frauen das Internet. International bewegen wir uns dabei auf Geschlechterparität zu (0,94 im Jahr 2024), mit Ausnahme der am wenigsten entwickelten Länder, in denen die Geschlechterparität 2024 von 0,74 auf 0,70 gesunken ist (ebd.).

Kontrolle und Manipulation von Information, Identitätsbetrug, diskriminierende Äußerungen, unerlaubter Zugriff, Überwachung, Drohungen, Verunglimpfung, nicht einvernehmliches Teilen privater Informationen, technologiegestützter sexueller Missbrauch und sexuelle Ausbeutung, Angriffe auf Kommunikationskanäle, fehlendes Durchgreifen von Regulierungsinstanzen, Erpressung und Überwachung und Stalking: All das sind Formen von technologiegestützter geschlechtsspezifischer Gewalt (TFGBV – Technology-Facilitated Gender-Based Violence),[9] von denen Frauen besonders betroffen sind und die durch digitale Werkzeuge erst ermöglicht bzw. verstärkt werden. (United Nations Human Rights Council 2018; UNRIC 2024). Cyberharassment (Online-Belästigung), bildbasierte sexuelle Gewalt, Cyberstalking und andere Formen von geschlechtsspezifischer Cyberkriminalität verzeichnen vor allem seit der Covid-19-Pandemie und seit kurzem auch mit der Ausbreitung kommerzieller KI-Tools einen drastischen Anstieg (Uhlich et al. 2024; UNRIC 2024). Ob und ab wann TFGBV wie z. B. Cyberharassment strafrechtlich verfolgt wird, hängt von der nationalen Gesetzgebung ab. Dessen ungeachtet können Schäden infolge kriminalisierter TFGBV auch durch nicht kriminalisierte TFGBV verschärft werden.

Dabei muss angemerkt werden, dass nicht alle Frauen gleichermaßen von TFGBV betroffen sind. Die «Troll Patrol»-Studie von Amnesty International zu Online-Gewalt gegen Politikerinnen und Journalistinnen zeigte zwar, dass alle in der Studie berücksichtigten Frauen – unabhängig von ihrer Selbstverortung im politischen Spektrum – alle 30 Sekunden einen beleidigenden oder problematischen Tweet erhielten; Frauen of Color waren aber mit einer 34 Prozent, Schwarze Frauen sogar mit einer 84 Prozent höheren Wahrscheinlichkeit Ziel eines solchen Tweets als Weiße (Amnesty International 2018). Auch Gruppen, die aufgrund von Identitätsmarkern wie kulturelle Identität(en)/Rassifizierung bzw. Aufenthaltsstatus marginalisiert werden, sind zunehmend schwerer von Online-Hassrede (Hatespeech) betroffen (Democracy Reporting International 2023).

Die Folgen für das Leben der Betroffenen, ihre Familien, Kinder, Beziehungen, das Arbeitsleben sowie die allgemeine mentale und körperliche Gesundheit sind frappierend. Der hohe Preis des individuellen Leidens ist mit keinem Betrag aufzurechnen, doch sollte nicht unerwähnt bleiben, dass sich die Gesamtkosten infolge von Cyberharassment und Cyberstalking von Frauen u. a. durch Kosten für Gesundheitsversorgung, Prozessführung und Schäden auf dem Arbeitsmarkt laut einer EU-Studie jährlich auf 45 bis zu 90 Milliarden Euro belaufen dürften (Council of Europe 2021).

Geschlechterspezifische Faktoren spielen auch bei der besonderen Vulnerabilität von Mädchen und Jungen eine Rolle, vor allem hinsichtlich Abbildungen von sexuellem Kindesmissbrauch (CSAM) und «Sextortion», also der sexuellen Nötigung und Erpressung von Kindern im Internet. So meldeten die Strafverfolgungsbehörden im US-Bundesstaat

9 Die 13 Erscheinungsformen von technologiegestützter geschlechtsspezifischer Gewalt sind *hier* detailliert aufgeführt.

Indiana, dass 2023 mindestens 3 000 (vor allem männliche) Minderjährige von Online-Sextortion betroffen waren (US Attorney's Office, Southern District of Indiana 2023). Auch das als Revenge Porn (Racheporno) geläufige, nicht einvernehmliche Teilen intimer Bilder (NCSII) nimmt als Form geschlechtsspezifischer Online-Gewalt stetig zu. Mit der Einführung kommerzieller KI-Generatoren lassen sich derartige sexuell explizite Inhalte (wie Deepfake-Pornos), die vor allem Mädchen und Frauen betreffen, einfach und ohne Zustimmung generieren (StopNCII.org o. D.). Es gibt kaum öffentliche Erhebungen zu diesem Feld, jedoch verzeichnet die Revenge Porn Helpline für NCSII-Betroffene einen jährlichen Anstieg der Vorfälle, 2020 während der Corona-Pandemie sogar eine Verdopplung (SWGfL o. D.).

Auch Cyberkriminalität, die sich nicht gegen bestimmte Individuen oder Gruppen richtet, kann je nach Geschlechtsidentität oder -ausdruck unterschiedlich schwere Auswirkungen haben. Aufgrund der Sensibilität von Daten und anderer Kontexteffekte kann Geschlecht die Vulnerabilität entscheidend beeinflussen. Wenn etwa gehackte und geleakte Daten medizinische Informationen preisgeben, die (wie etwa Schwangerschaftsabbrüche) Rückschlüsse erlauben auf sexuelle oder reproduktive Aspekte der Gesundheit, die Wahrnehmung von entsprechenden Rechten oder die persönliche Vergangenheit, dann ist das für Frauen und LGBTQIA+ in vielen Fällen mit größeren Risiken behaftet als für andere Gruppen. Grund dafür ist, dass Informationen zu Schwangerschaftsabbrüchen oder sexuellen Vorlieben vor allem in Staaten, in denen sie illegalisiert sind, zur weiteren Ausgrenzung und Einschüchterung der betroffenen Personen genutzt werden können (Pavlova 2024).

Neben anderen Identitätsmarkern kann sich auch der Beruf einer Person maßgeblich darauf auswirken, wie intensiv sie Cyberkriminalität ausgesetzt bzw. wie vulnerabel sie demgegenüber ist. Journalist*innen, Whistleblower*innen, (Menschenrechts-)Aktivist*innen, Dissident*innen und Anwärter*innen auf politische Ämter waren online häufiger Cyberharassment, sexualisierten Drohungen, Einschüchterungsversuchen und Überwachung ausgesetzt (Amnesty International 2018; Pavlova 2025; UNESCO 2020). So enthüllte beispielsweise das Pegasus Project, ein Gemeinschaftsprojekt von 17 Medienunternehmen, dass mindestens 180 Journalist*innen in 20 Ländern zwischen 2016 und 2021 potenzielle Ziele der Pegasus-Überwachungssoftware der israelischen NSO Group waren (Amnesty International 2021). Diese hohe Zahl, unter der sich nicht zuletzt mehrere Journalist*innen aus schwachen Demokratien und Ländern mit zunehmender Autokratisierung befinden, macht deutlich, wie Überwachungssoftware dazu genutzt wird, kritischen Journalismus einzuschüchtern oder zum Schweigen zu bringen (ebd.). Die NSO Group hat weder bestätigt noch dementiert, in staatlichem Auftrag gehandelt zu haben. Stattdessen wird behauptet, das Pegasus Project treffe «falsche Annahmen» (ebd.). In anderen Fällen konnten Regierungen klar als Täter identifiziert werden. Eine Untersuchung der israelischen Zeitung Haaretz enthüllte 2018 beispielsweise, dass die indonesische Regierung Software erworben hatte, um Daten von LGBTQIA+-Aktivist*innen zu sammeln und sie zu überwachen (Pavlova 2024 zitiert nach Haaretz 2018). «Schon die Tatsache oder Vermutung des Überwachtwerdens kann psychisch belasten, Sorge um die eigene

Privatsphäre und Sicherheit auslösen und damit abschrecken. Um herrschenden Normen zu entsprechen, ziehen sich betroffene Personen oft aus dem sozialen und öffentlichen Leben zurück oder passen ihr Verhalten an. Betroffene von intensiver Überwachung berichten zudem von psychischer Belastung, Verfolgungsangst, sozialer Isolation und Selbstzensur aus Furcht vor Sanktionen» (Pavlova 2024).

Gesetze gegen Cyberkriminalität als Instrument staatlicher Übergriffe

Menschenrechtskonforme Strafgesetzgebung kann Rahmenbedingungen schaffen, die den Betroffenen und Zeug*innen von Cyberkriminalität Schutz und Gerechtigkeit bieten können und sollten. Gesetze gegen Cyberkriminalität können Bestimmungen zur Unterstützung und zum Schutz von Betroffenen beinhalten, darunter auch Maßnahmen, die sie dabei unterstützen, sich physisch und psychisch von einem Angriff zu erholen. In vielen Fällen wurden im Zusammenhang mit Cyberkriminalität verabschiedete Gesetze jedoch zur Rechtfertigung von staatlichen Übergriffen missbraucht; auch dazu, antifeministische und patriarchale Programme durchzusetzen. Insbesondere autoritäre Staaten und Länder, in denen demokratische Strukturen zunehmend abgebaut werden, nutzen Gesetze gegen Cyberkriminalität, um individuelle Rechte und Freiheiten zu untergraben und Menschen zu kriminalisieren, die sich für die Rechte der vulnerabelsten Mitglieder der Gesellschaft einsetzen. So können Gesetze gegen Cyberkriminalität beispielsweise dazu eingesetzt werden, unverhältnismäßige Zensur und Überwachung durchzusetzen. In einigen Fällen werden diese Übergriffe noch durch eine diskriminierende Justiz verschärft (s. Kapitel 4).

3 Ein intersektional feministischer Blick auf Gesetze gegen Cyberkriminalität

Eine intersektional feministische Perspektive auf die Gesetzgebung gegen Cyberkriminalität[10] geht über Ansätze mit Schwerpunkt auf menschliche Sicherheit, Menschenrechte und die Teilhabe von Frauen hinaus. Sie baut auf dem Verständnis auf, dass die Verschränkung von Identitätsmarkern wie Geschlecht, Sexualität, Anstellung/Beruf, Klasse und Rassifizierung die potenziellen negativen Folgen von Cyberkriminalität und die missbräuchliche Anwendung von Cyberkriminalitätsgesetzen gegen historisch und/oder politisch marginalisierte Gruppen verschärfen kann (s. Kapitel 2). Dadurch werden Fortschritte bei der Umsetzung von Geschlechtergerechtigkeit, menschlicher Sicherheit und allgemeingültiger Menschenrechte untergraben und eingeschränkt.

Intersektional feministische Perspektiven auf die Gesetzgebung gegen Cyberkriminalität nehmen bei dem Entwurf, der Durchsetzung und der Bewertung von rechtlichen Maßnahmen gegen Cyberkriminalität besonders intersektionales Gender-Mainstreaming in den Blick.[11] Außerdem gehen sie über reine gesetzgebungsbezogene Gender-Mainstreaming-Bemühungen hinaus, indem sie Analysen von nationalen und globalen Politik- und Rechtssystemen sowie -strukturen berücksichtigen, in denen Gesetze gegen Cyberkriminalität verhandelt, etabliert, durchgesetzt und bewertet werden. Darüber hinaus erkennt dieser Ansatz an, dass Menschen hinsichtlich (der Wahrnehmung) ihrer Sicherheit und Menschenrechte auf ungleiche Weise ebenso von Cyberkriminalität und deren Auswirkungen on- und offline betroffen sind wie von Recht und Gesetz, mit dem Staaten

10 Hier wird berücksichtigt, dass in vielen Staaten keine gesonderte Gesetzgebung gegen Cyberkriminalität existiert. Stattdessen werden ggf. rechtliche Bestimmungen oder politische Programme bezüglich (verschiedener Formen von) Cyberkriminalität in relevante Cyberkriminalitätsstrategien, -gesetze und/oder -bestimmungen integrieret, z. B. Pressefreiheit, Urheber*innenrechte, Datenschutz, Missbrauch von Computern, Onlinehandel oder Maßnahmen zur Terrorismusbekämpfung. Die *Database of Legislation* (Datenbank der gesetzlichen Bestimmungen) der UNDOCS gibt einen umfassenden Überblick über die verschiedenen Bemühungen von UN-Mitgliedstaaten im Umgang mit Cyberkriminalität.

11 Intersektionales Gender-Mainstreaming bewertet alle Ebenen der geschlechtsspezifischen Auswirkungen von Politik und/oder Maßnahmen unter gleichzeitiger Berücksichtigung der Auswirkungen anderer Identitätsmarker wie Klassenzugehörigkeit und Rassifizierung. Es stellt sicher, dass alle Erfahrungen, Bedenken und Ziele von Gruppen, die aufgrund ihres Geschlechts oder anderer Identitätsmarker marginalisiert werden, bei der Erarbeitung, Verabschiedung und Überwachung von Richtlinien, insbesondere solcher, die sie direkt betreffen, zentral Berücksichtigung finden. Das erklärte Ziel von Gender-Mainstreaming ist die Förderung der Gleichstellung der Geschlechter, die Sicherstellung gleicher Rechte für alle, die Verringerung von Ungleichheit und die Unterstützung einer nachhaltigen Entwicklung.

versuchen, Cyberkriminalität zu verhindern, entschärfen und sanktionieren (s. Kapitel 2).[12] Der intersektional feministische Ansatz beleuchtet absichtlich und/oder unabsichtlich zugefügte Schäden durch Bestimmungen, die sich aus den gesetzlichen Regelungen, den damit einhergehenden Schutzmaßnahmen und deren praktischer Umsetzung ergeben können – insbesondere in Anbetracht der Tatsache, dass bestehende Gesetze zur Cyberkriminalität gegen bereits diskriminierte, marginalisierte oder Angriffen ausgesetzte Gruppen instrumentalisiert werden können bzw. zum Teil bereits werden (s. Kapitel 4).

Gesetze gegen Cyberkriminalität werden weder im luftleeren Raum entwickelt noch umgesetzt. In Gesetzen schlagen sich immer verschiedene kulturelle und/oder kontextuelle Auffassungen von «Cyberkriminalität» nieder (s. Hu, Chen & Bose 2013). Aus diesem Grund wird die Umsetzung nicht selten durch geschlechtsspezifische, patriarchale Normen beeinflusst (bzw. das, was autoritäre Regierungen oft als «Sitten» bezeichnen). Unter Umständen werden strafrechtliche Bestimmungen diskriminierend und tendenziös umgesetzt, um die Handlungen einer Zielperson auf Grundlage ihres Geschlechts oder anderer Identitätsmarker zu kriminalisieren. Trotz der Vielzahl geschlechtsspezifischer Folgen (s. Kapitel 2) wird Geschlechter(un)gerechtigkeit bei der Planung, Umsetzung und Evaluierung von Gesetzen gegen Cyberkriminalität jedoch nicht von allen Staaten in angemessenem Umfang berücksichtigt. Einige Staaten haben neue Gesetze verabschiedet oder alte so überarbeitet, dass zumindest einige Formen von technologiegestützter geschlechtsspezifischer Gewalt (TFGBV)[13] wie Sextortion[14] oder das nicht einvernehmliche Teilen intimer Bilder (NCSII, s. Kapitel 5) unter Strafe gestellt werden. In der intersektional feministischen Perspektive auf Cyberkriminalitätsgesetze wird aber hervorgehoben, dass diese inklusiv und unter Berücksichtigung tatsächlicher Erfahrungen und Bedürfnisse von Betroffenen gestaltet werden müssen, wenn sie Schaden abwenden oder abschwächen sollen.

12 Cybersicherheit und Cyberkriminalität sind miteinander verknüpfte und sich überschneidende Themen. Cybersicherheit ist jedoch ein proaktives und präventives Konzept, das vor allem darauf abzielt, Bedrohungen und Angreifbarkeit im und durch das Internet zu verhindern, während Cyberkriminalität sich auf bereits getätigte Angriffe bezieht, die mit dem Internet in Verbindung stehen. Bestimmungen zu Cyberkriminalität folgen also einem eher reaktiven Ansatz, da sich das Konzept mit der Untersuchung und strafrechtlichen Verfolgung solcher Handlungen befasst.

13 Die Platform of Independent Expert Mechanisms on Discrimination and Violence against Women (EDVAW Platform) des Hohen Kommissars der Vereinten Nationen für Menschenrechte bietet eine Liste von Länderbeispielen im Bericht «The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform» (Die digitale Dimension der Gewalt gegen Frauen, in der Analyse der sieben Expert*innengremien der EDVAW-Plattform, Europarat 2022).

14 In Abgrenzung zu anderem sexuell missbräuchlichem Verhalten spielen bei Sextortion sowohl sexuelle als auch erpresserische Aspekte eine Rolle. Zum einen vermittelt Sextortion die Aufforderung, auf sexuelle Handlungen einzugehen, zum anderen muss der*die Täter*in eine Machtposition innehaben oder seine*ihre Macht in einer Art Quidproquo ausnutzen (International Association of Women Judges o. D.).

Darüber hinaus wird in der intersektional feministischen Betrachtung von Gesetzgebung gegen Cyberkriminalität unterstrichen, dass sich überschneidende Identitäten eine entscheidende Rolle beim Access to Justice,[15] dem Zugang zum Recht, sowie dem Recht auf ein ordnungsgemäßes Verfahren und wirksame Rechtsmittel spielen (s. auch Derechos Digitales & Association for Progressive Communications 2023). Prinzipiell sind staatliche Rechtssysteme Geschlecht gegenüber nicht unvoreingenommen; vielmehr spiegeln sich in ihnen häufig patriarchale und diskriminierende Normen und Ungleichheiten in Bezug auf Geschlecht und andere (sich überschneidende) Identitätsmarker wider.

Für marginalisierte Personengruppen, z. B. rassifizierte Minderheiten, LGBTQIA+, Menschen mit Behinderungen und solche mit geringem Einkommen, ist der Zugang zum Recht oft mit Hürden verbunden. Neben den bereits erwähnten (geschlechtsspezifischen) Verzerrungen innerhalb eines Rechtssystems lässt sich das auch auf andere Faktoren wie eingeschränkte Mobilität, finanzielle Hürden, mangelnde Sprachkenntnisse oder digitalen Analphabetismus zurückführen (Creutzfeld et al. 2024; Ghai & Cottrell 2009). Selbst wenn marginalisierte Personen Zugang zum Recht haben, werden ihre Aussagen und der erlittene Schaden immer wieder heruntergespielt oder ihnen Glaubwürdigkeit abgesprochen. Diese Gruppen werden von Strafverfolgungsbehörden und dem Rechtssystem teilweise ungerecht oder unrechtmäßig behandelt bzw. beurteilt, absichtlich oder unabsichtlich reviktimisiert und anderen Diskriminierungsformen ausgesetzt (Penal Reform International 2012).

Vor diesem Hintergrund erscheinen in feministischer Perspektive auf Cyberkriminalitätsgesetze neben den Erfahrungen von Betroffenen und Zeug*innen von Cyberkriminalität ebenso die von Betroffenen eines Missbrauchs dieser Gesetze zentral. Daraus leitet sich die Forderung nach umfassender, intersektional geschlechtersensibler/-gerechter Unterstützung, diskriminierungssensiblen Verfahren und -praktiken und Verhinderung von Reviktimisierung ab.

Dabei muss angemerkt werden, dass mit dem intersektional feministischen Zugang zur Gesetzgebung gegen Cyberkriminalität in diesem Positionspapier keineswegs impliziert werden soll, dass Frauen, LGBTQIA+ und andere Gruppen per se vulnerabel sind. Sie nur als Betroffene zu sehen, verstellt den Blick auf ihre Handlungsfähigkeit, Widerstandskraft und aktive Rolle im Kampf gegen Cyberangriffe und in der Schaffung und Gestaltung sichererer inklusiverer Räume.

15 Zugang zum Recht ist ein grundlegendes Menschenrecht. Es garantiert, dass sich alle Menschen vor der Verletzung ihrer Rechte schützen sowie Rechtsmittel in Anspruch nehmen können, wobei sie sowohl Privatpersonen als auch Staaten zur Verantwortung ziehen können. Dies «gewährleistet, dass rechtliche und juristische Ergebnisse recht und billig sind» (Lima & Gomez 2021).

4 Gesetzgebung gegen Cyberkriminalität und staatliche Übergriffe

Wie in jedem anderen Bereich des Rechts ist es auch bei Gesetzen zur Bekämpfung von Cyberkriminalität unerlässlich, dass die Umsetzung von Bestimmungen Menschenrechte stärkt, statt sie zu verletzen. Darum müssen Vorkehrungen zur Festigung von Grundrechten festgeschrieben werden. Dazu gehören das Recht auf Meinungsfreiheit, auf Privatsphäre sowie weitere Menschenrechte, vor allem von marginalisierten Individuen und Gruppen. In verschiedenen Teilen der Welt werden Gesetze gegen Cyberkriminalität jedoch dazu missbraucht, on- und offline Kritik zu unterdrücken, zivilgesellschaftliche Räume zu beschneiden und autokratische Herrschaft durch die Überwachung, Zensur und Verfolgung von Frauen, LGBTQIA+, Journalist*innen, (feministischen) Menschenrechtsaktivist*innen und anderen Kritiker*innen zu festigen (Derechos Digitales & Association for Progressive Communications 2023; GenderIT.org 2008; Shires, Hassib & Swali 2024).

