Forderungspapier

UN Cybercrime Convention

27. November 2024

Ausgangslage

Seit dem Jahr 2004 ist in Europa und darüber hinaus die sogenannte "Budapest Konvention" des Europarats in Kraft, mit deren Hilfe Computerkriminalität bekämpft werden soll.[1] Dennoch erzielte Russland mit Unterstützung einiger weiterer Staaten[2] im Jahr 2019 eine knappe Mehrheit in der Generalversammlung der Vereinten Nationen, um ein Übereinkommen zur Bekämpfung von Computerkriminalität ("UN Cybercrime Convention") auf UN-Ebene zu erarbeiten. Am 8. August 2024 einigte man sich auf einen finalen Text. Dieser soll zwischen 15. und 20. Dezember 2024 von der Generalversammlung als Übereinkommen der Vereinten Nationen angenommen werden.

Der Widerstand gegen den Entwurf des Übereinkommens war und ist stark und umfasst Menschenrechtsgruppen, Organisationen für Medienfreiheit, das Büro des UN-Hochkommissars für Menschenrechte (OHCHR), führende Sicherheitsforscher, große Technologieunternehmen und Industrieverbände.

Er zeigt die Notwendigkeit einer klaren Abkehr von dem unverändert schädlichen und fehlgeleiteten Ansatz der Staatenvertreter:innen: Die Unterstützung Österreichs (gemeinsam mit den übrigen EU-Mitgliedsstaaten) für die Annahme des Textes als Übereinkommen der Vereinten Nationen würde zu einer raschen und breiten Ratifizierung weltweit beitragen, Demokratie, Menschenrechte und Rechtsstaatlichkeit untergraben, eine Vielzahl von marginalisierten Gruppen gefährden, sowie auch die Sicherheit und Privatsphäre von Internetnutzer:innen auf der ganzen Welt.

Doch auch für den Fall einer Annahme des Textes in der zweiten Dezemberhälfte haben sich erst zu Beginn dieses Monats die USA im „Third Committee" der Generalversammlung explizit gegen eine rasche Unterschrift und Ratifikation ausgesprochen und dies mit den Bedenken bezüglich fehlender Menschenrechts- und Sicherheitsgarantien begründet.

Konkrete Probleme

Übermäßig breiter Anwendungsbereich und Rechtsunsicherheit

Der Anwendungsbereich des Übereinkommens ist zu weit gefasst. Er umfasst auch Straftaten, bei denen ein Computersystem lediglich zur Ausführung verwendet wird, die an sich Straftat selbst aber auch auf andere Art und Weise begangen werden kann und bereits in den Strafgesetzen enthalten ist (z.B. Betrug → Internetbetrug), jedoch nicht Computerkriminalität im eigentlichen, engeren Sinn darstellen.

Außerdem wird der Anwendungsbereich auf eine unbestimmte Liste weiterer möglicher Straftaten ausgedehnt, was dem Legalitätsprinzip widerspricht.[3] Darüber hinaus soll bereits zwei Jahre

1 Aktuell zählt die Budapester Konvention 76 Mitglieder und 20 Beobachterstaaten, https://www.coe.int/en/web/cybercrime/parties-observers.

2 Diese waren China, Kambodscha, Belarus, Nord Korea, Myanmar, Iran, Venezuela und Nicaragua.

3 Etwa durch Verweis auf Straftaten, die in UN-Übereinkommen und Protokollen enthalten sind. Es wird hier aber nicht präzisiert, ob es sich dabei um ein Übereinkommen oder ein Protokoll handeln muss, das von der UN-Generalversammlung angenommen wurde, oder um einen Vertrag, der einfach gemäß Artikel 102 der UN-Charta bei den Vereinten Nationen

nach Annahme des Übereinkommens bei den Vereinten Nationen – und ohne abzuwarten, wie dieses sich in der Praxis bewährt - auch bereits über ein "ergänzendes Protokoll" verhandelt werden, das sich mit zusätzlichen Straftaten befasst. Dies erhöht zusätzlich die Gefahr einer weiteren Ausdehnung der strafbaren Handlungen, ohne Begleitung durch entsprechende menschenrechtliche Sicherheitsmaßnahmen (siehe dazu weiter unten). Diese Unsicherheiten bergen die Gefahr, dass legitime Online-Äußerungen kriminalisiert werden, was eine abschreckende Wirkung hat, die der Rechtsstaatlichkeit schadet.

Widerspruch zu europarechtlichen Bestimmungen

Dem Übereinkommensentwurf fehlt es an Klarheit über die Haftung von Online-Plattformen für Straftaten, die von ihren Nutzer:innen begangen werden.[4] Konkret fehlt die Erfordernis der vorsätzlichen Teilnahme an Straftaten, was auch im Widerspruch zur Bestimmung über die Beteiligung natürlicher Personen an einer Straftat steht, der Vorsatz voraussetzt.[5] Dies birgt die Gefahr, dass Online-Plattformen