Neben ernsthaften Konsequenzen für die ggf. subjektiv wahrgenommene Freiheit, Sicherheit und Wahrung der Menschenrechte der angegriffenen Personen hat das auch weitere soziale und politische Folgen. Für Frauen, LGBTQIA+ und andere marginalisierte Gruppen, die außerhalb des digitalen Raums historisch oder politisch von tatsächlicher politischer Teilhabe ausgeschlossen werden/wurden, hat das Internet eine Schlüsselrolle bei der Stärkung und Ausweitung ihrer Meinungs- und Versammlungsfreiheit gespielt. So haben Frauen beispielsweise im Iran und in Afghanistan soziale Medien dazu genutzt, Proteste zu organisieren, sich über das Leben unter autoritärer Herrschaft auszutauschen und Gleichberechtigung einzufordern (RadioFreeEurope/RadioLiberty 2021). So ließ sich «die Sichtbarkeit für Frauenrechtsaktivismus von der lokalen Ebene auf die globale heben» (Koutchesfahani 2022) und dadurch trotz erheblicher Beschränkungen der traditionellen Berichterstattung internationale Aufmerksamkeit generieren. Vor allem in Zusammenhängen, in denen Frauen, LGBTQIA+ und andere marginalisierte Gruppen in- oder außerhalb des digitalen Raums bei der Ausübung freier Meinungsäußerung vor (geschlechtsspezifische) Hürden gestellt werden, können Gesetze gegen Cyberkriminalität die Situation weiter verschärfen. Da sie den staatlichen Behörden meist unangemessene Ermittlungsgewalt übertragen, können die Rechtssysteme einzelner Staaten die Privatsphäre und den persönlichen Datenschutz (geschlechtsspezifisch) verletzen bzw. missbrauchen (s. Kapitel 4.2). Schon allein die Angst, ins Visier der Behörden zu geraten, kann zu Selbstzensur oder weniger Ausübung freier Meinungsäußerung führen (United Nations Human Rights Council 2020). Angesichts der Allgemeingültigkeit, Unteilbarkeit und Wechselwirkung von Menschenrechten müssen staatliche Übergriffe, die Gesetze gegen Cyberkriminalität ausnutzen, um das Recht auf Meinungsfreiheit und Privatsphäre zu unterhöhlen, als Angriff auf Gleichberechtigung, allgemeine Menschenrechte und als Bedrohung für eine nachhaltige Entwicklung, Frieden und Demokratie gewertet werden – vor allem dann, wenn sie sich gegen marginalisierte Gruppen wenden (United Nations

General Assembly 2021; United Nations Human Rights Council 2020). Es existiert eine Bandbreite strategischer, kontextübergreifender Handlungsmuster, mit denen Staaten die Rechte von Frauen, LGBTQIA+ und anderen marginalisierten Gruppen unangemessen eingeschränkt haben. Diese Muster zeigen sich sowohl in der Ausarbeitung der Gesetze zur Bekämpfung von Cyberkriminalität (etwa bei der Definition von Bestimmungen und deren Geltungsbereich) als auch bei ihrer Durchsetzung durch Strafverfolgungsbehörden (Zugang zum Recht, gerichtliche Verfahren, verfügbare Rechtsmittel). Darüber hinaus ermöglichen Gesetze gegen Cyberkriminalität staatlichen Autoritäten unter dem Vorwand von Ermittlungen häufig den Missbrauch von Überwachungstechnologie sowie den Zugriff auf persönliche Daten und deren Speicherung (s. Kapitel 4.2).

Obwohl die hier ausgewählten Fälle aus unterschiedlichen geografischen und kulturellen Kontexten stammen, scheinen viele der Gesetze und dazugehörige (Straf-/Rechts-)Systeme nach den ähnlichen autoritären Spielregeln gestaltet zu sein. Letztere sind meist stark von Antifeminismus geprägt, das heißt von kulturellen Vorstellungen und Überzeugungen und/oder Normen, die einer Gleichstellung der Geschlechter und anderen feministischen und menschenrechtlichen Forderungen ablehnend gegenüberstehen (Derechos Digitales & Association for Progressive Communications 2023: 9).[16] Einige der hier betrachteten Staaten stellen zudem gleichgeschlechtliche Beziehungen unter Strafe und/oder lehnen eine Gleichstellung der Geschlechter grundsätzlich ab.

Dabei ist zu beachten, dass in diesem Kapitel beispielhaft eine Analyse potenzieller und tatsächlicher Fallstricke nationaler Gesetze zur Bekämpfung von Cyberkriminalität vorgenommen wird, aber keine Analyse von Gesetzgebung gegen Cyberkriminalität an sich.

16 Autokratisierung und demokratischer Verfall sind oft eng mit Antifeminismus verflochten. Wie das CFFP in der Publikation «Strongmen and Violence: Interlinkages of Anti-Feminism and Anti-Democratic Developments» (Machthaber und Gewalt: Verbindungen zwischen Antifeminismus und antidemokratischen Entwicklungen) hervorhebt, nutzen antidemokratische und autoritäre Akteur*innen «antifeministische Diskurse und Strategien, um ihre Macht auf nationaler, regionaler und internationaler Ebene zu festigen und Rechtsstaatlichkeit und andere Pfeiler der Demokratie auszuhöhlen» (Seitenova, Kobel & Bernarding 2024: 2). Während Rolle und Funktion von Antifeminismus stark vom Kontext anhängen, arbeitet der Text des CFFP zwei grundsätzliche Funktionsweisen heraus: Zum einen bedienen sich autoritäre Akteure antifeministischer Narrative, um innerstaatliche Unterdrückung gegen marginalisierte Gruppen zu rechtfertigen. Zum anderen werden sie dazu genutzt, um die Außenpolitik dieser Akteur*innen voranzutreiben und oder Konflikte auszulösen und zu rechtfertigen (ebd.: 3).

4.1 Warum es eindeutige Definitionen braucht: Weit gefasste Geltungsbereiche in Gesetzen zur Bekämpfung von Cyberkriminalität und deren unbeabsichtigte Folgen

Nationale Gesetze zur Bekämpfung von Cyberkriminalität enthalten oft unspezifische, vage und sehr breit gefasste Begriffe. Damit können sie von Regierungen leicht für repressive und willkürliche Zwecke ausgelegt und eingesetzt werden (Human Rights Watch 2021). Viele Gesetze gegen Cyberkriminalität ermöglichen eine umfassende Kriminalisierung von Äußerungen im Internet auf der Grundlage von Paragraphen gegen «Fakenews/Falschnachrichten», «Desinformation», «Verschwörung» oder «anstößige Inhalte», die wahlweise die «nationale Sicherheit» oder «Einheit» bedrohen und/oder die «Sitten» bzw. «traditionelle Werte» untergraben. Die folgenden Fälle illustrieren, wie Staaten diese unklar abgegrenzten Begriffe missbrauchen und so bestehende Vorkehrungen zur Sicherung/Wahrung von Menschenrechten ebenso übergehen wie Prinzipien von Rechtmäßigkeit, Notwendigkeit, Angemessenheit und Diskriminierungsfreiheit; Prinzipien also, die die freie Meinungsäußerung gewährleisten und staatliche Übergriffe eigentlich verhindern sollen.

«Sitten» und «Familienwerte» als Waffe gegen Frauen, LGBTQIA+ und deren freie Meinungsäußerung im Internet

Die geschlechtsspezifischen Wurzeln und Auswirkungen nationaler Gesetze gegen Cyberkriminalität und/oder juristischer Entscheidungen zeigen sich vermutlich am deutlichsten dort, wo die Wahrung der «Sitten» als Begründung herangezogen wird, um Online-Beiträge zu kriminalisieren und Inhalte aus dem Internet zu entfernen. In vielen patriarchalen Gesellschaften, in denen Geschlechtsidentität, sexuelle Selbstbestimmung, Körper und Verhaltensweisen von Frauen und anderen marginalisierten Gruppen auf der Grundlage (binärer) Geschlechternormen Abwertung, Verurteilung und Kontrolle ausgesetzt sind, werden ihre Ton-, Video- oder Textbeiträge online meist als «anstößig» und «obszön» gewertet oder geframed.[17] Häufig behaupten die staatlichen Autoritäten dieser Länder, die Beschneidung der freien Meinungsäußerung von Frauen online sei unerlässlich, um Frauen und die Gesellschaft, die Kultur des Landes und/oder traditionelle Familienwerte oder Moralvorstellungen zu schützen (s. z. B. Bhandari & Kovacs 2021). «[I]n einem solch

17 Nach Verständnis der Autor*innen herrschen sowohl im Globalen Norden als auch im Globalen Süden in den meisten Gesellschaften patriarchale Verhältnisse. Darum soll in diesem Kapitel in keiner Weise unterstellt werden, dass patriarchale Systeme und deren schädlicher Einfluss auf Gesellschaften – besonders auf marginalisierte Communitys – nur ein Problem außerhalb Europas/des Globalen Nordens ist. Aufgrund des Rahmens und des Ziels dieses Positionspapiers werden hier jedoch nur Staaten besprochen, in denen Gesetze zur Bekämpfung von Cyberkriminalität nachweislich zur Diskriminierung von Frauen und anderen marginalisierten Gruppen eingesetzt wurden.

paternalistischen Verständnis bleibt das Einverständnis von Frauen [aber] unberücksichtigt, und jeder Ausdruck weiblicher Sexualität erscheint als problematisch, grenzüberschreitend und strafwürdig» (United Nations General Assembly 2021).

Der Europäische Gerichtshof für Menschenrechte (EGMR) und der UN-Menschenrechtsausschuss haben entschieden, dass es zur Einschränkung des Rechts auf freie Meinungsäußerung nicht reicht, sich ausschließlich auf das weit gefasste Konzept von «Sitten» zu berufen (Mendel o. D.; United Human Rights Committee 2011).[18] Des weiteren dürfen Beschränkungen der freien Meinungsäußerung «zur Wahrung der Sitten nicht allein auf Tradition fußen» (UN Human Rights Committee 2011: 8), sondern müssen «auf Grundlage universaler Menschenrechte und dem Prinzip der Diskriminierungsfreiheit» verstanden werden (ebd.). In den folgenden Beispielen aus Ägypten und Libyen werden diese Menschenrechtsstandards jedoch vorsätzlich ignoriert. Die geschlechtsspezifische, missbräuchliche Durchsetzung nationaler Gesetze gegen Cyberkriminalität ist ein alarmierendes Zeichen für den Zustand (digitaler) Frauenrechte und Gleichberechtigung in diesen Ländern.

Laut Human Rights Watch sind in Ägypten unter Präsident Abdel Fatah El-Sisi Verhaftungen von Frauen aufgrund von «‚sittlicher› [Vergehen] […] sprunghaft angestiegen» (zitiert nach Makooi 2023). Tatsächlich wurden Social-Media-Influencer*innen absichtlich von ägyptischen Behörden ins Visier genommen, nachdem das Gesetz Nr. 175 zu Cyberkriminalität und Straftaten im Bereich der Informationstechnologie 2018[19] verabschiedet worden war (im Folgenden Cyberkriminalitätsgesetz Nr. 175), und Frauen sich 2020 im Rahmen einer #MeToo-Kampagne in sozialen Medien Gehör verschafften (Allinson 2020; Juma & Knipp 2020). 2023 verhafteten ägyptische Behörden z. B. Model und TikTokerin Salma Elshimy aufgrund vager Anschuldigungen, sie würde durch ihre Social-Media-Posts zu «ausschweifender Lebensweise» und «Verstößen gegen Familienwerte» anstiften, was nach Aussage der Behörden «im Widerspruch zu gesellschaftlichen Werten und Moralvorstellungen» stehe (Makooi 2023). In den meisten ihrer TikTok-Posts filmte sich die Influencerin vollständig bekleidet beim Posieren, Singen oder Tanzen. Die Verhaftung und das Mundtotmachen von Frauen aus dem alleinigen Grund, dass sie online Videos und Fotos von sich teilen, die die ägyptische Regierung als obszön einstuft, bewertet Human Rights Watch nach Aufarbeitung mindestens 15 ähnlicher Fälle als Diskriminierung und «direkten Verstoß gegen das Recht auf freie Meinungsäußerung» (Human Rights Watch 2020). Im April 2023 wurde Elshimy laut ihrem Anwalt von einem Gericht in Alexandria den oben genannten, vagen Anklagepunkten entsprechend zu zwei

18 So muss eine Einschränkung der freien Meinungsäußerung nach Artikel 10 (2) der Europäischen Menschenrechtskonvention nicht nur eine der übergeordneten Interessen in Artikel 10 (2) schützen und gesetzlich vorgegeben sein, sondern auch «in einer demokratischen Gesellschaft notwendig» sein (Mendel o. D.).

19 Für den Gesetzestext in ganzer Länge s. «*Law No. 175 of 2018 on Anti-Cyber and Information Technology Crimes, Egypt, WIPO Lex*».

Jahren Gefängnis und einer Strafe von 100 000 ägyptischen Pfund verurteilt (etwa 3000 Euro; The New Arab 2023).

Seit langem diskriminiert der ägyptische Staat queere Communitys und hat «durch Gesetzesauslegung und Präzedenzfälle einen ganzen Justizapparat [aufgebaut, der] eine fortlaufende und gezielte Verfolgung von LGBTQIA+ ermöglicht» (Rigot 2020). In den vergangenen Jahren wurden LGBTQIA+-Fälle zudem zunehmend an Wirtschaftsgerichte verwiesen, die für das Cyberkriminalitätsgesetz Nr. 175 von 2018 zuständig sind. Da im besagten Gesetz enthaltene vage Begriffe wie «Familienwerte» nicht abschließend von höheren Gerichten definiert wurden, können sie bei jeder Anwendung neu ausgelegt werden, wie Afsaneh Rigot von der Menschenrechtsorganisation Article 19 betont (ebd.). Nicht nur schreckt dies viele LGBTQIA+ aus Angst vor rechtlicher Verfolgung von öffentlichen Äußerungen zu Geschlecht und Sexualität ab, es birgt auch das Risiko, dass andere repressive Regierungen Ägyptens Strategie übernehmen, LGBTQIA+ durch die Anwendung von IKT-Gesetzen zu kriminalisieren (ebd.).

Im Februar 2023 gab das libysche Innenministerium die Festnahme der bekannten Sängerin Ahlam al-Yamani und der Bloggerin Haneen al-Abdali wegen «Sittenwidrigkeiten» nach Gesetz Nr. 5 gegen Cyberkriminalität von 2022 bekannt.[20] Al-Yamani und al-Abdali wird vorgeworfen, «das Ansehen der tugendhaften und ehrwürdigen libyschen Frauen in unserer konservativen Gesellschaft mit Taten und Verhaltensweisen zu beleidigen, die uns fremd sind und die gegen unsere Bräuche, Traditionen und wahre Religion verstoßen» (zitiert nach Human Rights Watch 2023a). Das Gesetz wurde ohne Beratung mit der Zivilgesellschaft oder Technologie-Expert*innen verabschiedet und enthält keine nähere Definition des «Sitten»- Begriffs (Human Rights Watch 2023a; Africanews 2023). Es wurde gleichermaßen von UN-Expert*innen und Menschenrechtsaktivist*innen aufgrund der weitgefassten Definitionen, der Gefahr strafrechtlicher Verfolgung friedlicher Meinungsäußerung sowie vorgesehener Haftstrafen von bis zu 15 Jahren scharf kritisiert (United Nations Human Rights Council 2022). Bis Redaktionsschluss wurden keine weiteren Entwicklungen zum Fall bekannt.

Kriminalisierung von regierungskritischen Äußerungen im digitalen Raum durch Unterstellung der Verbreitung von «Fakenews und Fehlinformationen», «Diffamierung» oder des Versuchs, die «nationale Sicherheit zu untergraben»

Zusätzlich zu «Sittenvergehen» haben repressive Regierungen zunehmend Straftatbestände formuliert, die auf vage Begriffe wie die «Verbreitung von Fakenews», «Verleumdung» oder Online-Beiträge und Inhalte abzielen, die die «nationale Sicherheit untergraben». Die

20 Für den gesamten Text s. «قانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية - المجمع القانوني».

hier aufgeführten Beispiele aus Nicaragua, Tunesien und Jordanien zeigen, welche schwerwiegenden Auswirkungen das auf die Meinungsfreiheit von Menschenrechtsaktivist*innen, Journalist*innen und anderen Kritiker*innen hat – also allen, die auf repressive Praktiken aufmerksam machen und sich für die Rechte marginalisiertester Menschen und vulnerabelster Gruppen einsetzen.

Laut Irene Khan, der UN-Sonderberichterstatterin zur Förderung und Schutz des Rechts auf Freiheit der Meinung und des Ausdrucks, werden Gesetze zur Bekämpfung von Desinformation – manchmal als «Fakenews»-Gesetze bezeichnet – oft dazu missbraucht, Kritiker*innen zum Schweigen zu bringen (2021: 18). Das als «Maulkorbgesetz» bekannte Cyberkriminalitäts-Sondergesetz, das 2020 in Nicaragua in Kraft trat, ist nur eines von vielen erschütternden Beispielen. Es hatte die Verfolgung und Verhaftung mehrerer Oppositioneller und Journalist*innen wegen der angeblichen Verbreitung von Falschinformationen zur Folge (Stock 2021). Laut eines Berichts von Derechos Digitales verbietet Paragraf 30 des Sondergesetzes die Verbreitung von «Falschinformationen», ohne sie jedoch genau zu definieren (2023). So unterscheidet das Gesetz beispielsweise nicht, «ob die Verbreitung schädlicher Nachrichteninhalte unabsichtlich oder vorsätzlich geschieht» (ebd.). Für Personen, «die falsche oder irreführende Informationen verbreiten, die öffentliche Unruhe, Angst und Unbehagen auslösen», sieht das Sondergesetz zwei bis vier Jahre Haft vor (AP News 2020). Die Strafe erhöht sich auf drei bis fünf Jahre, wenn die Informationen «Hass oder Gewalt schüren, die die wirtschaftliche Stabilität, das Gesundheitswesen, die nationale Souveränität oder die öffentliche Ordnung gefährden» (ebd.). Auf Grundlage dieses Sondergesetzes wurden Kritiker*innen des Umgangs mit der Corona-Pandemie (Derechos Digitales 2023) sowie eine Reihe von Aktivist*innen zum Schweigen gebracht, darunter Mitglieder der Nichtregierungsorganisation (NGO) Front Line Defenders. So wurde beispielsweise Amaru Ruiz Alemán, ein im Exil lebender Aktivist für Indigene Rechte, im September 2021 wegen «der Verbreitung von Falschinformationen mittels Informations- und Kommunikationstechnologien» angeklagt, weil er auf Social-Media-Plattformen Verstöße gegen die Menschenrechte von Indigenen in Nicaragua benannt hatte - darunter ein Massaker gegen Aktivist*innen für Menschen- und Landrechte der Mayangna (ProtectDefenders.eu 2021; OMCT 2021). Aus Angst vor Verfolgung durch das Sondergesetz sind viele Journalist*innen und traditionelle Medienunternehmen ins Exil gegangen oder haben teilweise unter falschem Namen Online-Plattformen oder Social-Media-Konten ins Leben gerufen, um die Berichterstattung fortsetzen zu können (Derechos Digitales 2023). Die abschreckende Wirkung des Sondergesetzes auf kritischen Journalismus und Meinungsäußerungen könnte sich aufgrund jüngster Reformen von Präsident Daniel Ortega im September 2024 sogar noch weiter verschärfen. Sie ermöglichen die Anwendung des Sondergesetzes nicht nur auf Verbrechen, die mithilfe von «Informationstechnik» begangen wurden, sondern auch auf «die Nutzung von Social-Media-Netzwerken und Handyapps» (Miranda Aburto 2024). Darüber hinaus wurden durch die Reform die bereits erwähnten Haftstrafen auf fünf bzw. zehn Jahre erhöht (ebd.). Diese Änderungen sind Teil eines Reformpakets, das von (Menschen-)Rechtsexpert*innen

«als Versuch [bewertet wird], die Verfolgung von Kritiker*innen von Präsident Daniel Ortega sowohl inner- als auch außerhalb des Landes zu legitimieren» (AFP 2024).

Die tunesische Fernsehkommentatorin Sonia Dahmani wurde im Oktober 2024 nach Paragraph 24 der drakonischen Verordnung mit Gesetzeskraft Nr. 2022-54 vom 13. September 2022 gegen Vergehen im Zusammenhang mit Informations- und Kommunikationssystemen[21] (nachfolgend Verordnung 54) zu zwei Jahren Haft verurteilt, da sie sich zu Tunesiens Umgang mit Migrant*innen aus Ländern südlich der Sahara geäußert hatte. Die tunesische Gesetzgebung zu Cyberkriminalität kriminalisiert Aktivitäten, bei denen «Falschinformationen in der Absicht produziert, veröffentlicht oder verbreitet werden […], die Rechte anderer zu verletzen, der öffentlichen Sicherheit oder nationalen Verteidigung zu schaden oder die Bevölkerung in Angst zu versetzen» (AP News 2024). Dies kann mit bis zu fünf Jahren Haft und Geldstrafen von 50 000 Dinar (etwa 15 000 Euro) geahndet werden. Aufgrund früherer Äußerungen, etwa zu Rassismus gegen Schwarze Migrant*innen in Tunesien, wird Dahmani wegen vier weiterer Verstöße gegen Verordnung 54 angeklagt (La Presse 2024). Damit ist sie nicht das einzige Opfer von Präsident Kais Saieds Maulkorb – auch zwei ihrer Kolleg*innen wurden nach demselben Gesetz zu einem Jahr Gefängnis verurteilt. 2023 dokumentierte Human Rights Watch, wie die Verordnung 54 dazu instrumentalisiert wurde, zwei Oppositionelle aufgrund ihrer Kritik gegen Saieds Regierung zu Gefängnisstrafen zu verurteilen und «mindestens 20 Journalist*innen, Anwält*innen, Studierende und andere Kritiker*innen für öffentliche Aussagen, die sie online oder in Medien getätigt hatten, festzunehmen, anzuklagen oder unter Beobachtung zu stellen» (Human Rights Watch 2023b). Darum haben Meinungsfreiheits- und Menschenrechtsaktivist*innen die Verordnung 54 als «symptomatisch» für Saieds autoritäre Bemühungen beschrieben, demokratische Institutionen in Tunesien unter dem Vorwand des Schutzes der «nationalen Sicherheit» zu schwächen, indem die Meinungsfreiheit eingeschränkt bzw. internationale Standards zu Meinungsfreiheit missachtet werden (Boutry 2024; Benshimon 2024, ebd.).

Beschneidung der Meinungs-, Vereinigungs- und Versammlungsfreiheit sowie des Demonstrationsrechts[22]

Das 2023 verabschiedete jordanische Gesetz Nr. 17 zur Bekämpfung von Cyberkriminalität (im Folgenden Gesetz Nr. 17)[23] weist große Ähnlichkeiten mit den bereits

21 Der vollständige Gesetzestext findet sich *hier*. Die Organisation Article 19 hat die Vereinbarkeit von Verordnung 54 mit internationalen Menschenrechten und der Meinungsfreiheit *rechtswissenschaftlich analysiert*.

22 Die Organisation Civicus hat eine große Zahl von Fällen dokumentiert, in denen Gesetze gegen Cyberkriminalität im Zusammenhang mit Pro-Palästina-Protesten und damit verbundenen Online-Inhalten gegen Protestierende, Menschenrechtsaktivist*innen und Journalist*innen eingesetzt wurden: «*Draconian Cybercrime law used to target protesters, HRDs, journalists amid pro-Palestine protests*».

23 Der vollständige Text ist *hier* einsehbar.

besprochenen Gesetzen auf. Es erweitert die Tragweite der Vergehen, die 2015 im Gesetz Nr. 27 zur Strafverfolgung von Cyberkriminalität festgehalten wurden, und führt härtere Gefängnisstrafen von mindestens drei Monaten und Geldstrafen von bis zu 32 000 jordanischen Dinar ein (etwa 40 000 Euro). Es verwendet unpräzise, dehnbare Formulierungen, die mit internationalem Recht unvereinbar sind. Darüber hinaus kriminalisiert es die Veröffentlichung und Verbreitung von Online-Inhalten, darunter Informationen, die von der Regierung als «Fake» oder «üble Nachrede» eingestuft werden, und führt höhere Strafen für andere vage definierte Vergehen wie «Bedrohung des sozialen Friedens», «Blasphemie», «Unruhestiftung» und «Cyberrufmord» ein (Jbour 2023; Amnesty International 2024b)[24]. Seit Verabschiedung 2023 hat die jordanische Regierung das Gesetz instrumentalisiert, «um Personen, die sich den staatlichen Autoritäten gegenüber kritisch äußern, in sich häufenden Angriffen auf die Meinungs-, Vereinigungs- und Versammlungsfreiheit zu schikanieren, einzuschüchtern oder zu bestrafen» (Amnesty International 2024b). Nach dem Terrorangriff der Hamas am 7. Oktober 2023 und der darauffolgenden militärischen Reaktion Israels wurden Hunderte von Aktivist*innen, Journalist*innen, Politiker*innen und Internetuser*innen gemäß Gesetz Nr. 17 strafrechtlich verfolgt und/oder verhört, die in Videos oder Posts ihre Solidarität mit Palästina ausgedrückt, die jordanische Politik gegenüber Israel kritisiert (z. B. das Friedensabkommen beider Staaten) oder auf Social-Media-Plattformen zu friedlichem Protest aufgerufen haben (ebd.; Amnesty International 2024b). Die folgenden zwei von Amnesty International dokumentierten Fälle sollen diese Situation illustrieren:

> *Die Journalistin Hiba Abu Taha verbüßt im Moment eine einjährige Haftstrafe im al-Juwaida Correction and Rehabilitation Centre im Süden von Amman aufgrund eines Artikels, indem sie die jordanische Regierung dafür kritisierte, im April 2024 iranische Raketen auf Israel abgefangen zu haben. Ein Gericht verurteilte sie am 11. Juni 2024 für die Nutzung von Social-Media-Plattformen zur «Verbreitung von Falschinformationen oder zur Beleidigung und Herabwürdigung der staatlichen Autoritäten und Organe» und für die «Anstiftung zu*

24 Beschränkungen und Verletzungen von Meinungsfreiheit im Kontext pro-palästinensischer Proteste und Solidaritätsbekundungen on- und offline müssen auch in Jordanien als Teil einer größeren Entwicklung eingeordnet werden. «Der Konflikt in Gaza hat weltweit eine Krise der freien Meinungsäußerung ausgelöst» (UN General Assembly 2024b), und zwar nicht nur in autoritären, sondern auch in demokratischen Staaten (ebd.). Irene Khan, UN-Sonderberichterstatterin zur Förderung und Schutz des Rechts auf Freiheit der Meinung und des Ausdrucks, schreibt in ihrem Bericht von 2024, dass Medienfreiheit beschnitten und pro-palästinensischer Protest und Kritik on- und/oder offline zensiert und unterdrückt wurde (2024: 7 f., 10), während gleichzeitig antisemitische und antimuslimische Hassrede und Cyberharassment sprunghaft anstiegen (New York Times 2023; BBC 2024). Das «weitreichende Auftreten unrechtmäßiger, diskriminierender und unverhältnismäßiger Vorfälle von Einschränkungen und Unterdrückungen der Meinungsfreiheit, insbesondere der palästinensischen Aktivist*innen und ihrer Unterstützer*innen in Westeuropa und Nordamerika» (UN General Assembly 2024: 19) ist nicht Bestandteil der Analyse dieses Positionspapiers, da dies größtenteils nicht auf Gesetzen zur Bekämpfung von Cyberkriminalität beruht.

Aufruhr, Aufwiegelung, Bedrohung des gesellschaftlichen Friedens oder das Schüren von Hass und Gewalt».

(Amnesty International 2024b)

Im zweiten Fall wurde die Aktivistin Fatima Shubeilat in einem Einkaufszentrum in Amman festgenommen, nachdem ein Video in den sozialen Medien verbreitet wurde, das ihre Teilnahme an einer pro-palästinensischen Protestaktion in Amman zeigte.

> *Nach Aussagen ihrer Verteidigung wurde sie zunächst wegen «Verstoßes gegen die Versammlungsgesetze», «Widerstand gegen Sicherheitskräfte» und «Beamtenbeleidigung gemäß […] Strafgesetzbuch» angeklagt. Die Staatsanwaltschaft stimmte zunächst einer Freilassung auf Kaution zu, zog dies jedoch später mit der Begründung zurück, dass die Abteilung für Cyberkriminalität ein eigenes Verfahren nach Paragraph 5 (über das Verbreiten von Fakenews oder übler Nachrede) und Paragraph 17 (über Anstiftung zu Aufruhr und Aufwiegelung) des Cyberkriminalitätsgesetzes eröffnet habe. Am 30. April 2024 wurde sie auf Kaution entlassen, das Verfahren ist in beiden Fällen jedoch weiterhin anhängig.*

(ebd.)

Beabsichtigte (geschlechtsspezifische) «Nebenwirkungen» der Verfolgung von Kritik unter Vorwand der Cyberkriminalitätsbekämpfung

In anderen Fällen nutzten Regierungen die Strafverfolgung (marginalisierter) Einzelpersonen wegen kriminalisierter Äußerungen nicht nur dazu, im digitalen Raum Kritik jedweder Art zum Schweigen zu bringen, sondern auch, um bestimmte repressive (geschlechtsspezifische) «Nebenwirkungen» im Sinne ihrer autoritären und oft antifeministischen Agenda zu provozieren.

Das zeigte sich auch im Fall der ugandischen Wissenschaftlerin Dr. Stella Nyanzi deutlich. 2017 wurde die bekennende Feministin und Kritikerin von Präsident Yoweri Museveni nach Ugandas Gesetz gegen Computermissbrauch[25] von 2011 wegen «übler Nachrede» und «Cyberharassment» angeklagt (The Independent 2023; Columbia University o. D.). Verhaftet wurde sie aufgrund von Facebook-Posts, in denen sie Präsident Museveni u. a. als «Arsch mit Ohren» bezeichnet hatte. Es gibt jedoch starke Indizien dafür, dass Nyanzi nicht nur aufgrund ihres Online-Protests angeklagt wurde. Im selben Jahr hatte Nyanzi die Kampagne #padsforgirlsUG ins Leben gerufen, nachdem Musevini sein Versprechen gebrochen hatte, die Bildung junger Frauen durch die Bereitstellung von Monatsbinden in Schulen zu unterstützen. Infolge dieser Kampagne wurde Nyanzi verhaftet. Sie verlor zudem ihren Posten an der Makerere-Universität, nachdem sie auf Twitter mit der Ehefrau

25 Der vollständige Text kann *hier* eingesehen werden.

des Präsidenten über die Verhaftung diskutiert hatte (Human Rights Foundation 2017; Mwesigwa 2027).

Berichte zu geschlechtsspezifischer Diskriminierung und Gewalt in Uganda sind alarmierend: LGBTQIA+-Organisationen wurden verboten und einvernehmliche gleichgeschlechtliche Handlungen durch radikale und repressive Gesetze kriminalisiert, teilweise sogar unter Todesstrafe gestellt (Human Rights Watch 2024a). Vor diesem Hintergrund haben Menschenrechtsexpert*innen wie Maria Burnett von Human Rights Watch Nyanzis Verfolgung (nicht nur als Regierungskritikerin, sondern auch oder vor allem als Frauenrechts- und LGBTQIA+-Aktivistin) als geschlechtsspezifisch motivierten Versuch gewertet, zwei Fliegen mit einer Klappe zu schlagen: «[Die Regierung] wollte sie, ihre Familie und ihren Unterstützer*innenkreis einschüchtern, der vor allem aus Mitgliedern von Ugandas Menschenrechts-, Frauenrechts- und LGBT-Bewegung besteht» (Slawson 2017, zitiert nach Derechos Digitales & Association for Progressive Communications 2023). Diese Einschätzung bestätigt die Aussage eines Regierungssprechers, der sich Berichten zufolge in einem Interview zum Prozess so äußerte: «Ich bezweifele, dass Nyanzi und die Hinterleute Besigye, seine Konsorten und die LGBT-Lobby aus irgendeiner politischen Auseinandersetzung mit der Regierung siegreich hervorgehen» (zitiert nach Columbia University o. D.).

4.2 Schutz der Privatsphäre und (zivilgesellschaftlicher und öffentlicher) digitaler Räume: staatliche Überwachung und Einschüchterung mittels nationaler Cyberkriminalitätsgesetze

Wie der 2019 erschienene Bericht «Überwachung und Menschenrechte» der UN-Sonderberichterstatterin zur Förderung und Schutz des Rechts auf Freiheit der Meinung und des Ausdrucks darlegt, sind «Privatsphäre und Meinungsäußerung im digitalen Zeitalter eng miteinander verwoben, wobei eine geschützte Online-Privatsphäre eine Möglichkeit ist, das Recht auf freie Meinungsbildung und -äußerung zu sichern» (United Nations Human Rights Council 2019a: 8). Die internationale Gesetzgebung zum Schutz der Menschenrechte definiert eindeutig, wann Eingriffe in die Privatsphäre erlaubt sind (s. ebd.: 7 f., III. A. 24.). Die Resolution der Generalversammlung der Vereinten Nationen 73/179, in der sich diese Prinzipien wiederfinden, legt zudem fest, dass «eine Überwachung digitaler Kommunikation […] nur auf Grundlage eines rechtlichen Rahmens ausgeführt werden kann, der öffentlich zugänglich, klar, präzise, verständlich und diskriminierungsfrei sein muss» (United Nations Human Rights Council 2019a: 8 f.). Werden diese Prinzipien nicht beachtet, kann zielgerichtete Überwachung zu Selbstzensur führen, kritische Berichterstattung verhindern und «Journalist*innen und Menschenrechtsaktivist*innen Möglichkeiten [nehmen], Recherche zu betreiben und Kontakt zu Informationsquellen aufzubauen

bzw. zu pflegen» (United Nations Human Rights Council 2019a: 9) – mit katastrophalen Folgen für die Demokratie und den Schutz von Menschenrechten. Die folgenden Beispiele unterstreichen die Risiken und Schäden infolge nationaler Gesetzgebung gegen Cyberkriminalität, wenn diese eine (breite und/oder zielgerichtete) staatliche Überwachung ermöglicht.

Nachdem 2022 in Libyen das Gesetz gegen Cyberkriminalität verabschiedet wurde, forderten UN-Expert*innen[26] dessen Rücknahme, da sie befürchteten, dass es «erhebliche Auswirkungen auf die Ausübung des Rechts auf Meinungs- und Redefreiheit sowie des Rechts auf Privatsphäre haben könnte» (United Nations Human Rights Council 2022: 1). Im Bericht vom März 2022, ein halbes Jahr vor der Verabschiedung des Gesetzes durch das libysche Abgeordnetenhaus, schreiben die UN-Expert*innen, das Gesetz «würde den libyschen Behörden weitreichende Befugnis erteilen, mittels Internet- und anderer digitaler Technologien Massenüberwachung von Personen durchzuführen» (ebd.: 8). Vor allem Paragraph 7 des Gesetzes wurde im Bericht und von Fachleuten der Zivilgesellschaft mit Verweis auf das Risiko staatlicher Massenüberwachung kritisiert (Human Rights Watch 2023a). Es ermögliche der Nationalen Behörde für Information und Sicherheit (NISSA), Informationen und Inhalte zu überwachen, die im oder über das Internet oder andere Technologien bereitgestellt, verbreitet oder wiedergegeben werden. Das birgt die Gefahr, dass elektronische Nachrichten von Journalist*innen, Menschenrechtsaktivist*innen und anderen kritischen (marginalisierten) Stimmen überwacht werden. Nach Gesetz ist eine Überwachung ohne gerichtliche Anordnung nur in Fällen von besonderen «‚Sicherheitsanforderungen oder Dringlichkeit› oder wenn der betreffende Inhalt gegen die ‹Sitten› verstößt» erlaubt (ebd.). Jedoch sind die entsprechenden Begriffe im Gesetz, im Widerspruch zu den bereits erwähnten Prinzipien, vage definiert und können daher breit ausgelegt werden. Darüber hinaus kann NISSA gemäß Artikel 7 offenbar ohne gerichtliche Aufsicht Webseiten und Inhalten sperren, wenn diese «rassistischer und anderweitig herkunftsbezogener Verunglimpfung bzw. religiösen oder konfessionellen Ideologien und Extremismus Vorschub leisten, die die Sicherheit und Stabilität der Gesellschaft untergraben» (United Nations Human Rights Council 2022: 10). Wie bereits im vorangegangenen Kapitel (4.1) zur breiten Anwendung nationaler Cyberkriminalitätsgesetze herausgearbeitet wurde, kann das Fehlen von definitorischer Trennschärfe und von (verfahrensrechtlichen und juristischen) Schutzmaßnahmen zu umfassenden Verstößen gegen das Recht auf Freiheit der Meinung und des Ausdrucks führen. Angesichts der mangelhaften Gleichstellung der Geschlechter in Libyen, der Illegalisierung von Homosexualität und Schwangerschaftsabbrüchen durch das Strafgesetzbuch des Landes (UN Women o. D.; UNFPA et al. 2019) ist es als wahrscheinlich zu erachten, dass Inhalte über sexuelle und

26 Der Bericht wurde verfasst von den UN-Sonderberichterstatter*innen zur Meinungsfreiheit (Irene Khan), zur Versammlungs- und Organisationsfreiheit (Clément Nyaletsossi Voule), zur Lage von Menschenrechtsaktivist*innen (Mary Lawlor) und zum Recht auf Privatsphäre (Ana Brian Nougrères).

reproduktive Gesundheit und Rechte bzw. zu anderweitigen Themen der Geschlechtervielfalt unter diese Bestimmung fallen würden. Darüber hinaus schreibt das Gesetz fest, dass die Nutzung, Produktion und Verbreitung von Verschlüsselungstechnologie von NISSA genehmigt werden muss, was die Arbeit und Sicherheit von Regierungskritiker*innen, Menschenrechtsaktivist*innen und anderen historisch oder politisch marginalisierten Gruppen weiter gefährdet (ebd.).

In Tunesien öffnet die Verordnung 54 nicht nur die Tür für die Kriminalisierung der Redefreiheit (s. Kapitel 4.1), sondern enthält auch unzureichende rechtliche Garantien zum Schutz der Privatsphäre. Dies ist eine der zentralen Erkenntnisse des passend betitelten Berichts der internationalen Organisation für digitale Rechte Access Now aus dem Jahr 2023:[27] «Redefreiheit in Tunesien in Gefahr: eine Rechtsordnung, die Schweigen begünstigt». Sowohl die Analysen von Access Now als auch von Amnesty International zeigen, dass besonders die Paragraphen 6, 9, 10 und 35 der Verordnung 54 den staatlichen Behörden weitreichende Überwachungsbefugnisse gewähren. Sie ermöglichen es zum einen, persönliche Daten zu sammeln, wenn diese zur «Wahrheitsfindung beitragen könnten», und zum anderen, diese Informationen an andere Regierungen weiterzugeben (Zaghdoudi 2023; Amnesty International 2022). Das Gesetz verpflichtet Telekommunikationsanbieter außerdem, «persönliche Daten von Kund*innen [für mindestens zwei Jahre] zu speichern und den Behörden den Zugriff darauf zu ermöglichen» (Amnesty International, 2022: 3). Laut Büro des Hohen Kommissars für Menschenrechte überschreiten solche Gesetze «die Grenzen dessen, was als notwendig und verhältnismäßig angesehen werden kann» (United Nations High Commissioner for Human Rights 2018: 6; zitiert nach ebd.).

Das ägyptische Cyberkriminalitätsgesetz von 2018 wirft ähnliche alarmierende Fragen auf, indem es Massenüberwachung autorisiert. Internetdienstanbieter sind gezwungen, «Nutzungsdaten der Kund*innen für 180 Tage zu speichern, darunter Daten zur Identifizierung der Nutzer*innen, Daten über Inhalte des Informationssystems und zu den verwendeten Geräten» (Access Now 2018). Nationale Sicherheitsbehörden dürfen auf diese Daten zugreifen und sie sichten (ebd.). Das Gesetz ebnet nicht nur Verstößen gegen das Recht auf Privatsphäre und freie Meinungsäußerung sowie der Selbstzensur den Weg (wie in den bereits erwähnten Fällen), es hat auch weitreichende Konsequenzen für den digitalen Raum, da Plattformen «zunehmend unter der ständigen Angst vor strafrechtlicher Verfolgung operieren und vorsorglich Inhalte entfernen, um ihr zu entgehen» (Ben-Hassine & Samaro 2019).

Repressive staatliche Kontrolle von Informationen und Kommunikation im digitalen Raum hat auch eine abschreckende Wirkung. So ist es wahrscheinlich, dass besonders historisch oder politisch marginalisierte Gruppen (Journalist*innen, Menschenrechtsaktivist*innen,

27 Der vollständige Bericht kann *hier* eingesehen werden.

Whistleblower*innen, Dissident*innen etc.) das Internet zunehmend seltener oder unter Selbstzensur nutzen, mit weitreichenden sowohl persönlichen als auch gesellschaftlichen Konsequenzen. Einzelpersonen, Gruppen und Organisationen wird so der Zugang zu Informationen erschwert bzw. Wege verbaut, gesellschaftliche und/oder politische Veränderungen anzustoßen, wobei auch die Online-Teilhabe am politischen Diskurs beeinträchtigt wird (beispielsweise in Form von öffentlicher Regierungskritik). Dies wirkt sich vor allem dort auf die Arbeit von Journalist*innen und Menschenrechtsaktivist*innen aus, wo autokratische Bedingungen oder demokratischer Verfall vorherrschen, die Meinungsfreiheit also bereits offline eingeschränkt ist. Mit solchen Entwicklungen auf der persönlichen Ebene werden langfristig zivilgesellschaftliche und öffentliche digitale Räume für den Austausch politischer Meinungen und Ideen weiter schrumpfen und so die Autokratisierung und der demokratische Verfall weiter verschärft.

4.3 Zugang Einzelner zum Recht, Recht auf rechtsstaatliche Verfahren und wirksamen Rechtsbehelf

Betroffene von Cyberkriminalität und alle, die unter repressiven Cyberkriminalitätsgesetzen auf diskriminierende (geschlechtsspezifische) und rechtswidrige Weise strafrechtlich verfolgt werden, machen oft zusätzliche belastende Erfahrungen bei dem Versuch, nach einer Festnahme oder Inhaftierung rechtliche Schritte zu ergreifen. (Geschlechtsspezifische) institutionelle Bias und die zumindest teilweise damit verbundenen autoritären Programme im Rechtssystem patriarchaler Gesellschaften erschweren es Frauen, LGBTQIA+ und anderen marginalisierten Gruppen, Wiedergutmachungen zu verlangen und/oder Staaten für Übergriffe zur Verantwortung zu ziehen (s. Kapitel 2).[28] Zu derartigen sich gegenseitig verstärkenden negativen Angelegenheiten zählt auch, wenn die Erfahrungen der Betroffenen von Cyberkriminalität ignoriert, heruntergespielt oder diskreditiert werden; außerdem wenn sie rechtswidrige und/oder unfaire Behandlungen erleben oder absichtliche oder unabsichtliche Reviktimisierung erfahren.

Verstärkungseffekte unterschiedlicher geschlechtsspezifischer Gewalterfahrungen

Die bereits erwähnte feministische Aktivistin Stella Nyanzi erlebte auf mehreren Ebenen des ugandischen Rechtssystems geschlechtsspezifische Gewalt. Zusätzlich zu der Verletzung ihres Rechts auf freie Meinungsäußerung (s. S. 25) verstieß Nyanzis Festnahme und Haft laut einer Stellungnahme der UN-Arbeitsgruppe gegen willkürliche Verhaftungen

28 Wie bereits in Fußnote 16 erwähnt, wird hier berücksichtigt, dass (geschlechtsspezifische) institutionelle Bias sowohl in demokratischen als auch in autoritären Staaten vorkommen – u. a. auch in dem jeweiligen Justizsystem und der Strafgesetzgebung.

(WGAD – Working Group on Arbitrary Detention) «gegen ihr Recht auf […] ein faires Verfahren, gegen die Unschuldsvermutung, gegen die persönliche Freiheit und Sicherheit und den Schutz vor Folter oder grausamer, unmenschlicher oder herabwürdigender Behandlung» (Columbia University o. D.). Nachdem sie von Polizeikräften in Zivil gewaltsam festgenommen worden war, wurde Nyanzi inhaftiert und physisch misshandelt. Außerdem wurden ihr über 18 Stunden sowohl der Kontakt zu einem Rechtsbeistand als auch zu Menstruationsprodukten verweigert (ebd.). In einem Interview mit dem Guardian berichtete Nyanzi von weiteren Fällen absichtlicher, eindeutig geschlechtsspezifischer Gewalt im Gefängnis: «Wir mussten uns vor anderen [Gefangenen] ausziehen» (Mwesigwa 2017).

Cyberkriminalitätsgesetze als Baustein eines institutionellen Unterdrückungsapparats gegen Kritik

Amnesty International[29] hat untersucht, wie die Anwendung des Gesetzes Nr. 17 in Jordanien im Zusammenhang mit pro-palästinensischen Protesten zu einer Verschärfung der (angedrohten) Repression geführt hat (s. S. 29). Die zwei nachfolgenden Fälle zeigen, wie Cyberkriminalitätsgesetze als Teil eines Apparats repressiver Maßnahmen dazu missbraucht werden können, Kritiker*innen einzuschüchtern bzw. zu verfolgen und den Zugang zu Rechtsstaatlichkeit und Rechtsmitteln sogar noch weiter zu erschweren. Das sogenannte Gesetz zur Verbrechensverhütung in Jordanien ermöglicht eine Administrativhaft mit begrenzter gerichtlicher Prüfung – ohne Anklage oder Gerichtsverfahren. Damit untergräbt es die Garantien für ein faires Verfahren, die das jordanische Strafprozessrecht eigentlich vorsieht (Amnesty International 2024b). Nachdem der Aktivist Majd al-Farraj auf Social Media pro-palästinensischen Content gepostet hatte, wurde er im Dezember 2023 gemäß dem jordanischen Cyberkriminalitätsgesetz Nr. 17 angeklagt. Ein Strafgericht sprach ihn zwar später frei, während eines Protestes wurde er jedoch erneut verhaftet und über einen Monat in Administrativhaft festgehalten. Eine ähnliche Strategie nutzten die jordanischen Behörden, um den Aktivisten Samer al-Qassem im April 2024 zu verhaften, nachdem er auf TikTok ein Video über palästinensische Geflüchtete geteilt hatte. Laut des Berichts von Amnesty International wurde er drei Wochen nach der Festnahme zunächst auf Bewährung freigelassen, bis der Gouverneur von Amman forderte, ihn für einen weiteren Monat in Administrativhaft zu nehmen (2024b). Am 30. Juni 2024 wurde al-Qassem gemäß Gesetz Nr. 17 angeklagt, weil er «Social-Media-Plattformen zur Aufwiegelung genutzt und den gesellschaftlichen Frieden bedroht hatte», was zu einer dreimonatigen Haftstrafe und einer Geldbuße von 5 000 jordanischen Dinar (ca. 6 200 Euro) führte (ebd.). Human Rights Watch hat ähnliche Fälle dokumentiert. Jordanische Anwält*innen und Aktivist*innen berichteten gegenüber Amnesty, dass «ungeachtet einer Freilassung auf Anordnung der Staatsanwaltschaft oder Gerichten das Innenministerium Menschen erneut festnehmen ließ oder durch Missbrauch von Administrativhaft in Gewahrsam hielt. Dabei seien

29 Dieser Abschnitt beruht auf dem Bericht von Amnesty International vom 13. August 2024: «*Jordan's new Cybercrimes Law stifling freedom of expression one year on*».

Gefangene gezwungen worden, Erklärungen zu unterschreiben, die ihnen die Teilnahme oder die Initiierung von Protesten unter Androhung einer Geldstrafe von 50 000 jordanischen Dinar untersagten» (ca. 62 000 Euro; Human Rights Watch 2024b).

Mangelhafte Unterstützung für Betroffene von Cyberkriminalität trotz gesicherten Rechtszugangs

In den meisten Länder fehlen für Betroffene von Cyberkriminalität noch immer landesweite Hilfsangebote, die deren Bedürfnisse und Erfahrungen adäquat abbilden; auch in Ländern mit formal zugänglichem Rechtssystem, in denen derartig Betroffene das Recht auf rechtsstaatliches Verfahren und wirksamen Rechtsbehelf wahrnehmen können. Oft werden Betroffene von Vertreter*innen der Justiz oder der gesamten Gesellschaft retraumatisiert und reviktimisiert (Leukfeldt, Notté & Malsch 2019; Robalo & Abdul Rahim 2023).

Eine 2021 durchgeführte Studie zu den Folgen der Viktimisierung von Betroffenen von Hackingangriffen zeigt nicht nur die direkten negativen Folgen auf (z. B. Angstzustände, Depressionen, Gefühl der Verletzung der persönlichen Sicherheit, Privatsphäre und des Kontrollverlusts), sondern arbeitet auch indirekte Langzeitfolgen für die mentale Gesundheit von Betroffenen heraus (Palassis, Speelman & Pooley 2021). Während einige Betroffene von Hackingangriffen von einer mangelnden Unterstützung seitens der Service-Provider berichten, fühlten sich andere allgemein hilf- und machtlos und erlebten sekundäre Viktimisierung durch Schuldumkehr (victim-blaming) (ebd.). Ähnliche Probleme und entsprechende Kritik an Exekutiv- und anderen Staatsorganen wurden auch von Betroffenen anderer Cyberverbrechen formuliert. Zu erwähnen ist hier Sextortion, also die sexuelle Nötigung und Erpressung im Internet, ein geschlechtsspezifisches Cyberverbrechen, das in letzter Zeit weltweit vor allem unter Jugendlichen drastisch zugenommen hat, wie etwa in den USA oder dem Vereinigten Königreich (McCubbin 2024; Smith & Crawford 2024; Tidy 2024). Sextortion kann Betroffene sogar zum Suizid führen (Garvilovic Nilsson et al. 2019). Fehlende Polizeiausbildung im geschlechtersensiblen Umgang mit Betroffenen führt hierbei oft dazu, dass diese sich «wie Kriminelle fühlen» (McCubbin 2024). Neben (nach Geschlecht aufgeschlüsselten) Statistiken und rechtlicher Hilfe für Betroffene (von geschlechtsspezifischer Cyberkriminalität) fehlen auch landesweite psychologische/emotionale Hilfsangebote (z. B. Hilfsgruppen). Außerdem versäumt es der Staat, die Öffentlichkeit für dieses Thema zu sensibilisieren. Besonders der letzte Punkt könnte entscheidend dazu beitragen, Stigmatisierung entgegenzuwirken und Betroffene zu ermutigen, der Polizei beispielsweise Fälle von Sextortion zu melden, und dabei die Gefahr einer gesellschaftlichen Reviktimisierung zu reduzieren.

Daher suchen sich Betroffene von Cyberkriminalität immer wieder Unterstützung bei landes- oder weltweit agierenden Organisationen der Zivilgesellschaft. So informiert die Wohltätigkeitsorganisation Victim Support öffentlich über Verbrechen und das Strafjustizsystem und bietet kostenlose, unabhängige und vertrauliche Betroffenenberatung an. Access Now, eine Organisation für digitale Rechte, hat neben anderen Maßnahmen auch

die Digital Security Helpline ins Leben gerufen, die rund um die Uhr in neun Sprachen erreichbar ist. Die Digital Rights Foundation aus Pakistan bietet für Betroffene von Cyberharassment über die Cyber Harassment Helpline Rechtsberatung, psychologischen Beistand und Verweisberatung an. SMEX, eine libanesische NGO für digitale Rechte, berät und unterstützt über den Helpdesk – SMEX (Menschenrechts-)Aktivist*innen, Journalist*innen und andere marginalisierte Gruppen aus Westasien und Nordafrika bei internetbezogenen Vorfällen.

4.4 Verstärkende und kumulative Effekte

Die bereits besprochenen Fälle zeigen, wie stark Gesetze zur Bekämpfung von Cyberkriminalität und eine patriarchale, repressive Justiz die freie Meinungsäußerung, das Recht auf Privatsphäre und Zugang zum Recht sowie die Sicherheit von vulnerablen und marginalisierten Gruppen on- und offline beeinträchtigen. In der intersektional feministischen Perspektive offenbaren sich aber noch weitere verstärkende und kumulative Effekte von Cyberkriminalität und/oder Gesetzen zu ihrer Bekämpfung, also Effekte, die sich verschärft bei denjenigen auswirken, die bereits repressiven Cyberkriminalitätsgesetzen zum Opfer fallen.

Geschlechtsspezifische Schädigungen durch Cyberkriminalität, die Gesetze zu ihrer Bekämpfung verstärken

Yamen, ein 25-jähriger homosexueller Mann aus Jordanien, und Aya, eine 17-jährige Influencerin, mussten das Worst-Case-Szenario verstärkender und kumulativer Effekte erleben. Hier wurde eine bereits marginalisierte, von geschlechtsspezifischer Cyberkriminalität betroffene Person zusätzlich durch diskriminierende staatliche Übergriffe gegen sexuelle und geschlechtliche Minderheiten geschädigt.

Yamen wurde das Ziel von Sextortion, als ein Mann, den er auf einer Dating-App kennengelernt hatte, ihm mit der Veröffentlichung eines Videos drohte, das ihn beim Cybersex zeigte. Daraufhin erstattete er Anzeige bei der jordanischen Sondereinheit Cyberkriminalität (Jain 2024). Die Anzeige wurde jedoch nicht nur ignoriert: Yamen – der sich vor geschlechtsspezifischer Online-Gewalt schützen wollte – wurde nach Paragraph 9 des jordanischen Cyberkriminalitätsgesetzes Nr. 17 wegen «Anbahnung von Prostitution im Internet» angeklagt (ebd.). Wie er in einem Interview mit Human Rights Watch angibt, wurde Yamen während des Gerichtsprozesses erneut geschlechtsspezifisch diskriminiert, als er von Staatsbeamt*innen als «derjenige, der den Mann verführen wollte» «feminisiert» wurde (Human Rights Watch 2023c). Yamen wurde zu einem Monat Haft und einer Geldstrafe verurteilt.

2022 war auch die auf Social Media als «Menna Abdelaziz» bekannte Aya nach einem Fall von Sextortion von sich gegenseitig verschärfenden Auswirkungen betroffen. Wie Human

Rights Watch berichtete, wurde die 17-Jährige von einer Gruppe Männer und Frauen zusammengeschlagen und von einigen der Männer vergewaltigt. Sie filmten die Tat und erpressten Aya danach mit dem Videomaterial. Nachdem Aya in einem Videopost davon erzählt hatte, wurde sie von den ägyptischen Behörden verhaftet. Zwei Tage später hieß es in einer vom «Büro des Generalstaatsanwalts veröffentlichten Erklärung, die Staatsanwaltschaft habe ihre Inhaftierung zum einen veranlasst, um in dem Fall der gegen Aya verübten sexuellen Gewalt, zum anderen aber auch gegen sie als Verdächtige zu ermitteln, da sie in ihren Videos Sittenwidrigkeiten begangen haben soll» (Human Rights Watch 2020). Obwohl die an dem Übergriff beteiligten Männer und Frauen vor Gericht gestellt wurden und Aya in einem Frauenhaus unterkam, wurden die Ermittlungen wegen sittlicher Vergehen unter dem Cyberkriminalitätsgesetz Nr. 175 von 2018 fortgesetzt. Das hatte ernsthafte und sich gegenseitig verschärfende Auswirkungen. Die zusätzliche Beschneidung von Ayas Recht auf freie Meinungsäußerung und die damit verbundene (Re-)Viktimisierung, der sie unter dem Gesetz Nr. 175 ausgesetzt war, trug entscheidend zu den psychologischen und physischen Folgen bei, die sie als Betroffene von sexueller Gewalt und Sextortion erleben musste.

Human Rights Watch hat die ägyptischen Behörden aufgefordert, Aya unverzüglich freizulassen und «für ihre Sicherheit und eine angemessene Behandlung zu sorgen» (Human Rights Watch 2020). Dabei verwies die Organisation auf internationales Recht, das «die Inhaftierung von Kindern ausschließlich als allerletztes Mittel und für die kürzest mögliche Zeitspanne gestattet» (ebd.).

Staatliche Einschränkungen der freien Meinungsäußerung, durch die wiederum private Akteur*innen zivilgesellschaftliche Räume aktiv einschränken

Kumulative, also sich gegenseitig verstärkende Effekte wurden im Zusammenhang mit dem jordanischen Cyberkriminalitätsgesetz Nr. 17 deutlich. Kurz nach Verabschiedung des Gesetzes informierten zwei unabhängige Nachrichtenportale Amnesty International, dass sie aufgrund Paragraph 33 des Gesetzes ihre Kommentarspalten geschlossen hatten. Dieser Paragraph «befuge Staatsanwaltschaft oder Gericht, jedem Webseitenbetreiber, jeder Social-Media-Plattform und jeder für einen öffentlichen Account zuständigen Person anzuordnen, Inhalte, die gegen das Gesetz verstoßen, zu entfernen oder zu blockieren, sowie die Person, die den Inhalt erstellt oder verbreitet hat, vorübergehend zu sperren und relevante Informationen wie persönliche Daten weiterzugeben» (Amnesty International 2023). Hatte, wie bereits beschrieben, schon das Gesetz Nr. 17 die freie Meinungsäußerung vieler Social-Media-User*innen besonders im Zusammenhang mit pro-palästinensischen Protesten und Solidaritätsbekundungen online eingeschränkt, sehen sich dieselben User*innen nun mit zusätzlichen Einschränkungen konfrontiert, da Medienunternehmen die Möglichkeiten zur Meinungsäußerung zu Nachrichteninhalten aus Angst vor strafrechtlicher Verfolgung weiter begrenzen. Entwicklungen wie diese führen zum kontinuierlichen Verschwinden digitaler Räume der Zivilgesellschaft (s. auch Hassan &

Hellyer 2024), «wo doch in Jordanien kaum noch Räume und Foren für freie Meinungsäußerungen zur Verfügung stehen» (Amnesty International 2023). Das kann als sich gegenseitig verstärkende Auswirkungen gewertet werden.

In diesem Kapitel wurde herausgearbeitet, wie nationale Gesetzgebung zur Bekämpfung von Cyberkriminalität instrumentalisiert werden kann, um staatliche Übergriffe vorwiegend gegen Frauen, LGBTQIA+, (Menschenrechts-)Aktivist*innen, Journalist*innen sowie andere Kritiker*innen und marginalisierte Gruppen zu ermöglichen. Statt Bürger*innen sowie deren Grundfreiheiten und Menschenrechte zu schützen, nutzen viele, insbesondere autoritäre Regierungen vage formulierte und unverhältnismäßig breit anwendbare Cyberkriminalitätsgesetze aus, um abweichende Meinungen zu unterdrücken, freie Meinungsäußerungen im digitalen Raum zu kriminalisieren und gezielte und/oder massenhafte Staatsüberwachung durchzusetzen. In Verbindung mit dem für marginalisierte Gruppen bereits eingeschränkten Rechtszugang führt dies häufig zu Selbstzensur und zum Verschwinden zivilgesellschaftlicher digitaler Räume. Diese Gesetze verweisen häufig auf Konzepte wie «Sittlichkeit» oder «nationale Sicherheit», rechtfertigen die Einschränkung (digitaler) Menschenrechte und reproduzieren und festigen ggf. offline diskriminierende patriarchale und autokratische Machtstrukturen in und mithilfe von digitalen Räumen. In diesem Kapitel wird daher die Notwendigkeit von Cyberkriminalitätsgesetzen deutlich, die sich an grundlegenden Menschenrechten orientieren und Rechte wie auf Privatsphäre, Diskriminierungsfreiheit und die freie Meinungsäußerung sichern.

5 Die UN-Konvention zur Bekämpfung von Cyberkriminalität

Auf Grundlage der Lehren und Erkenntnisse aus den Untersuchungen der nationalen Kontexte erfolgt in diesem Kapitel eine Analyse der UN-Konvention gegen Cyberkriminalität aus einer intersektional feministischen Perspektive. Zur Vorbeugung negativer Auswirkungen wie in Kapitel 4 angeführt sollen neben den Chancen des Abkommens auch dessen Risiken, Stolpersteine und Missbrauchspotenzial herausgearbeitet werden.

Die UN-Konvention gegen Cyberkriminalität

Auf Initiative Russlands beschloss die UN-Vollversammlung 2019 im Beschluss 74/247 die Einberufung eines zeitlich unbegrenzten, internationalen Ad-Hoc-Ausschusses für die Ausarbeitung einer Konvention zur Bekämpfung von Cyberkriminalität (AHC – Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes). Nach einer ersten, rein organisatorischen Sitzung im Mai 2021 nahm die AHC zur Ausarbeitung einer umfassenden internationalen Konvention zur Bekämpfung des Gebrauchs von IKT zu kriminellen Zwecken ihre inhaltliche Arbeit im Februar 2022 auf. Im August 2024 wurde auf einer abschließenden Sitzung ein erster Entwurf der Konvention vorgelegt und im Dezember desselben Jahres von der Vollversammlung angenommen.[30] Vertreter*innen verschiedener Interessengruppen aus der Zivilgesellschaft, der Privatwirtschaft, der Wissenschaft und der Tech-Community brachten sich gemäß dem vorgeschriebenen Verfahren zur Einbeziehung verschiedener Interessengruppen in die Verhandlungen ein (AHC 2021). Obwohl dieses Vorgehen für seinen inklusiven Ansatz gelobt wurde, mussten die Interessengruppen letztendlich feststellen, dass das Abschlussdokument nur unzureichend auf die von ihnen geäußerten Bedenken einging und darum anfällig für Missbrauch ist.[31]

30 Für einen genaueren Überblick zur Verabschiedung der Konvention gegen Cyberkriminalität s. die *offizielle Homepage des AHC*.

31 Unter den Interessengruppen waren mehrere Menschenrechts- und Pressefreiheitsorganisationen (s. z. B. der *offene Brief an die EU*, mitunterzeichnet von CFFP; *Access Now 2024*; *Human Rights Watch 2024d*), das Büro des Hohen Kommissars für Menschenrechte (2024), Sicherheitsforscher*innen (*Gullo 2024*), das Advisory Network of the Freedom Online Coalition (*2024*), die Tech-Industrie (*Cybersecurity_Tech_Accord 2024a*; Microsoft 2024) und andere Vereinigungen der Privatwirtschaft (*International Chamber of Commerce 2024*).

5.1 Geschlechter und die UN-Konvention gegen Cyberkriminalität

Obwohl einige Staaten sich dagegen aussprachen, dass die Konvention explizit auf Geschlecht eingeht, war dies bei den Diskussionen des AHC ein zentrales Thema. In diesen Debatten wurde die komplexe Verwobenheit von Geschlecht und Cyberkriminalität herausgestellt (Hakmeh 2025). Mehrere Mitgliedstaaten sprachen sich für Bestimmungen aus, die die spezifischen Risiken berücksichtigen, denen Frauen und Mädchen im Zusammenhang mit technologiegestützter geschlechtsspezifischer Gewalt (TFGBV) sowie Jungen, insbesondere im Kontext von Abbildungen sexuellen Kindesmissbrauchs (CSAM), im digitalen Raum ausgesetzt sind. Es wurde unterbreitet, die Gleichstellung der Geschlechter als Teil der Menschenrechte in der allgemeinen Erklärung festzuschreiben und das Thema Geschlecht in der gesamten Konvention zu verankern (Chatham House 2022). In der Präambel des endgültigen Texts wird bekräftigt, wie wichtig das Mitdenken von Geschlecht für die Prävention und Bekämpfung von Cyberkriminalität ist. Die Notwendigkeit, geschlechtsspezifische Gewalt im digitalen Raum gezielt anzugehen, wird insbesondere in Artikel 53 (h) zu Präventionsmaßnahmen deutlich. Dort wird vorgeschlagen, «in Abstimmung mit der nationalen Gesetzgebung Strategien und Leitlinien zu entwickeln, um geschlechtsspezifische Gewalt, die durch die Nutzung von IKT verübt wird, zu verhindern und dabei bei der Entwicklung von Präventivmaßnahmen die besonderen Umstände und Bedürfnisse von Menschen in vulnerablen Situationen zu berücksichtigen». Obwohl sich darin das Verständnis erkennen lässt, dass Menschen aufgrund ihres Geschlechts unterschiedlich von Cyberkriminalität betroffen sind, scheitert das Abkommen daran, breitere geschlechtersensible und -bewusste Ansätze festzuschreiben. Im UN-Rahmen wären klar eindeutige und bindende Formulierungen wünschenswert, die Vertragsstaaten explizit verpflichten, sich gleichzeitig aktiv für den Schutz vor Diskriminierung und für eine Gleichstellung der Geschlechter einzusetzen.

5.2 Von Cyberkriminalität zu Datenzugriff: Verallgemeinerungsgefahr durch umfassenden Geltungsbereich

Im vorangegangenen Kapitel wurde gezeigt, wie breit gefasste Bestimmungen und vage Definitionen zu beliebigem und willkürlichem Vollzug führen können, der sich besonders oft gegen Frauen, marginalisierte Gruppen und Einzelpersonen in vulnerablen Situationen richtet. Trotz umfangreicher Belege und erheblicher Risiken wird in der Konvention ein breiter Geltungsbereich angelegt, der vor allem in den Abschnitten zur internationalen Zusammenarbeit und Verfahrensmaßnahmen deutlich wird. Im Zusammenspiel mit minimalen Schutzmaßnahmen kann dieses Abkommen unbeabsichtigte, nachteilige Folgen nach sich ziehen. So einigten sich die Staaten beispielsweise gemäß Artikel 35 (c) zu

allgemeinen Grundsätzen der internationalen Zusammenarbeit darauf, über die in der Konvention festgelegten Straftatbestände hinaus zu kooperieren und die Zusammenarbeit auf das «Sammeln, Erlangen, Sichern und Teilen von Beweismitteln in elektronischer Form in Bezug auf jede schwere Straftat auszuweiten». Gemäß Artikel 2 (h) zur Terminologie wird eine schwere Straftat als «eine Handlung definiert, die mit einer Höchststrafe von mindestens vier Jahren Freiheitsentzug oder einer schwereren Strafe geahndet werden kann». Auch wenn diese Definition auf das Übereinkommen gegen die grenzüberschreitende organisierte Kriminalität zurückgeht (UNTOC – UN Convention against Transnational Organized Crime and the Protocols thereto), könnte die Anwendung auf Cyberkriminalitätsdelikte zu einer bis dato ungekannten Ausweitung des Geltungsbereichs des neuen Abkommens führen (Tennant & Oliveira 2024). Angesichts der Tatsache, dass ein Großteil des modernen Lebens online stattfindet, wird es unter jeder nationalen Gesetzgebung elektronische Beweise für nahezu jede Straftat geben.

Die für die Verhinderung möglichen Missbrauchs geeignetste Bestimmung findet sich in Artikel 6. Darin heißt es, dass «in Einklang mit geltendem internationalen Menschenrecht nichts in diesem Abkommen dazu herangezogen werden darf, Menschenrechte oder Grundfreiheiten wie das Recht auf Meinungs-, Gewissens-, Religions- und Glaubensfreiheit sowie das Recht auf friedliche Versammlung und Vereinigung zu beschneiden». Diese allgemeine Bestimmung gilt für den gesamten Text und sollte für die Anwendung des Abkommens und seine Übertragung in staatliche Rechtssysteme bestimmend sein (Walker & Oliveira 2024). Die restlichen Bestimmungen zum Schutz von Menschenrechten sind an bestimmte Abschnitte gebunden. Hinsichtlich internationaler Zusammenarbeit legt Artikel 40 (22) zu allgemeinen Grundsätzen und Vorgehensweisen bei der gegenseitigen Rechtshilfe fest, dass «nichts in diesem Abkommen so ausgelegt werden darf, dass es eine Verpflichtung zur gegenseitigen Rechtshilfe begründet, wenn der ersuchte Staat stichhaltige Gründe für die Annahme hat, dass das Gesuch zu dem Ziel gestellt wurde, eine Person aufgrund von Geschlecht, Race, Sprache, Religion, Nationalität, Herkunft oder politischer Meinung zu verfolgen oder zu bestrafen […]». Vor allem für die Rechte und Freiheiten von Personen, die bereits überdurchschnittlich oft marginalisiert werden oder Angriffen ausgesetzt sind, bietet diese Klausel unter Umständen keinen wirksamen Schutz. Stellt das Vergehen in zwei Staaten eine Straftat dar, die sich zu einer Kooperation und damit beispielsweise zum Austausch elektronischer Beweise entschlossen haben, kann das Dokument die Türen für möglichen Missbrauch öffnen. Je nach Auslegung können selbst Bestimmungen, die sich nicht explizit auf das Thema Geschlecht beziehen, erhebliche geschlechtsspezifische Wirkung entfalten.

Zur Veranschaulichung: Die Konvention könnte Strafverfolgungsbehörden dazu verpflichten, bei der Verfolgung von LGBTQIA+ und deren Unterstützer*innen zu kooperieren. In Russland kann die Zugehörigkeit zur «internationalen LGBT-Bewegung» zu Anklagen wegen Extremismus führen (Human Rights Watch 2024c). Handlungen wie das Zeigen der Regenbogenflagge, die als «Symbol einer extremistischen Gruppierung» gewertet wird, werden unter Umständen strafrechtlich verfolgt. Bei der ersten Verurteilung

drohen bis zu fünfzehn Tage, bei Wiederholung bis zu vier Jahre Haft. Eine Wiederholungstat würde nach dem Abkommen als «schwere Straftat» gelten und somit eine Kooperation zwischen Strafverfolgungsbehörden verschiedener Staaten ermöglichen (Rodriguez 2024). Jegliche Sichtbarkeit oder Zugehörigkeit zur LGBTQIA+-Community könnte somit das Sammeln elektronischer Beweismittel – einschließlich Daten zu Traffic, User*innen und sogar zum Inhalt – und deren Weitergabe zwischen Staaten rechtfertigen. Ähnliche Überlegungen gelten für den Zugang zu sexueller und reproduktiver Gesundheit. In 22 Ländern gilt ein vollständiges Verbot von Schwangerschaftsabbrüchen, in vielen weiteren sind diese nur unter bestimmten Bedingungen gestattet (Council on Foreign Relations 2024). Das Abkommen könnte theoretisch ermöglichen, sensible Daten zu sammeln, wie z. B. Standortdaten, die über Besuche in Gesundheitseinrichtungen Aufschluss geben, Daten aus Zyklus-Apps oder auch Browserverläufe von Personen, die nach Angeboten der sexuellen und reproduktiven Gesundheitsversorgung suchen (Chatham House 2022; Gollan 2023).

Die im Vertrag enthaltenen Maßnahmen zum Schutz von Daten und Privatsphäre sind angesichts der vielfältigen, komplexen und weitreichenden Risiken unzureichend. In einem Absatz der Präambel wird das Recht auf Schutz vor willkürlichen oder rechtswidrigen Eingriffen in die Privatsphäre sowie die Bedeutung des Schutzes personenbezogener Daten betont. Mit diesem Hinweis wird zwar das Risiko anerkannt, dass Regierungen durch das Abkommen willkürlich in die Privatsphäre eingreifen könnten, jedoch fehlt das notwendige Gewicht, dies wirksam zu verhindern. Bei der Umsetzung des Abkommens sollten spezifisch verstärkte Datenschutzvorkehrungen für besonders schützenswerte Formen der Kommunikation gelten, darunter medizinische, juristische, religiöse oder im öffentlichen Interesse stehende Inhalte. Diese Differenzierung ist notwendig, um Rechte und Wohlergehen von Frauen und Menschen mit diverser Geschlechtsidentität, -ausdruck und sexueller Orientierungen zu wahren, nicht zuletzt in Rechtssystemen, in denen der Zugang zu Abtreibung und/oder die Sichtbarkeit von LGBTQIA+-Identitäten aktuell illegal ist (Chatham House 2022).

5.3 Risiken des Datenaustausch und gegenseitiger Rechtshilfe

Auf Grundlage der UN-Konvention werden weltweit mehr Regierungen im Namen des Kampfes gegen Cyberkriminalität auf immer mehr persönliche Daten zugreifen. Zwar ist der Austausch elektronischer Beweismittel zwischen Strafverfolgungsbehörden notwendig, um grenzüberschreitende Cyberkriminalität zu bekämpfen, das Abkommen schwächt jedoch den Spielraum demokratischer Staaten, problematische Anfragen von autoritären Regimen abzulehnen. Die Voraussetzungen internationaler Zusammenarbeit können Länder darin einschränken, andere Staaten von der Beteiligung an unzulässigen, repressiven Ermittlungen autoritärer Regime abzubringen (Adams & Podair 2024). Durch Artikel 40

sind Vertragsstaaten dazu verpflichtet, bestmögliche Rechtshilfe im Rahmen von Ermittlungen zu leisten, die unter das Abkommen fallen. Da die allgemeinen Grundsätze und Verfahren zur Rechtshilfe breit und ohne klare Schutzbestimmungen formuliert sind, können staatlichen Behörden ohne wirksame Transparenz- oder Rechenschaftspflichten agieren. Im Prinzip können Staaten zwar eine Zusammenarbeit ablehnen, wenn die Tat nur im anderen Land einen Straftatbestand darstellt, sind daran aber nicht gebunden. Die Regelung zur Rechtshilfe wird auch dadurch nicht beschränkt, ob sich die Daten überhaupt auf dem Territorium des ersuchten Staates befinden. Darüber hinaus enthält der Artikel 22 eine auch als passives Opferstaatsprinzip bekannte Bestimmung, die es Staaten ermöglicht, Rechtsprechung auch außerhalb ihres Staatsgebietes auszuüben, wenn Staatsangehörige dort zu Schaden gekommen sind. Diese Regelung birgt das Risiko, hiermit zu legitimieren, dass Staaten ihre Strafgesetze gezielt zur Verfolgung von Personen im Ausland nutzen (Scher-Zagier 2024).

Viele der Personen, deren Informationen weitergegeben werden, sind sogenannte «Personen von besonderem polizeilichem Interesse», gegen die jedoch nie ein Strafverfahren eingeleitet wird. Keine Bestimmung der Konvention verpflichtet die zuständigen Behörden dazu, diese Personen zu informieren, wenn Regierungen den Zugriff auf ihre privaten Daten beantragt und erhalten haben. Dadurch wird den Betroffenen die Möglichkeit genommen, sich zu schützen und ihre Rechte zu verteidigen (Cybersecurity Tech Accord 2024b). Umfassende Verfahrensbefugnisse ohne die nötigen Vorkehrungen zur Sicherung von Transparenz und Kontrolle bergen ein erhebliches Risiko für staatliche Übergriffe. Vor diesem Hintergrund sind die Bestimmungen der Konvention höchst problematisch, die Staaten das Recht einräumen, für eine Verurteilung «relevante Daten zu sammeln oder aufzuzeichnen» sowie Dienstanbieter zur Herausgabe belastender Informationen oder Dokumente zu «zwingen». Der Vertragstext erleichtert zudem geheime Zugriffe auf gesicherte Systeme, die Abschöpfung von Daten außerhalb des Staatsgebiets und das verdeckte Sammeln von Echtzeitdaten ohne hinreichende und belastbare Bedingungen und Schutzmaßnahmen, mit denen sich sicherstellen ließe, dass Staaten bei der Bekämpfung von Cyberkriminalität nur im angemessenen notwendigen Rahmen handeln. Grundsätze der Notwendigkeit und Angemessenheit finden in der Konvention kaum Erwähnung. Bei Fragen zum Schutz von Menschenrechten wird auf nationale Gesetzgebung statt auf internationale Menschenrechte verwiesen. Wenn Länder ihre internationalen Verpflichtungen nicht in innerstaatliches Recht übertragen oder Menschenrechte in der Praxis verletzen, verpflichtet die Konvention die Behörden nicht dazu, bei der Umsetzung der darin festgeschriebenen Bestimmungen internationale Standards zu berücksichtigen. Dass Länder mit negativer Menschenrechtsbilanz wie Belarus, China, Iran, Nicaragua, Kuba und Russland zu den stärksten Befürwortern der Konvention zählen, trägt nicht gerade dazu bei, das Vertrauen in sie zu stärken. In letzter Minute forderte der Iran sogar noch eine Abstimmung darüber, Anmerkungen zum Schutz von Menschenrechten aus dem Text zu streichen – jedoch erfolglos (Walker & Oliveira).

Die Konvention schafft Anreize für die Beschaffung von Überwachungstechnologien, die für Ermittlungen gegen Cyberkriminalität notwendig sind. Während der Einsatz von Dual-Use-Technologie und Überwachungssoftware für bestimmte Ermittlungszwecke legitim sein kann, begünstigt er unbeabsichtigt staatliche Übergriffe sowohl in Form von gezielter als auch massenhafter Überwachung sowie durch fortgeschrittene Technologien der Datenerfassung und der Zensur. Artikel 28 zur Durchsuchung und Beschlagnahme gespeicherter elektronischer Daten verpflichtet die Vertragsstaaten, die zuständigen Behörden mit der Befugnis auszustatten, Überwachungskapazitäten für gespeicherte elektronische Daten innerhalb ihres Hoheitsgebiets zu erwerben. Laut Artikel 29 und 30 sind Staaten darüber hinaus verpflichtet, Übergriffe wie Echtzeitüberwachung von Daten zu Traffic und Inhalten technisch zu ermöglichen. Dabei müssen Staaten weder Menschenrechtsfolgen prüfen, noch wird die Inanspruchnahme kommerzieller Cyber-Überwachungstechnologie untersagt, was wiederum dem globalen Markt für Cyber-Söldnertum zusätzlichen Auftrieb verleiht.

5.4 Gefahren rechtsverbindlicher Regelungen zu Cyber-Extremismus und -Terrorismus

In den Verhandlungen zum Abkommen wurde intensiv über die Aufnahme von inhaltsbezogenen Straftaten wie extremismus- und terrorismusbezogene Straftaten und die Verbreitung von Falschinformationen diskutiert.[32] Da das internationale Recht keine universellen Definitionen von Terrorismus und Extremismus kennt, sahen Kritiker*innen hier Grund zur Besorgnis. Oft haben Staaten die breite Auslegbarkeit dieser Begriffe zur Rechtfertigung von Repressionen dafür genutzt, das Recht auf freie Meinungsäußerung, Versammlungs-, Meinungs- und Glaubensfreiheit unverhältnismäßig zu beschneiden. Die bereits beschriebenen Fälle (s. Kapitel 4) haben gezeigt, dass nach Cyberkriminalitätsgesetzen geahndete inhaltsbezogene Straftaten weitreichende Folgen haben, insbesondere für Frauen, die in patriarchalen und autoritären Regimen verfolgt werden, sowie für marginalisierte Gruppen und einzelne Menschenrechtsaktivist*innen, Journalist*innen und Oppositionelle. Wie die UN-Sonderberichterstatterin für den Schutz der Menschenrechte bei Terrorismusbekämpfung hervorhebt, «wird in vielen Teilen der Welt jede Form von Meinungsäußerung, die der offiziellen Haltung des Staates widerspricht, Menschenrechtsverletzungen thematisiert oder auf mögliche Verbesserungen der Menschrechtslage hinweist, als Akt des Terrorismus, gewaltbereiter Extremismus oder als umfassende ‹Bedrohung der nationalen Sicherheit› gewertet, was oft sowohl Terrorismus als auch Extremismus einschließt». Einige Staaten unterdrücken mithilfe dieser Bestimmungen die Zivilgesellschaft und bringen Aktivist*innen für LGBTQIA+-Rechte damit zum Schweigen (United Nations Human Rights Council 2019b). Ohne klar abgegrenzte, eng gefasste und

32 Das konsolidierte Verhandlungsdokument findet sich *hier* (Stand 21. Januar 2023).

menschenrechtskonforme Definitionen würden Terrorismusbezüge in der Konvention Gefahr laufen, bereits zu breit gefasste Gesetze zur Terrorismusbekämpfung auch auf Cyberkriminalität zu erweitern und dadurch weitere Menschenrechtsverletzungen zu begünstigen.

Besorgniserregend ist zudem, dass einige Staaten zunehmend zu Mitteln und Gesetzen zur Bekämpfung von Cyberkriminalität greifen, um Aktivist*innen, Journalist*innen, Whistleblower*innen, Oppositionsangehörige und Minderheiten unter dem Vorwand nationaler Sicherheit, des Erhalts der öffentlichen Ordnung oder der Bekämpfung von Extremismus, Terrorismus oder sogenannter Fakenews zu verfolgen. Derartige Bezüge im internationalen Rechtsrahmen einer Konvention würden Regierungen ermöglichen, repressive Gesetze zur Kriminalisierung freier Meinungsäußerung im digitalen Raum zu verabschieden und dies mit Verweis auf internationale Institutionen wie die UN zu legitimieren. Im endgültigen Vertragstext konzentriert sich das Kapitel zur Kriminalisierung mit den konkret zu bekämpfenden Straftaten vor allem auf cyberabhängige Delikte. Die Konvention erlaubt jedoch Zusatzbestimmungen (Artikel 61 und 62), ohne zu definieren, welche Sachverhalte dadurch geregelt werden dürfen. So lässt sich der Geltungsbereich mithilfe zukünftiger Zusatzregelungen – wie von Russland in den Verhandlungen vorgeschlagen – auch auf Äußerungsdelikte ausweiten (Walker & Oliverira 2024).

5.5 CSAM und NCSII

Zu den inhaltsbezogenen Straftatbeständen im Kapitel zur Kriminalisierung zählen Vergehen im Zusammenhang mit kinderpornografischem Material bzw. Darstellungen des sexuellen Missbrauchs von Kindern (Artikel 14), Anbahnung oder Grooming mit dem Ziel der Begehung sexueller Straftaten an Kindern (Artikel 15) sowie die nicht einvernehmliche Verbreitung intimer Bilder (Artikel 16). Unter CSAM (Child Sexual Abusive Material) werden Inhalte zusammengefasst, die sexuellen Missbrauch oder sexuelle Ausbeutung von Kindern oder Jugendlichen zeigen oder auf andere Weise damit im Zusammenhang stehen. Dazu gehören Bilder, Videos oder Livestreams, die den sexuellen Missbrauch von echten Kindern zeigen. In der Konvention sind Konsequenzen für Herstellung, Angebot, Verkauf, Verbreitung, Übertragung, Ausstrahlung, Bewerbung, Beschaffung, Besitz, Finanzierung sowie für den Konsum solcher Inhalte formuliert. Besonders in Anbetracht der langfristigen verheerenden Auswirkungen für die Überlebenden und die Häufigkeit dieses Verbrechens hat der Kampf gegen CSAM oberste Priorität. Allerdings bergen die vorgesehenen Bestimmungen das Risiko, für eine Ausweitung der Kriminalisierung missbraucht zu werden: Der weitgefasste Anwendungsbereich könnte die strafrechtliche Verfolgung legitimer Online-Aktivitäten ermöglichen und ggf. zu schweren Menschenrechtsverletzungen wie der Strafverfolgung von Kindern führen. Insbesondere könnten Personen unter 18 Jahren strafrechtlich belangt werden, die etwa «Nacktfotos oder anzügliche Selfies» aufnehmen. Der Artikel schließt mit dem Hinweis, dass «internationale Verpflichtungen, die der Wahrung von Kinderrechten dienlicher sind, von dem Abkommen

unberührt bleiben sollen». Möglicherweise reicht diese Formulierung jedoch nicht aus, um Kinder vor einer Kriminalisierung durch genau die Paragraphen zu bewahren, die sie eigentlich schützen sollen (Hollingworth 2024).

Die Konvention kriminalisiert das nicht einvernehmliche Teilen von privatem Bildmaterial mit sexuellem Inhalt (Artikel 16). Durch die Festschreibung der Strafbarkeit der nicht einvernehmlichen Verbreitung intimer Bilder (NCIID) in der Konvention wird ein wichtiger internationaler Rahmen geschaffen, der die Verhinderung, Ermittlung und strafrechtliche Verfolgung bildbasierter Gewalt ermöglicht. Da Frauen, Mädchen und andere Menschen mit diverser Geschlechtsidentität bzw. -ausdruck stärker von dieser Form der Online-Gewalt betroffen sind, wird NCIID als geschlechtsspezifisch gewertet (Chatham House 2022). Darüber hinaus gehen entsprechende Erpressungsdelikte häufig von internationalen Netzwerken Krimineller aus, die gezielt vulnerable Personen ausnutzen. Als sogenannte «Revenge-Porn-Gesetze» existieren in einer bedeutenden Anzahl von Staaten zahlreiche Bestimmungen zu NCIID. In einigen anderen Ländern verhindert ein fehlender Rechtsrahmen oder ein unangemessener Umgang mit NCIID die Anerkennung dieses Verbrechens als solches. Um in Fällen von NCIID angemessen zu ermitteln, sie strafrechtlich zu verfolgen und aus geschlechtersensibler Perspektive zu bewerten, ist ein stärkeres Bewusstsein und eine größere Aufmerksamkeit für NCIID und andere Missbrauchskriminalität unerlässlich. So erhofft sich etwa die britische NGO South West Grid for Learning (SWGfL), die mit der Revenge Porn Helpline und StopNCII.org zusammenarbeitet, dass Plattformen, Regierungen und die Zivilgesellschaft durch die Konvention bei nicht einvernehmlicher Veröffentlichung von Inhalten schnell und entschlossen handeln können. Die Aufnahme von NCIID in das internationale Strafrecht zur Cyberkriminalität könnte hier einen Schulterschluss ermöglichen, der Betroffenen die nötige Unterstützung, Hilfe und Entschädigung gewährleistet (Wright 2024).

5.6 Betroffenenunterstützung und Zeug*innenschutz

Wie Menschen von Cyberkriminalität betroffen sind, hängt von Geschlechtsidentität und -ausdruck sowie anderen Identitätsmarkern wie beispielsweise Race ab (s. Kapitel 2). Unterschiedliche Arten des Betroffenseins erfordern für den Schutz von Zeug*innen und Betroffenen eine geschlechtssensible Vorgehensweise, die individuelle Bedürfnissen berücksichtigt. Geschieht das nicht, kann ein unangemessener Umgang bereits existierende Vulnerabilität und soziale Ungleichheit verschärfen und so den Zugang zu Recht und Rechtsmitteln verstellen, wodurch sich Folgeschäden noch verstärken. In der Präambel der UN-Konvention wird die «zunehmende Zahl von Betroffenen von Cyberkriminalität sowie die Notwendigkeit [anerkannt], dass diesen Betroffenen Gerechtigkeit widerfährt und dass die Bedürfnisse von Personen in vulnerablen Situationen bei den Maßnahmen zur Verhinderung und Bekämpfung der durch die Konvention festgelegten Straftaten berücksichtigt werden müssen.» In den Bestimmungen zur Hilfe und zum Schutz von Betroffenen (Artikel 34) heißt es weiter, dass Staaten «Betroffenen von durch diese Konvention

festgelegten Straftaten, vor allem in Fällen von Vergeltungsmaßnahmen und Einschüchterung, Hilfe und Schutz bieten müssen.» Das beinhaltet Abfindungen und Entschädigungen, auch um physische und psychische Genesung sicherzustellen, sowie die Unterstützung von internationalen Organisationen, NGOs und anderen zivilgesellschaftlichen Einrichtungen. Bei der Umsetzung dieser Bestimmungen sollten Staaten «Alter, Geschlecht, besondere Umstände und Bedürfnisse der Betroffenen, darunter die besonderen Umstände und Bedürfnisse von Kindern berücksichtigen». Bedauerlicherweise sind diese Hilfsmaßnahmen jedoch als optional definiert, wobei ggf. auf nationale Rechtsprechung verwiesen wird, die jedoch nicht immer verlässlichen Schutz bietet. Betroffene sind also von Behörden abhängig, die vielfach selbst diskriminierend agieren. Damit können Betroffene häufig keinerlei juristische Garantien bzw. ihr Recht auf Wiedergutmachung wahrnehmen oder die Rückgabe von Eigentum durchsetzen.

Ähnliche Bedenken bestehen bei Artikel 33 zum Schutz von Zeug*innen. Staaten sollen effektive Maßnahmen ergreifen, um Zeug*innen vor Vergeltung und Einschüchterung zu schützen und ihre körperliche Unversehrtheit zu garantieren. Häufig legen nationale Gesetze jedoch weder angemessene Schutzmaßnahmen noch Rechtsmittel oder Verfahren fest. Außerdem sehen Staaten oft keinen Anlass, sich an internationalen Rechtsstandards zu orientieren. Der Kampf gegen Cyberkriminalität muss die erheblichen Auswirkungen und Schäden für Betroffene berücksichtigen, die häufig die Vulnerabelsten der Gesellschaft sind. Darum ist entscheidend, dass sich Staaten bei der Umsetzung der Konvention an bewährte Verfahren halten. Außerdem sollten Staaten beispielsweise Kooperationen zwischen Strafverfolgungsbehörden, Rechtsexpert*innen und Einrichtungen der Opferhilfe aufbauen, um die Betroffenenperspektive konsequent in den Mittelpunkt zu rücken.

Nächste Schritte

Die Konvention triff laut Artikel 64 in Kraft, sobald der 40. Mitgliedstaat seine Ratifikation, Zustimmung, Annahme oder seinen Beitritt hinterlegt hat. Allerdings wurde dafür kein zeitlicher Rahmen festgelegt. Da die AHC-Abschlusssitzung mit einem Konsens zu einem Resolutionsentwurf endete, galt die Verabschiedung des vereinbarten Texts durch die UN-Generalversammlung als Formsache. Dennoch könnte sich die Ratifizierung erheblich in die Länge ziehen. Erst nach Einbeziehung der jeweiligen Parlamente und anderer staatlicher Instanzen können Staaten, deren Vertretung die Konvention unterstützt, die Einhaltung des internationalen Abkommens verbindlich zusichern. Die Umsetzung des Gesetzes hängt vielerorts also von der Legislative ab, was das Inkrafttreten der Konvention massiv verzögert (Walker & Oliveira 2024). Außerdem ist von einer uneinheitlichen Umsetzung auszugehen, die sich je nach Land stark unterscheidet. Trotzdem dürfte das Abkommen weltweit die Ausgestaltung von Cyberkriminalitätsgesetzen beeinflussen. Die tatsächliche Wirksamkeit und der tatsächliche Nutzen/Schaden hängt letztlich davon ab, welche Staaten das Abkommen ratifizieren und wie sie es umsetzen. Darum ist es unabdinglich, dass Zivilgesellschaft und Menschenrechtsorganisationen zur Umsetzung

Stellung beziehen und streng beobachten, wie die Bestimmungen in die nationalen Rechtssysteme überführt werden. Wo die verantwortlichen Behörden bereits generell durch Diskriminierungen und Repressionen gegenüber bestimmten Geschlechtsidentitäten, sexuellen Orientierungen oder marginalisierten Gruppen aufgefallen sind, werden sich diskriminierende Praktiken wahrscheinliche auch im Zusammenhang mit der Cyberkriminalitätsbekämpfung der nationalen Gesetzgebung und Strafverfolgung niederschlagen (Shires, Hassib & Swali 2024).

6 Der Weg nach vorn: Empfehlungen für Regierungen, UN-Institutionen und zivilgesellschaftliche Akteur*innen

Mit der intersektional feministischen Perspektive auf die Gesetzgebung zur Bekämpfung von Cyberkriminalität konnte in diesem Positionspapier offengelegt werden, wie Staaten nationale Cyberkriminalitätsgesetze immer wieder missbrauchen und instrumentalisieren. Solche staatlichen Übergriffe haben sowohl unterschiedliche als auch sich gegenseitig verstärkende, kumulative Effekte auf Einzelpersonen und Gruppen, von denen viele bereits aufgrund ihres Geschlechts und/oder anderer (sich überschneidender) Identitätsmarker Diskriminierungen erfahren. Unter dem Vorwand der Bekämpfung von Cyberkriminalität haben Regierungen Kritik zum Schweigen gebracht, Äußerungen abweichender Meinungen unterdrückt, Menschenrechts- und LGBTQIA+-Aktivismus eingeschränkt sowie journalistische Arbeit und Pressefreiheit beschnitten.

Legislativer Machtmissbrauch durch Cyberkriminalitätsgesetze kann online zu einem Schrumpfen zivilgesellschaftlicher Räume führen und begünstigt so autoritäre, antidemokratische und antifeministische Programme (s. Kapitel 4). Diese Praktiken verdeutlichen einmal mehr die Notwendigkeit von menschenrechtszentrierten, geschlechtssensiblen und intersektional feministischen Perspektiven auf institutionelle Cyberkriminalitätsbekämpfung. Die Verhandlungen zur UN-Konvention gegen Cyberkriminalität boten eine Gelegenheit, solche Anliegen auch auf internationaler Ebene festzuschreiben. Wie in den vorangegangenen Kapiteln anhand nationaler Kontexte gezeigt wurde (s. Kapitel 4), birgt das angenommene Abkommen jedoch multiple Risiken. Staaten müssen dieses Missbrauchspotenzial berücksichtigen, wenn sie über die Unterzeichnung und Ratifizierung und ggf. Umsetzung des Abkommens entscheiden, bzw. wenn entsprechende Kontrollmechanismen in Kraft treten.

Unabhängig davon bieten folgende Empfehlungen eine Orientierungshilfe im Umgang mit Cyberkriminalitätsgesetzen im Allgemeinen und der UN-Konvention gegen Cyberkriminalität im Besonderen. Diese Empfehlungen sind nicht abschließend formuliert, sollen jedoch eine inklusive Beteiligung verschiedenster zivilgesellschaftlicher Akteur*innen und die Verankerung menschenrechtsbasierter, intersektional feministischer Perspektiven fördern.

Richtlinienempfehlungen

1. **Diverse Interessensgemeinschaften bei der Entscheidung, die UN-Konvention gegen Cyberkriminalität zu unterzeichnen und zu ratifizieren, aktiv in Diskussionen und Beratungen und ggf. die zukünftige Umsetzung einbinden.**
   Angesichts der Schwächen und Stolperfallen der UN-Konvention gegen Cyberkriminalität (s. Kapitel 5) sollten sich **(feministische und Menschenrechts-)Organisationen der Zivilgesellschaft, die Privatwirtschaft und Fachkreise nicht nur in überwachender, sondern auch beratender Funktion einbringen.** So wird sichergestellt, dass gesetzliche Bestimmungen zur Cyberkriminalität menschenrechtkonform umgesetzt werden und sich an einer intersektional feministischen Perspektive orientieren. Damit diese Bemühungen erfolgreich sind, müssen Staaten sich aktiv mit verschiedenen Interessengemeinschaften auseinandersetzen und zivilgesellschaftliche Organisationen in Beratungsprozesse zu finalen Entscheidungen hinsichtlich der Unterzeichnung und Ratifizierung der UN-Konvention gegen Cyberkriminalität und ggf. zur Umsetzung einbinden.
   Daher sollten Staaten auf der nationalen und internationalen Ebene, beispielsweise beim UNODC (United Nations Office on Drugs and Crime/Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung) oder der Vertragsstaatenkonferenz der UN-Konvention gegen Cyberkriminalität (s. Artikel 57, bei Inkrafttreten), **verbindliche Beratungsverfahren unter Einbeziehung verschiedener Interessengemeinschaften schaffen und institutionalisieren.** Ein solches Verfahren, damit verbundene Prozesse und jeglicher sonstige Austausch mit Interessengemeinschaften sollten **inklusiv und leicht zugänglich** sein. Besondere Umstände der Teilnehmenden sollten also Berücksichtigung finden und insbesondere zivilgesellschaftliche Vertreter*innen, Aktivist*innen und Expert*innen aus dem sogenannten Globalen Süden sollten finanziell oder bei Visaangelegenheiten Unterstützung erhalten. Darüber hinaus muss eine Online-Teilnahme ermöglicht werden, und die Modalitäten von AHC 1 sollten in AHC 2 fortgeführt werden.

2. **Die Vereinbarkeit der Unterzeichnung der UN-Konvention gegen Cyberkriminalität mit dem Schutz von Menschen- und Grundrechten und anderen (politischen) Verpflichtungen prüfen.**
   Zusätzlich zu den erwähnten Beratungen mit Interessengemeinschaften sollten einzelne Staaten sowie die Europäische Union (EU) **alle verfügbaren Informationsquellen und (rechtlichen) Prüfverfahren ausschöpfen,** um die Vereinbarkeit der UN-Konvention gegen Cyberkriminalität mit (rechtlich) verbindlichen Zusagen zum Schutz von Menschen- und Grundrechten zu prüfen. Dies sollte auch andere (politische) Verpflichtungen gegenüber feministischen Konzepten, Prinzipien und Zielen umfassen, wie etwa gegenüber feministischer Außenpolitik. Im Fall der EU sollte beim Europäischen Gerichtshof durch einen Mitgliedstaat der EU, die EU-Kommission, das EU-Parlament oder den Rat ein Gutachten eingeholt werden, um zu prüfen,

«ob das geplante [UN-]Abkommen mit anderen Abkommen vereinbar ist» (Vertrag über die Arbeitsweise der Europäischen Union, Artikel 218, Absatz 11).

3. **Sich zu etablierten Menschenrechtsprinzipien und -schutzmaßnahmen bei der Durchsetzung der UN-Konvention gegen Cyberkriminalität und zu engmaschiger Kontrolle einer menschenrechtskonformen Umsetzung mit verschiedenen Interessengruppen verpflichten, inklusive angemessener, effektiver und inklusiver Prüfverfahren sowie Sicherungs- und Förderungsmaßnahmen für Menschenrechte.**
Analysen der Umsetzung von UNTOC und UNCAC (United Nations Convention against Corruption/UN-Übereinkommen gegen Korruption) haben wichtige Erfahrungswerte hinsichtlich der Berücksichtigung von Menschenrechten für die Umsetzung der UN-Konvention gegen Cyberkriminalität aufgezeigt. Hierzu zählt, dass «in Wien, wo die Umsetzung von UNTOC und UNCAC geprüft und zivilgesellschaftliche Beteiligung besonders restriktiv gehandhabt wird, Fragen der Menschenrechte und entsprechende Regelungen noch immer kontrovers sind» (Tennant & Oliveira 2024). «Sollte die Prüfstelle für das Cyberkriminalitätsabkommen ebenfalls in Wien entstehen, könnte es hier zu ähnlichen Schwierigkeiten kommen. Angesichts der Gefahren für die Menschenrechte (sowohl hinsichtlich der Kriminalisierung von Akteur*innen der Zivilgesellschaft als auch des Missbrauchs staatlicher Kompetenzen bei strafrechtlichen Ermittlungen) dürfte der weit gefasste, dehnbare Spielraum für Kriminalisierung zu weiteren unbeabsichtigten Folgen führen – ähnlich wie bei der Durchsetzung staatlicher Befugnisse im Rahmen von UNTOC und UNCAC (z. B. Polizeigewalt im Kontext der Kriminalitätsbekämpfung, unzureichender Schutz von Zeug*innen und Betroffenen, Verletzung von Verfahrensrechten)» (ebd.).
Die von Tennant und Oliveira vorgeschlagenen **Grundsätze für zukünftige Prüfverfahren** der UN-Konvention gegen Cyberkriminalität (2024: 232) bieten Staaten eine hervorragende Arbeitsgrundlage. Im Folgenden werden einige dieser Grundsätze wiedergegeben und durch eine intersektional feministische Perspektive ergänzt.

   1. Für den Erfolg des Durchsetzungsverfahrens ist es notwendig, **intersektional feministische, menschenrechtsbasierte Perspektiven zentral und nicht als Nebenerwägung zu berücksichtigen.**

   2. Das Ziel jedes Verfahrens sollte auch eine Bewertung und Einschätzung der Auswirkungen sein – nicht bloß des Fortschritts bei der rechtlichen Durchsetzung. Dazu gehört eine **intersektionale Folgenabschätzung in Bezug auf den Faktor Geschlecht** in Anlehnung an bestehende zivilgesellschaftliche Instrumente (z. B. der Association for Progressive Communication von 2023) sowie in Bezug auf demokratische Prozesse, Internetfreiheit und Menschenrechte, insbesondere von marginalisierten Gruppen. Als Teil davon sollten die Verfahrensmechanismen Zugriff auf die neusten (intersektional nach Geschlecht aufgeschlüsselten) Daten und Erkenntnisse haben und Expert*innen aus verschiedensten Interessengemeinschaften aktiv bei der Bewertung konsultieren und einbinden (s. Empfehlung 7).

3. Einfacher und sicherer Zugang zu Prüfverfahren und eine offene, inklusive Beteiligung aller Gesellschaftsbereiche sind Voraussetzung dafür (s. Empfehlung 1), dass aktuelle, relevante Informationen vorliegen und Rechenschaftspflichten eingehalten werden. Außerdem etablieren sich zivilgesellschaftliche Akteur*innen so auch zukünftig als Verhandlungspartner und Kontrollinstanz der Umsetzung.

Um im Zusammenhang mit den Stolperfallen der UN-Konvention gegen Cyberkriminalität mögliche Menschenrechtsverletzungen durch gezielte oder massenhafte Überwachung zu mindern (s. Kapitel 5), sollten Staaten sich den **«International Principles on the Application of Human Rights to Communications Surveillance» verpflichten** (Internationale Grundsätze zur Wahrung der Menschenrecht bei der Kommunikationsüberwachung, auch bekannt als die «13 Principles», 13 Grundsätze, oder «Necessary and Proportionate Principles», Grundsätze zur Notwendigkeit und Angemessenheit). Diese Prinzipien wurden von einer länderübergreifenden Koalition aus Vertreter*innen der Zivilgesellschaft, Forscher*innen, die zu Überwachungsgesetzen arbeiten, sowie Datenschutz- und Technikexpert*innen entwickelt. Über 600 Organisationen und über 270 000 Menschen weltweit unterstützen den Vorstoß (s. Necessary and Proportionate o. D.). Die «Grundsätze zur Notwendigkeit und Angemessenheit» zeigen auf, wie internationales Menschenrecht vor allem in Hinblick auf moderne Überwachung im digitalen Raum Anwendung finden sollte. Staaten sollten im nationalen wie internationalen Austausch sowie bei der Umsetzung von inter-/nationalen Rahmenbedingungen zur internationalen Datenweitergabe und Überwachung zudem den Leitfaden «Grundsätze zur Notwendigkeit und Angemessenheit» von Access Now (2015) berücksichtigen.[33]

4. **Die intersektional feministische Perspektive auf die Gesetzgebung im Kampf gegen Cyberkriminalität auch zukünftig bei der Entwicklung gemeinsamer Leitlinien und Gesprächsforen fördern, bei Inkrafttreten insbesondere auf der Vertragsstaatenkonferenz der UN-Konvention gegen Cyberkriminalität.**
In internationalen Gesprächen und Verhandlungen, insbesondere auf der Vertragsstaatenkonferenz zur UN-Konvention gegen Cyberkriminalität (s. Artikel 57), sollten Staaten **auf die unterschiedlichen Auswirkungen von Cyberkriminalität auf Frauen, LGBTQIA+ und andere marginalisierte Gruppen hinweisen** und damit die Bedeutung ihrer **Bedürfnisse und Erfahrungen** ins Zentrum stellen (auch in Hinblick auf die weitere internationale und entsprechende nationale Gesetzgebung). Außerdem sollten Staaten **auf die Risiken hinweisen, denen diese Personen und Gruppen aufgrund der Schwachstellen der UN-Konvention gegen Cyberkriminalität potenziell oder mit großer Wahrscheinlichkeit ausgesetzt sein werden** (s. Kapitel 5).
Bei ihren Bemühungen, gemeinsame Leitlinien zu erarbeiten, sollten Staaten auf

33 Diese Empfehlung wurde durch Diskussionen mit Expert*innen inspiriert, denen im Impressum gedankt wird.

bestehendes Wissen und Ressourcen wie das «Inclusive Cyber-Norms»-Toolkit von Global Partners Digital von 2023 zurückgreifen.

5. **Die Umsetzung des UN-Abkommens gegen Cyberkriminalität auf nationaler Ebene und die Anpassung der entsprechenden nationalen Gesetzgebung sollten regelmäßig nach intersektional feministischen Prinzipien auf ihre Folgen in Bezug auf geschlechtsspezifische Benachteiligung hin untersucht werden, und zwar in Zusammenarbeit mit der (feministischen) Zivilgesellschaft und verschiedenen Interessengemeinschaften.** Staaten sollten unter klarem Bekenntnis zur Geschlechtergerechtigkeit etwaige Bemühungen in sämtliche Richtlinien zu Cyber- und Anticyberkriminalitätspolitik integrieren. Die zuständigen Institutionen **sollten ein Verfahren anstoßen, mit dem Richtlinien und Gesetze zum digitalen Raum und der Bekämpfung von Cyberkriminalität kritisch aus einer intersektionalen Perspektive analysiert werden.** Dabei sollten Rahmenbedingungen mit Wirkung auf Geschlecht und Geschlechtergerechtigkeit um eine digitale Dimension erweitert werden (wie die nationalen Aktionspläne «Women, Peace, and Security»).
   Wie in den vorangegangenen Kapiteln ausgeführt, können Richtlinien und Gesetze zur Bekämpfung von Cyberkriminalität geschlechtsspezifische oder anderweitig identitätsbezogene Schädigungen verschärfen oder überhaupt erst erzeugen. **Staaten sollten darum vorhandenes Wissen und Ressourcen der verschiedenen Interessengruppen nutzen,** wie etwa die Bewertungsmethode zur Entwicklung einer geschlechtergerechten Sicherheit im digitalen Raum der Association for Progressive Communication.[34] Dieses Instrument soll politischen Entscheidungsträger*innen und Exekutivorganen dabei helfen, feministische Methoden und Grundsätze sowie geschlechtsbezogene Analysen und Folgenabschätzungen in ihre Arbeit einzubinden. Gleichzeitig soll es für Geschlechtergerechtigkeit sorgen und verhindern, dass Richtlinien Ungleichheiten im digitalen Raum unabsichtlich verschärfen.
   Partizipatorische und inklusive Ansätze unterstützen Staaten, bei der intersektionalen Analyse geschlechtsspezifischer Ungleichheit und Folgenabschätzung Lücken zu schließen sowie lokale, kontextabhängige Dimensionen von Geschlechterungleichheit und andere auf (sich überschneidende) Identitätsmerkmale zurückgehende Diskriminierungsformen besser zu verstehen. **Um während der Erstellung von Richtlinien, der Anpassung bereits bestehender Gesetze und Richtlinien und deren Umsetzung eine proportionale und angemessene Repräsentation von Frauen und anderen marginalisierten Teilen der Bevölkerung zu fördern, sollte die Zusammenarbeit mit relevanten Gruppen angestrebt werden. Dazu zählen solche, die sich für LGBTQIA+-, Frauen- und Menschenrechte einsetzen sowie Forschungseinrichtungen und Organisationen an der Basis mit belastbaren Netzwerken und direktem Kontakt zu Betroffenen.** Verschiedene Interessengruppen sollten ausdrücklich mit einbezogen werden, damit sie ihre Perspektiven, Befunde und Einsichten teilen können. Staaten sollten dafür die

34 Diese Methode wird *hier* umfassend dargestellt.

Zusammenarbeit mit Wissenschaft und feministischer Zivilgesellschaft institutionalisieren, etwa durch permanente, vergütete und barrierefreie Konsultationen (s. Empfehlung 1).

6. **Kapazitätsaufbau, Zugang zum Recht und geschlechtersensible Hilfestrukturen für Betroffene von Cyberkriminalität und staatlichem Machtmissbrauch fördern und finanziell unterstützen.**
   Für die Umsetzung der Konvention ist Kapazitätsaufbau unerlässlich. Dennoch ist «hinsichtlich eines internationalen Kapazitätsaufbaus, der auch undemokratische Empfangsstaaten einbezieht, Vorsicht geboten», da Staaten ohne demokratische Kontrolle und/oder mit repressiven Systemen sonst unabsichtlich unterstützt werden könnten (Hansel & Silomon 2023).
   In diesem Zusammenhang sollten Beschränkungen für Technologietransfer im Rahmen zwischenstaatlicher technischer Zusammenarbeit sorgfältig geprüft werden. Der Aufbau von Kapazitäten staatlicher Stellen zur wirksamen Bekämpfung von Cyberkriminalität ist zwar zentral für eine effektive Umsetzung der vereinbarten Bestimmungen, birgt jedoch Risiken, die sowohl beabsichtigte als auch unbeabsichtigte Schäden verursachen und teilweise weitreichende Folgen für konkret betroffene Gruppen haben können (Chatham House o. D.). Dies gilt insbesondere, wenn im Rahmen von Kapazitätsaufbau sogenannte Dual-Use-Technologien bereitgestellt werden. Vor allem Überwachungstechnologien sind besonders missbrauchsanfällig und stellen ein erhebliches Risiko für Menschenrechte und Grundfreiheiten dar (s. Kapitel 4). Daher **sollten vor Kapazitätsaufbau und Erbringung technischer Unterstützung deren Folgen für Menschenrechte und Geschlechtergerechtigkeit geprüft werden.** Diese Prüfung sollte wiederum bei der Zielsetzung und Folgenabschätzung sowie bei Auswahl und Einsatz entsprechender Technologie berücksichtigt werden. Außerdem sollten Kapazitätsaufbau und technische Unterstützung geltende internationale Menschenrechte einhalten und unter unabhängiger Aufsicht stehen.
   Staaten müssen zudem **verhindern, dass Einzelpersonen und/oder Gruppen reviktimisiert werden, die von Cyberkriminalität oder dem Missbrauch von Cyberkriminalitätsgesetzen betroffen sind.** Es gilt hier also ein Gleichgewicht zwischen der Viktimisierung und der Handlungsfähigkeit marginalisierter Menschen zu finden. Demzufolge muss die Strafjustiz befähigt werden, den Einfluss von Geschlecht und anderen (sich überschneidenden) Identitätsmarkern auf die Folgen von Datenmissbrauch zu untersuchen und entsprechende Beweise zu sammeln. Für einen zielführenden Umgang mit Fällen von Cyberkriminalität sind **besondere Ausbildungsmaßnahmen für Polizei, Staatsanwaltschaft und Richter*innen** unerlässlich. So kann die technische Kompetenz und das Fachwissen für die Sicherung und Auswertung von Beweisen, für gründliche Ermittlungen und die Verfolgung von Straftäter*innen vermittelt werden, die für gerechte Verfahren und den Schutz der Betroffenen von Cyberkriminalität nötig sind. Staaten sollten die Kapazitäten der für die Cyberkriminalitätsbekämpfung zuständigen Behörden stärken und intersektionale Perspektiven auf Geschlechtergerechtigkeit (und damit verbundene verstärkende und kumulative Effekte) in deren institutionellen Mandaten, Abläufen und Praktiken festschreiben (Pavlova 2024).

Angebote zur Unterstützung von Betroffenen sollten systematisch finanziert werden, und Staaten **sollten deren Kapazitäten ausbauen, um geschlechtersensible und -gerechte Unterstützung bereitzustellen, die Betroffene bei Wiedergutmachung und Entschädigung in den Mittelpunkt stellt.** Staaten sollten zudem in Strafverfolgungsbehörden Spezialeinheiten einrichten (CVSUs – Cyber Victim Support Units), die sich auf die Unterstützung von Betroffenen von Cyberkriminalität konzentrieren und dabei einen besonderen Fokus auf Straftaten mit geschlechtsspezifischer Komponente legen, wie z. B. Cyberstalking, Belästigung oder Doxing. Zweck dieser Einheiten wäre nicht nur, Überlebende geschlechtsbezogener oder auf weitere (intersektionale) Identitätsmerkmale bezogener Cyberkriminalität wirksam durch institutionell integrierte Expertise zu unterstützen, sondern auch für das erhöhte Risiko von Frauen, LGBTQIA+ und anderen marginalisierten Gruppen zu sensibilisieren (Wong 2024). Da die Strafjustiz und -verfolgungsbehörden nicht geschlechterneutral arbeiten, sehen sich aufgrund von Sexualität oder Geschlecht marginalisierte Personen bei der Suche nach Hilfe häufig mit erheblichen Hürden konfrontiert (s. Kapitel 4.3). Ist der Staat der Täter, fehlt Betroffenen von Cyberkriminalität vor allem in autoritären Kontexten Zugang zum Recht. Unterstützungsangebote für Betroffene von geschlechtsspezifischen Cyberangriffen und anderer durch Technologie ermöglichter geschlechtsspezifischer Gewalt sind zurzeit noch rar gesät. Organisationen der Zivilgesellschaft und Initiativen für soziale Gerechtigkeit bieten hier lediglich einen Flickenteppich an Ersatzangeboten. Diese chronisch unterfinanzierten Organisationen sind nicht in der Lage, die komplexen Bedürfnisse von Betroffenen von Cyberkriminalität oder staatlichem Machtmissbrauch adäquat abzubilden. Dies würde Rechts- und psychologische Beratung sowie effektive Maßnahmen gegen Reviktimisierung umfassen, die Reviktimisierungen vorbeugen (Pavlova 2024). Daher **sollten von der Zivilgesellschaft aufgebaute und betriebene Unterstützungsangebote für Betroffene durch staatliche finanzielle Förderung und gezielte Sensibilisierung unterstützt werden.**

Beispielsweise bietet die Revenge Porn Helpline der gemeinnützigen Organisation South West Grid for Learning UK (SWGfL) Unterstützung für Betroffene von Sextortion an, eine häufig von internationalen kriminellen Gruppen verübte Ausbeutung schutzbedürftiger Personen. Mit einer Quote von über 90 Prozent konnte die Helpline seit ihrer Gründung im Jahr 2015 über 200 000 nicht einvernehmliche intime Bilder aus dem Internet entfernen. Aktuelle Daten zeigen, dass die gemeldeten Sextortion-Fälle im letzten Jahr um 54 Prozent zugenommen haben. Sextortion führt bei Betroffenen häufig zu Angstzuständen angesichts der angedrohten Verbreitung der Bilder im Internet. Eine effektive Zusammenarbeit ist für den Kampf gegen Cyberkriminalität und die Unterstützung von Betroffenen unerlässlich. Zusammen mit internationalen NGOs und Technologieplattformen bietet StopNCII.org eine gerätebasierte Hashing-Technologie an, mit der Betroffene ihre Inhalte vor Verbreitung schützen können. Durch die Erstellung von Hash-Werten und die Kommunikation mit Plattformen ermöglicht dieses Tool eine Echtzeit-Blockierung, ohne dabei die Daten der Betroffenen zu speichern oder weiterzugeben. Das argentinische

Projekt Acoso Online stellt grundlegende Unterstützung und rechtliche Informationen bei Fällen von NCSII und anderen Formen von durch Technologie vermittelter geschlechtsspezifischer Gewalt (TFGBV) bereit. Bei sämtlichen Maßnahmen zum Kapazitätsaufbau im Bereich Cyberkriminalitätsbekämpfung sollten Staaten **auf bestehendes Wissen und Ressourcen zurückgreifen,** etwa auf das Toolkit Integrating Gender in Cybercrime Capacity-Building von Chatham House.

7. **Unabhängige interdisziplinäre Forschung unterstützen, insbesondere feministische Wissenschaftler*innen sowie die Arbeit (feministischer) zivilgesellschaftlicher Organisationen zu Cyberkriminalität und entsprechender Gesetzgebung.**
   Vor dem Hintergrund technologischer Entwicklungen und deren Einfluss auf die Art, Intensität und Wirkung von Cyberkriminalität sollten Staaten sicherstellen, dass sie **Daten zu Cyberkriminalität auf der Grundlage von Geschlecht und weiterer (sich überschneidender) Identitätsmerkmale erheben (z. B. Behinderung, soziale Herkunft, Ethnizität, Race etc.).** Um die sich schnell wandelnden Zusammenhänge von Cyberkriminalität einschließlich ihrer Ursachen, Täter*innen, Betroffenen sowie ihrer Formen, Intensität und kumulativen und sich wechselseitig verstärkenden negativen Auswirkungen zu verstehen und evidenzbasierte Richtlinien zu entwickeln, ist die Einrichtung einer nach geschlechtsrelevanten Kriterien aufgeschlüsselten Datenbank unerlässlich (s. auch Pavlova 2024). Mitarbeitende von Behörden und anderen mit der Erhebung solcher Daten betraute Stellen sollten vor allem dann, wenn sie mit Betroffenen von Cyberkriminalität Kontakt haben, in geschlechter- und traumasensibler Kommunikation geschult werden, um **Retraumatisierung oder andere negative Folgen für die Befragten zu vermeiden.**
   Außerdem sollten Staaten **bestehende zivilgesellschaftliche Initiativen unterstützen, die qualitative und quantitative Daten zu cyberkriminellen Handlungen auf Basis von Geschlecht und anderen (sich überschneidenden) Identitätsfaktoren erheben** und deren Auswirkungen auf marginalisierte Gruppen erforschen. Ein Beispiel hierfür ist das Projekt Words Matter von Democracy Reporting International (DRI), in Zusammenarbeit mit Partnern in der MENA-Region: Gemeinsam mit DRI und der TAMAM Coalition hat die Jordan Open-Source Association das Open-Source-Tool Nuha (arabisch für «Verstand» oder «Gehirn») entwickelt, um insbesondere in sozialen Netzwerken geschlechtsspezifische Gewalt und Hassrede auf jordanischem Arabisch zu erkennen. Dass Nuha trotz Herausforderungen wie unausgeglichenen Datensätzen oder Einschränkungen durch Twitter-APIs zuverlässig funktioniert, beweist laut DRI (2023) eine F1-Score-Treffergenauigkeit von 72 Prozent bei der Erkennung von Hassrede.
   Abgesehen von der Datenverfügbarkeit liegt eine zentrale Herausforderung bei Cyberkriminalität (und entsprechender Gesetzgebung) in ihrem interdisziplinären Charakter: «Traditionelle Fachgrenzen verhindern häufig ein umfassendes Verständnis von Cyberkriminalität, einschließlich ihrer technischen, rechtlichen und sozialen Aspekte» (Hansel & Silomon 2023: 29). Um Cyberkriminalität und unbeabsichtigte Folgewirkungen gesetzlicher Maßnahmen besser zu bewältigen, **sollten Staaten interdisziplinäre Forschung finanziell unterstützen, die «verschiedene, oft voneinander**

getrennte Wissensbereiche und Forschungsmethoden zusammenführt» (ebd.) und auf die Zusammenarbeit verschiedener Interessengruppen setzt, wie z. B. von Wissenschaft und (feministischer) Zivilgesellschaft.

Literaturverzeichnis

Access Now 2015, Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance, viewed 12 February 2025, *https://necessaryandproportionate.org/files/implementation_guide_international_principles_2015.pdf*.

Access Now 2018, Statement opposing Egypt's legalization of website blocking and communications surveillance, viewed 12 February 2025, *https://www.accessnow.org/press-release/statement-opposing-egypts-legalization-ofwebsite-blocking-and-communications-surveillance-2/*.

Access Now 2024, Oral Statement – UN Ad Hoc Committee on Cybercrime Reconvened Concluding Session 30 July 2024, viewed 13 February 2025, *https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP8/Oral_Statement_-_UN_Ad_Hoc_Committee_on_Cybercrime_Reconvened_Concluding_Session_30_July_2024.pdf*.

Access Now n.d., Digital Security Helpline, viewed 12 February 2025, *https://www.accessnow.org/help/*.

Adams, A.C. & Podair, D. 2024, ‹Confusion & Contradiction in the UN «Cybercrime» Convention›, Lawfare, viewed 13 February 2025, *https://www.lawfaremedia.org/article/confusion---contradiction-in-the-un--cybercrime--convention*.

AFP 2024, Nicaragua's new legal reforms target opponents and critics, viewed 12 February 2025, *https://ticotimes.net/2024/10/05/nicaraguas-new-legal-reforms-target-opponents-and-critics*.

Africanews 2023, Libya: HRW asks to repeal a law on cybercrime, viewed 12 February 2025, *https://www.africanews.com/2023/04/04/libya-hrw-asks-to-repeal-a-law-on-cybercrime/*.

AHC 2021, Proposed Outline and Modalities for the Ad Hoc Committee on Cybercrime Conference room paper submitted by Australia, Canada, Chile, the Dominican Republic, Honduras, Japan, New Zealand, Norway, the United Kingdom and the United States of America, status date 4 December 2020, A/AC.291/CRP.1, viewed 13 February 2025, *https://www.unodc.org/documents/Cybercrime/AdHocCommittee/CRPs/V2100299.pdf*.

Al Sur 2024, Al Sur's open letter on international convention cybercrime, viewed 13 February 2025, *https://www.alsur.lat/en/blog/alsurs-open-letter-international-convention-cybercrime*.

Allinson, T. 2020, ‹Egypt's rising #MeToo movement dealt blow›, DW, viewed 12 February 2025, *https://www.dw.com/en/setback-to-egypts-metoo-movement-as-rape-witnesses-reportedly-charged/a-54958956*.

Amnesty International 2018, Crowdsourced Twitter study reveals shocking scale of online abuse against women, viewed 12 February 2025, *https://www.amnesty.org/en/latest/press-release/2018/12/crowdsourced-twitter-study-reveals-shocking-scale-of-online-abuse-against-women/*.

Amnesty International 2021, Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally, viewed 12 February 2025, *https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/*.

Amnesty International 2022, Tunisia: Repeal Draconian Cybercrime Decree, viewed 12 February 2025, *https://www.amnesty.org/en/documents/mde30/6290/2022/en/*.

Amnesty International 2023, Jordan's new proposed cybercrimes law will strongly undermine digital rights, viewed 13 February 2025, *https://www.amnesty.org/en/documents/mde16/7053/2023/en/*.

Amnesty International 2024a, The State of the World's Human Rights: April 2024, viewed 11 February 2025, *https://www.amnesty.org/en/documents/pol10/7200/2024/en/*.

Amnesty International 2024b, Jordan: New Cybercrimes Law stifling freedom of expression one year on, viewed 12 February 2025, *https://www.amnesty.org/en/latest/news/2024/08/jordan-new-cybercrimes-law-stifling-freedom-of-expression-one-year-on/*.

Amnesty International 2024c, Jordan: New Cybercrimes Law stifles freedom of expression, viewed 12 February 2025, *https://www.amnesty.org/en/documents/mde16/8424/2024/en/*.

AP News 2020, Nicaragua approves «cybercrimes» law, alarming rights groups, viewed 12 February 2025, *https://apnews.com/general-news-ce252ed4721a759ed329798a7e2e30db*.

AP News 2024, Tunisian commentator sentenced to two years under controversial anti-fake news law, viewed 12 February 2025, *https://apnews.com/article/tunisia-dahmani-decree-54-misinformation-crackdown-dissent-5d1cd879bb081796439a469db744014e*.

Article 19 2023, Tunisia: Decree-law No 54 of 2022, viewed 13 February 2025, *https://www.article19.org/wpcontent/uploads/2023/03/Analysis-of-decree-law-54-English.pdf*.

Association for Progressive Communications 2023, A framework for developing gender-responsive cybersecurity policy: Assessment tool, viewed 12 February 2025, *https://www.apc.org/en/pubs/framework-developing-gender-responsive-cybersecurity-policy-assessment-tool*.

Bada, M., Chua, Y.T., Collier, B. & Pete, I. 2021, ‹Cybersecurity and cybercrime: rethinking threats and responses›, in M. Christen, B. Gordijn & M. Loi (eds), The ethics of cybersecurity, The International Library of Ethics, Law and Technology, vol. 21, Springer, Cham, pp. 263–283, viewed 12 February 2025, *https://doi.org/10.1007/978-3-030-60527-8_14*.

BBC News 2024, Europe facing ‹wave of antisemitism›, survey finds, viewed 13 February 2025, *https://www.bbc.com/news/articles/c147w9572dvo*.

Benshimon, S. 2024, ‹Tunisie: Sonia Dahmani, avocate et chroniqueuse, condamnée à deux ans de prison›, Sahel Intelligence, viewed 12 February 2025, *https://sahel-intelligence.com/35554-tunisie-sonia-dahmani-avocate-etchroniqueuse-condamnee-a-deux-ans-de-prison.html*.

Bernarding, N. & Kobel, V. 2023, ‹Feminist Perspectives on the Militarisation of Cyberspace›, Centre for Feminist Foreign Policy, viewed 12 February 2025, *https://centreforfeministforeignpolicy.org/wordpress/wp-content/uploads/2023/06/CFFP_Briefing_Cybersecurity_final.pdf*.

Bhandari, V. & Kovacs, A. 2021, ‹What's sex got to do with it? Mapping the impact of questions of gender and sexuality on the evolution of the digital rights landscape in India›, Internet Democracy Project, viewed 12 February 2025, *https://cdn.internetdemocracy.in/idp/assets/downloads/reports/whats-sex-got-to-do-with-it-mapping-the-impact-of-questions-of-gender-and-sexuality-on-the-evolution-of-the-digital-rights-landscape-in-india/Vrinda-Bhandariand-Anja-Kovacs-Whats-Sex-Got-To-Do-with-It.pdf*.

Boutry, T. 2024, ‹Tunisie : une avocate et chroniqueuse condamnée à 8 mois de prison en appel pour avoir critiqué le pays›, Le Parisien, viewed 12 February 2025, *https://www.leparisien.fr/international/tunisie-uneavocate-et-chroniqueuse-condamnee-a-8-mois-de-prison-en-appel-pour-avoir-critique-le-pays-11-09-2024-RMEP-BERTQBDTRHFKY0H0D6CNWY.php*.

Centre for Feminist Foreign Policy 2021, The CFFP Glossary, viewed 13 February 2025, *https://centreforfeministforeignpolicy.org/2021/03/08/feminist-glossary-2/*.

Chatham House 2022, Gender mainstreaming and the proposed cybercrime convention: Commentary on the consolidated draft, viewed 13 February 2025, *https://www.chathamhouse.org/sites/default/files/2022-12/2022-12-21-Gender-mainstreaming-and-the-proposed-cybercrime-convention.pdf*.

Chatham House 2023, Integrating gender in cybercrime capacity-building: a toolkit, viewed 13 February 2025, *https://www.chathamhouse.org/sites/default/files/2023-07/2023-07-05-integrating-gender-in-cybercrimecapacity-building-emerson-keeler-et-al.pdf*.

Chatham House n.d., How can the cybercrime convention adopt a strategic approach to cybercrime capacity building and protect against potential harms and misuses?, viewed 13 February 2025, *https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/Multi-stakeholders/Chatham_House.pdf*.

Civicus Monitor 2023, Draconian cybercrime law used to target protesters, HRDs, journalists amid pro-Palestine protests, viewed 13 February 2025, *https://monitor.civicus.org/explore/draconian-cybercrime-law-used-to-targetprotesters-hrds-journalists-amid-pro-palestine-protests/*.

Columbia University n.d., ›Nyanzi v. Uganda', Global Freedom of Expression, viewed 12 February 2025, *https://globalfreedomofexpression.columbia.edu/cases/case-dr-stella-nyanzi/*.

Council of Europe 2021, Protecting women and girls from violence in the digital age: the relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women, viewed 12 February 2025, *https://rm.coe.int/the-relevance-of-the-ic-and-the-budapest-conventionon-cybercrime-in-a/1680a5eba3*.

Council of Europe 2022, The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform: Thematic paper of the Platform of Independent Expert Mechanisms on Discrimination and Violence against Women (EDVAW), viewed 13 February 2025, *https://www.ohchr.org/sites/default/files/documents/hrbodies/cedaw/statements/2022-12-02/EDVAW-Platform-thematic-paper-on-the-digital-dimension-of-VAW_English.pdf*.

Council on Foreign Relations 2024, Abortion Law: Global Comparisons, viewed 13 February 2025, *https://www.cfr.org/article/abortion-law-global-comparisons*.

Creutzfeldt, N., Kyprianides, A., Bradford, B. & Jackson, J. 2024, ‹Marginalized groups and unmet legal needs›, in Access to justice, digitalization and vulnerability: exploring trust in justice, Policy Press, Bristol, viewed 12 February 2025, *https://doi.org/10.1332/policypress/9781529229523.003.0009*.

Cybersecurity Tech Accord 2024a, Cybersecurity Tech Accord Statement to Reconvened concluding session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, viewed 13 February 2025, *https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP9/Cybersecurity_Tech_Accord_Statement_07.30_AHC7.13.pdf*.

Cybersecurity Tech Accord 2024b, Cybersecurity Tech Accord Submission to the Concluding Session of the Ad Hoc Committee to Elaborate a UN Convention on Countering Cybercrime, viewed 13 February 2025, *https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Concluding_session/Submissions/Multi-Stakeholders/Cybersecurity_Tech_Accord_-_7th_AHC_session_submission.pdf*.

Democracy Reporting International 2023, Online public discourse in the MENA region: Anti-immigrant hate speech, AI solutions, detecting online violence against women, and regional strategies, viewed 13 February 2025, *https://democracy-reporting.org/en/office/global/publications/online-public-discourse-in-the-mena-region-persistent-tactics-of-disinformation-and-an-increase-in-online-gender-based-violence*.

Derechos Digitales 2023, Human rights in digital environments in Nicaragua, viewed 12 February 2025, *https://www.derechosdigitales.org/nicaragua-2023-eng/*.

Derechos Digitales & Association for Progressive Communications 2023, When protection becomes an excuse for criminalisation: Gender considerations on cybercrime frameworks, viewed 12 February 2025, *https://www.apc.org/en/pubs/when-protection-becomes-excuse-criminalisation-gender-considerations-cybercrime-frameworks*.

Digital Rights Foundation n.d., Cyber Harassment Helpline, viewed 12 February 2025, *https://digitalrightsfoundation.pk/cyber-harassment-helpline/*.

Egypt 2018, Law No. 175 of 2018 on Anti-Cyber and Information Technology Crimes, WIPO Lex, viewed 13 February 2025, *https://www.wipo.int/wipolex/en/legislation/details/19959*.

EPICenter Works n.d., Joint letter to EU and member states on UN Cybercrime Convention, viewed 13 February 2025, *https://epicenter.works/fileadmin/user_upload/Joint_letter_to_EU_and_member_states_on_UN_Cybercrime_Convention.pdf*.

Freedom House 2024, Freedom on the Net 2024: The Struggle for Trust Online, viewed 11 February 2025, *https://freedomhouse.org/report/freedom-net/2024/struggle-trust-online*.

Freedom Online Coalition 2024, FOC Advisory Network Proactive Advice on UN Convention Against Cybercrime, viewed 13 February 2025, *https://freedomonlinecoalition.com/foc-advisory-network-proactive-advice-un-convention-against-cybercrime/*.

Gavrilovic Nilsson, M., Tzani Pepelasi, K., Ioannou, M. & Lester, D. 2019, ‹Understanding the link between sextortion and suicide›, International Journal of Cyber Criminology, vol. 13, no. 1, pp. 55–69, viewed 12 February 2025, *https://pure.hud.ac.uk/en/publications/understanding-the-link-between-sextortion-and-suicide*.

Ghai, Y. & Cottrell, J. (eds) 2009, Marginalized Communities and Access to Justice, Routledge, London, viewed 12 February 2025, *https://worldjusticeproject.org/our-work/publications/edited-volumes/marginalized-communities-and-access-justice*.

GenderIT.org 2008, Cybercrime legislation and gender, viewed 12 February 2025, *https://www.genderit.org/edition/cybercrime-legislations-and-gender*.

GenderIT.org 2018, 13 Manifestations of Gender-Based Violence Using Technology, viewed 13 February 2025, *https://www.genderit.org/resources/13-manifestations-gender-based-violence-using-technology*.

Gollan, J. 2023, ‹Websites Selling Abortion Pills Are Sharing Sensitive Data With Google›, Ms. Magazine, viewed 13 February 2025, *https://msmagazine.com/2023/01/18/google-abortion-pills-privacy-data/*.

Gullo, K. 2024, Protect Good Faith Security Research Globally in Proposed UN Cybercrime Treaty, Electronic Frontier Foundation, viewed 13 February 2025, *https://www.eff.org/deeplinks/2024/02/protect-good-faith-security-research-globally-proposed-un-cybercrime-treaty*.

Hakmeh, J. & Saunders, J. 2024, The Strategic Approach to Countering Cybercrime (SACC) Framework, Chatham House, London, viewed 12 February 2025, *https://www.chathamhouse.org/sites/default/files/2024-07/2024-07-11-strategic-approach-countering-cybercrime-framework-hakmeh-saunders.pdf*.

Hakmeh, J. 2024, ‹The UN convention on cybercrime: a milestone in cybercrime cooperation?›, Journal of Cyber Policy, vol. 9, no. 2, pp. 125–130, viewed 13 February 2025, *https://doi.org/10.1080/23738871.2024.2441549*.

Hassan, Z. & Hellyer, H.A. 2024, Suppressing Dissent: Shrinking Civic Space, Transnational Repression and Palestine–Israel, Carnegie Endowment for International Peace, viewed 13 February 2025, *https://carnegieendowment.org/research/2024/10/suppressing-dissent-shrinking-civic-space-transnational-repression-and-palestine-israel?lang=en*.

Human Rights Foundation 2017, Uganda: Drop «Cyber-Harassment» Charges Against Activist for Facebook Posts, viewed 12 February 2025, *https://archive.hrf.org/press-release-uganda-drop-cyber-harassment-charges-against-activist-for-facebook-posts/*.

Human Rights Watch 2020, Egypt: Spate of «Morality» prosecutions of women, viewed 12 February 2025, *https://www.hrw.org/news/2020/08/17/egypt-spate-morality-prosecutions-women*.

Human Rights Watch 2021, Abuse of cybercrime measures taints UN talks, viewed 12 February 2025, *https://www.hrw.org/news/2021/05/05/abuse-cybercrime-measures-taints-un-talks*.

Human Rights Watch 2023a, Libya: revoke repressive anti-cybercrime law, viewed 12 February 2025, *https://www.hrw.org/news/2023/04/03/libya-revoke-repressive-anti-cybercrime-law*.

Human Rights Watch 2023b, Tunisia: cybercrime decree used against critics, viewed 12 February 2025, *https://www.hrw.org/news/2023/12/19/tunisia-cybercrime-decree-used-against-critics*.

Human Rights Watch 2023c, «All This Terror Because of a Photo»: Digital Targeting and Its Offline Consequences for LGBT People in the Middle East and North Africa, viewed 13 February 2025, *https://www.hrw.org/report/2023/02/21/all-terror-because-photo/digital-targeting-and-its-offline-consequences-lgbt*.

Human Rights Watch 2024a, Uganda: Court Upholds Anti-Homosexuality Act, viewed 12 February 2025, *https://www.hrw.org/news/2024/04/04/uganda-court-upholds-anti-homosexuality-act*.

Human Rights Watch 2024b, Jordan: Arrests, Harassment of Pro-Palestine Protesters, viewed 12 February 2025, *https://www.hrw.org/news/2024/02/06/jordan-arrests-harassment-pro-palestine-protesters*.

Human Rights Watch 2024c, Russia: First Convictions Under LGBT «Extremist» Ruling, viewed 12 February 2025, *https://www.hrw.org/news/2024/02/15/russia-first-convictions-under-lgbt-extremist-ruling*.

Human Rights Watch 2024d, Upcoming cybercrime treaty will be nothing trouble, viewed 13 February 2025, *https://www.hrw.org/news/2024/08/07/upcoming-cybercrime-treaty-will-be-nothing-trouble*.

Hu, Y., Chen, X. & Bose, I. 2013, ‹Cybercrime enforcement around the globe›, Journal of Information Privacy and Security, vol. 9, no. 3, pp. 34–52, viewed 12 February 2025, *https://doi.org/10.1080/15536548.2013.10845684*.

Hollingworth, D. 2024, ‹Tech companies call for changes to draft UN Cybercrime Convention›, Cyber Daily, viewed 13 February 2025, *https://www.cyberdaily.au/security/10895-tech-companies-call-for-changes-to-draft-uncybercrime-convention*.

International Association of Women Judges n.d., Naming, shaming, ending sextortion: A Toolkit, viewed 13 February 2025, *https://www.unodc.org/res/ji/import/guide/naming_shaming_ending_sextortion/naming_shaming_ending_sextortion.pdf*.

International Chamber of Commerce 2024, Global business urges governments to reject new international cybercrime treaty, viewed 13 February 2025, *https://iccwbo.org/news-publications/news/global-business-urges-governments-to-reject-new-international-cybercrime-treaty/*.

International Telecommunication Union 2023, Population of global offline continues steady decline to 2.6 billion people in 2023, viewed 12 February 2025, *https://www.*

itu.int/en/mediacentre/Pages/PR-2023-09-12-universaland-meaningful-connectivity-by-2030.aspx.

International Telecommunication Union 2024, Measuring Digital Development: Facts and Figures 2024, viewed 12 February 2025, *https://www.itu.int/hub/publication/D-IND-ICT_MDD-2024-4/*.

Jain, G. 2024, ‹From buttocks to electronic bracelets: How governments are using cybercrime laws to target women and LGBTQIA+ people›, Association for Progressive Communications, viewed 13 February 2025, *https://www.apc.org/en/news/buttocks-electronic-bracelets-how-governments-are-using-cybercrime-laws-target-women-and*.

Jbour, A. 2023, ‹Jeopardizing digital rights in Jordan›, Carnegie Endowment for International Peace, viewed 12 February 2025, *https://carnegieendowment.org/sada/2023/08/jeopardizing-digital-rights-in-jordan?lang=en*.

Jordan Prime Minister's Office قانون رقم 17 لسنة 2023 لمكافحة الجرائم الإلكترونية , 2023 [Jordan's new Law No. 17 of 2023 on Combating Cybercrimes], viewed 13 February 2025, *https://perma.cc/7RSM-6S4K*.

Juma, A. & Knipp, K. 2020, ‹Egypt imprisons female TikTok influencers›, DW, viewed 12 February 2025, *https://www.dw.com/en/egyptian-tiktok-stars-jailed/a-54371869*.

Kävrestad, J., Birath, M. & Clarke, N. 2024, ‹Cyber-Dependent Crime, Cyber-Enabled Crime, and Digital Evidence›, in Fundamentals of Digital Forensics, Texts in Computer Science, Springer, Cham, viewed 12 February 2025, *https://doi.org/10.1007/978-3-031-53649-6_6*.

Kataeva, Z., Durrani, N., Izekenova, Z. & Roshka, V. 2024, ‹Thirty years of gender mainstreaming: Evolution, development, and future research agenda through a bibliometric approach›, Women's Studies International Forum, vol. 107, viewed 13 February 2025, *https://doi.org/10.1016/j.wsif.2024.103010*.

La Presse 2024, Décret loi n°54 : Sonia Dahmani condamnée à un an de prison, viewed 12 February 2025, *https://lapresse.tn/2024/07/06/decret-loi-n54-sonia-dahmani-condamnee-a-un-an-de-prison/*.

Leukfeldt, E.R., Notté, R.J. & Malsch, M. 2019, ‹Exploring the needs of victims of cyber-dependent and cyber-enabled crimes›, Victims & Offenders, vol. 15, no. 1, pp. 60–77, viewed 12 February 2025, *https://doi.org/10.1080/15564886.2019.1672229*.

Lima, V. & Gomez, M. 2021, ‹Access to Justice: Promoting the Legal System as a Human Right›, in Leal Filho, W, Marisa Azul, A, Brandli, L, Lange Salvia, A, Özuyar, P.G & Wall, T (eds), Peace, Justice and Strong Institutions.

Encyclopedia of the UN Sustainable Development Goals, Springer, Cham, viewed 13 February 2025, *https://doi.org/10.1007/978-3-319-95960-3_1*.

Libya 2022, Law No. 5 of 2022 regarding Combating Cybercrimes, The Law Society of Libya, viewed 13 February 2025, *https://lawsociety.ly/en/legislation/law-no-5-of-2022-regarding-combating-cybercrimes/*.

McCubbin, J. 2024, ‹Sextortion: The deadly scam targeting young men›, BBC News, viewed 12 February 2025, *https://www.bbc.com/news/articles/cq82lyg5vpjo*.

McGuire, M. & Dowling, S. 2013, Cyber crime: A review of the evidence: Research Report 75 - Summary of key findings and implications, UK Home Office, viewed 13 February 2025, *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf*.

Makooi, B. 2023, ‹Egypt's female social media influencers face arrest, jail on „morality« charges›, France 24, viewed 12 February 2025, *https://www.france24.com/en/middle-east/20230411-egypt-s-female-social-media-influencers-face-arrest-jail-on-morality-charges*.

Maimon, D. & Louderback, E.R. 2019, ‹Cyber-Dependent Crimes: An Interdisciplinary Review›, Annual Review of Criminology, vol. 2, no. 1, pp. 191–216, viewed 12 February 2025, *https://doi.org/10.1146/annurev-criminol-032317-092057*.

Mendel, T. n.d., ‹Freedom of expression: a guide to the interpretation and meaning of Article 10 of the European Convention on Human Rights›, Council of Europe, viewed 12 February 2025, *https://rm.coe.int/16806f5bb3*.

Microsoft 2024, Cybercrime Convention Negotiations Microsoft's submission to the Seventh Reconvened Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, viewed 13 February 2025, *https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/0P9/Microsoft_-_Reconvened_Substantive_Session.pdf*.

Miranda Aburto, W. 2024, ‹Nicaragua tightens control of social media to censor dissent›, El País, viewed 12 February 2025, *https://english.elpais.com/international/2024-09-12/nicaragua-tightens-control-of-social-mediato-censor-dissent.html*.

Mwesigwa, A. 2017, ‹Jailed for calling Ugandan president a «pair of buttocks», activist vows to fight on›, The Guardian, viewed 12 February 2025, *https://www.theguardian.com/global-development/2017/jun/19/jailed-for-calling-ugandan-president-museveni-a-pair-of-buttocks-activist-vows-to-fight-on-stella-nyanzi*.

Nord, M., Lundstedt, M., Altman, D., Angiolillo, F., Borella, C., Fernandes, T., Gastaldi, L., Good God, A., Natsika, N. & Lindberg, S.I. 2024, Democracy Report 2024: Democracy Winning and Losing at the Ballot, V-Dem Institute, University of Gothenburg, viewed 12 February 2025, *https://v-dem.net/documents/43/v-dem_dr2024_lowres.pdf*.

OMCT 2021, Nicaragua: criminalización de Amaru Ruiz Alemán, viewed 12 February 2025, *https://www.omct.org/es/recursos/llamamientos-urgentes/nicaragua-criminalizaci%C3%B3n-de-amaru-ruiz-alem%C3%A1n*.

OHCHR 2018, Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective, A/HRC/38/47, viewed 12 February 2025, *https://www.ohchr.org/en/documents/thematic-reports/ahrc3847-report-special-rapporteur-violenceagainst-women-its-causes-and*.

Palassis, A., Speelman, C.P. & Pooley, J.A. 2021, ‹An Exploration of the Psychological Impact of Hacking Victimization›, SAGE Open, vol. 11, no. 4, pp. 1–12, viewed 12 February 2025, *https://doi.org/10.1177/21582440211061556*.

Pavlova, P. 2024, Gendered Harms of Data Weaponization: Historical Patterns, New Battlefields, and the Implications for Democracy and National Security, New America, viewed 12 February 2025, *https://www.newamerica.org/future-security/reports/gendered-harms-of-data-weaponization/*.

Penal Reform International 2012, Access to Justice: Discrimination of Women in Criminal Justice Systems, viewed 12 February 2025, *https://cdn.penalreform.org/wp-content/uploads/2013/08/BRIEFING-Discrimination-womencriminal-justice.pdf*.

ProtectDefenders.eu 2021, Nicaragua: harassment and killings of human rights defenders, viewed 12 February 2025, *https://protectdefenders.eu/nicaragua-harassment-and-killings-of-human-rights-defenders/*.

RadioFreeEurope/RadioLiberty 2021, Afghan women move protests to social media to evade violent Taliban response, viewed 12 February 2025, *https://www.rferl.org/a/afghanistan-women-rights-protests-taliban/31598129.html*.

Revenge Porn Helpline n.d., South West Grid for Learning (SWGfL), viewed 12 February 2025, *https://swgfl.org.uk/research/revenge-porn-helpline-annual-report/*.

Rigot, A. 2020, ‹Egypt's economic courts are being used to target LGBTQ people›, Slate, viewed 12 February 2025, *https://slate.com/technology/2020/12/egypt-lgbtq-crime-economic-courts.html*.

Rodriguez, K. 2024, ‹EFF's Concerns About the UN Draft Cybercrime Convention›, Electronic Frontier Foundation, viewed 13 February 2025, *https://www.eff.org/deeplinks/2024/07/effs-concerns-about-un-draft-cybercrime-convention*.

Robalo, T.L.A.S. & Abdul Rahim, R.B.B. 2023, ‹Cyber Victimisation, Restorative Justice and Victim-Offender Panels›, Asian Journal of Criminology, vol. 18, no. 1, pp. 61–74, viewed 12 February 2025, *https://doi.org/10.1007/s11417-023-09396-9*.

Sarre, R, Lau, L.Y-C & Chang, L.Y.C. 2018, ‹Responding to cybercrime: current trends›, Police Practice and Research, vol. 19, no. 6, pp. 515–518, viewed 12 February 2025, *https://doi.org/10.1080/15614263.2018.1507888*.

Scher-Zagier, E. 2024, ‹The New UN Cybercrime Treaty Is a Bigger Deal Than Even Its Critics Realize›, Lawfare, viewed 13 February 2025, *https://www.lawfaremedia.org/article/the-new-un-cybercrime-treaty-is-a-bigger-dealthan-even-its-critics-realize*.

Seitenova, A., Kobel, V. & Bernarding, N. 2024, Strongmen and Violence: Interlinkages of Anti-Feminism and Anti-Democratic Developments, Centre for Feminist Foreign Policy, viewed 13 February 2025, *https://centreforfeministforeignpolicy.org/wordpress/wp-content/uploads/2024/02/CFFP-strongmen-and-violence.pdf*.

Shires, J., Hassib, B. & Swali, A. 2024, Gendered Hate Speech, Data Breach, and State Overreach: Identifying the Connections Between Gendered Cyber Harms to Shape Better Policy Responses, Chatham House, viewed 12 February 2025, *https://www.chathamhouse.org/sites/default/files/2024-05/2024-05-24-gendered-cyber-harmss-hires-et-al_0.pdf*.

Smith, T. & Crawford, A. 2024, ‹Sextortion guides sold on social media, BBC finds›, BBC News, viewed 12 February 2025, *https://www.bbc.com/news/articles/cp00y03q-93mo*.

SMEX n.d., Digital Safety Helpdesk, viewed 12 February 2025, *https://smex.org/help-desk/*.

StopNCII.org n.d., Stop Non-Consensual Intimate Image Abuse, viewed 12 February 2025, *https://stopncii.org/*.

Stock, E. 2021, ‹Two new laws intensify the crackdown on journalists in Nicaragua›, International Center for Journalists,viewed 12 February 2025, h*ttps://www.icfj.org/news/two-new-laws-intensify-crackdown-journalists-nicaragua*.

SWGfL n.d., Intimate image abuse: an evolving landscape, SWGfL, viewed 12 February 2025, *https://revengepornhelpline.org.uk/assets/documents/intimate-image-abuse-an-evolving-landscape.pdf*.

Tennant, I. & Oliveira, A.P. 2024, ‹Applying the right lessons from the negotiation and implementation of the UNTOC and the UNCAC to the implementation of the newly agreed UN «cybercrime» treaty›, Journal of Cyber Policy, vol. 9, no. 2, pp. 221–238, viewed 13 February 2025, *https://doi.org/10.1080/23738871.2024.2428655*.

The Independent 2023, Law that criminalised Stella Nyanzi, Kakwenza kicked out, viewed 12 February 2025, *https://www.independent.co.ug/law-that-criminalised-stella-nyanzi-kakwenza-kicked-out/*.

The New Arab 2023, Egyptian model sentenced to 2 years in jail for «debauchery», viewed 12 February 2025, *https://www.newarab.com/news/egyptian-model-sentenced-2-years-jail-debauchery*.

The New York Times 2023, Antisemitic and Anti-Muslim Hate Speech Surges Across the Internet, viewed 13 February 2025, *https://www.nytimes.com/2023/11/15/technology/hate-speech-israel-gaza-internet.html*.

Tidy, J. 2024, ‹Dead in 6 hours: How Nigerian sextortion scammers targeted my son›, BBC News, viewed 12 February 2025, *https://www.bbc.com/news/articles/c2llzppyx05o*.

Treaty on the Functioning of the European Union [2008] OJ C115/47, art 218(11), Official Journal of the European Union, viewed 12 February 2025, *https://eur-lex.europa.eu/eli/treaty/tfeu_2008/art_218/oj/eng*.

Tunisia 2022, Décret Loi n°2022-54 du 13 septembre 2022 relatif à la lutte contre les infractions se rapportant aux systèmes d'information et de communication, DCAF, viewed 13 February 2025, *https://legislation-securite.tn/latest-laws/decret-loi-n-2022-54-du-13-septembre-2022-relatif-a-la-lutte-contre-les-infractions-se-rapportant-auxsystemes-dinformation-et-de-communication/*.

Uganda 2011, The Computer Misuse Act, Government of Uganda, viewed 13 February 2025, *https://commons.laws.africa/akn/ug/act/2011/2/media/publication/ug-act-2011-2-publication-document.pdf*.

United Nations General Assembly 2021, Promotion and protection of the right to freedom of opinion and expression, A/76/258, viewed 12 February 2025, https://documents.un.org/doc/undoc/gen/n21/212/16/pdf/n2121216.pdf.

United Nations General Assembly 2024a, Resolution 79/243: United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, viewed

11 February 2025, *https://documents.un.org/access.nsf/get?DS=A/RES/79/243&Lang=E*.

United Nations General Assembly 2024b, Global threats to freedom of expression arising from the conflict in Gaza, United Nations, viewed 13 February 2025, *https://documents.un.org/doc/undoc/gen/n24/247/88/pdf/n2424788.pdf*.

United Nations Human Rights Committee 2011, General comment no. 34: Article 19: freedoms of opinion and expression, CCPR/C/GC/34, viewed 12 February 2025, *https://documents.un.org/doc/undoc/gen/g11/453/31/pdf/g1145331.pdf*.

United Nations Human Rights Council 2019a, Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/41/35, viewed 12 February 2025, *https://www.ohchr.org/en/documents/thematic-reports/ahrc4135-surveillance-and-human-rights-report-special-rapporteur*.

United Nations Human Rights Council 2019b, Impact of measures to address terrorism and violent extremism on civic space and the rights of civil society actors and human rights defenders: Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/40/52, viewed 12 February 2025, *https://docs.un.org/en/A/HRC/40/52*.

United Nations Human Rights Council 2020, Report of the Special Rapporteur on the right to privacy, A/HRC/43/52, viewed 12 February 2025, *https://documents.un.org/doc/undoc/gen/g20/071/66/pdf/g2007166.pdf*.

United Nations High Commissioner for Human Rights 2018, The Right to Privacy in the Digital Age, A/HRC/39/29, United Nations, viewed 12 February 2025, *https://digitallibrary.un.org/record/1640588/files/A_HRC_39_29-EN.pdf?ln=en*.

United Nations High Commissioner for Human Rights n.d., Information Note: Human rights and the draft Cybercrime Convention, viewed 13 February 2025, *https://www.ohchr.org/sites/default/files/documents/issues/civicspace/DRAFT-CYBERCRIME-CONVENTION.pdf*.

UN News 2024, UN adopts landmark convention to combat cybercrime, viewed 11 February 2025, *https://news.un.org/en/story/2024/12/1158521*.

UNODC n.d., Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, viewed 13 February 2025, *https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home*.

UNODC n.d., University Module Series: Cybercrime - Module 2: General Types of Cybercrime, viewed 13 February 2025, *https://www.unodc.org/e4j/en/cybercrime/module-2/index.html*.

UNODC n.d., SHERLOC – Database on Cybercrime Legislation, viewed 12 February 2025, *https://sherloc.unodc.org/cld/v3/sherloc/legdb/search.html?lng=en#?c=%7B%22filters%22:%5B%7B%22fieldName%22:%22en%23__el.legislation.crimeTypes_s%22,%22value%22:%22Cybercrime%22%7D%5D,%22sortings%22:%22%22%7D*.

UNODC 2023, Consolidated negotiating document on the general provisions and the provisions on criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, viewed 13 February 2025, *https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/CND_21.01.2023_-_Copy.pdf*.

UNRIC 2024, Cyberviolence against women and girls: the growing threat of the digital age, viewed 12 February 2025, *https://unric.org/en/cyberviolence-against-women-and-girls-the-growing-threat-of-the-digital-age/*.

UN Women n.d., Libya, viewed 12 February 2025, *https://arabstates.unwomen.org/en/countries/libya*.

U.S. Attorney's Office, Southern District of Indiana 2023, FBI and partners issue national public safety alert on sextortion schemes, viewed 12 February 2025, *https://www.justice.gov/usao-sdin/pr/fbi-and-partners-issue-national-public-safety-alert-sextortion-schemes*.

Uhlich, M., Tan, R.K.J., Azevedo, V. et al. 2024, ‹Online harassment during COVID-19: a cross-sectional analysis across 10 countries from the I-SHARE consortium›, Journal of Public Health (Berl.), viewed 12 February 2025, *https://doi.org/10.1007/s10389-024-02332-w*.

Victim Support n.d., viewed 12 February 2025, *https://www.victimsupport.org.uk/*.

Walker, S. & Oliveira, A.P. 2024a, ‹The final call: UN member states adopt a new cybercrime treaty›, Global Initiative Against Transnational Organized Crime, viewed 13 February 2025, *https://globalinitiative.net/wp-content/uploads/2024/09/Summer-Walker-Ana-Paula-Oliveira-The-final-call-UN-member-states-adopt-a-new-cybercrimetreaty-GI-TOC-September-2024.pdf*.

Walker, S. & Oliveira, A.P. 2024b, ‹The Final Call: UN Member States Adopt a New Cybercrime Treaty›, Global Initiative Against Transnational Organized Crime, viewed 13 February 2025, *https://globalinitiative.net/analysis/the-final-call-un-member-states-adopt-a-new-cybercrime-treaty/*.

Wong, O. 2024, Cyberwarfare: The ‹Pink Tax› of Hacking, Centre for International and Defence Policy, Queen's University, Kingston, Ontario, viewed 13 February 2025, *https://www.queensu.ca/cidp/sites/cidpwww/files/uploaded_files/9-2%20CIDP%20-%20PolicyBrief%20Owen%20Wong%20Apr2024.pdf*.

Wright, D. 2024, ‹A Global Framework for Change: Discussing NCII at the UN Cybercrime Convention›, SWGfL, viewed 13 February 2025, *https://swgfl.org.uk/magazine/a-global-framework-for-change-discussing-ncii-at-the-uncybercrime-convention/*.

Zaghdoudi, A. 2023, Freedom of Expression at risk in Tunisia: a legal framework that favors silence, Access Now, viewed 12 February 2025, *https://www.accessnow.org/wp-content/uploads/2023/05/FoE-Report-English-Final.pdf*.

Die Autor*innen

Vivienne Kobel ist Projektmanagerin beim Centre for Feminist Foreign Policy in Berlin. Sie hat einen Bachelor of Arts in Internationalen Beziehungen (TU-Dresden) und Master of Arts in International Affairs der FU Berlin und SciencePo Paris.

Pavlina Pavlowa ist Expertin für internationale Cybersicherheit und Cyberkriminalität mit langjähriger Erfahrung in Politik, Diplomatie und Governance, unter anderem bei den Vereinten Nationen und der OSZE. Pavlova war an zentraler Stelle in UN-Verhandlungen zu verantwortungsvollem staatlichen Verhalten im Cyberspace und zum Übereinkommen gegen Cyberkriminalität beteiligt und leitet die Arbeitsgruppe Cybercrime bei Crime Alliance.

Impressum

Herausgeberin: Heinrich-Böll-Stiftung e.V., Gunda-Werner-Institut und
Globale Einheit für Menschliche Sicherheit
Schumannstraße 8, 10117 Berlin
Fachkontakt: Katherina Klappheck, Gunda-Werner-Institut **E** *klappheck@boell*,
Simon Ilse, Globale Einheit für Menschliche Sicherheit (Büro Wien) **E** *simon.ilse@at.boell.org*

Erscheinungsort: *www.boell.de*
Erscheinungsdatum: Oktober 2025
Übersetzung: Friederike Hofert
Covermotiv: © Freepik/EyeEm

Weitere E-Books zum Downloaden unter: *www.boell.de/publikationen*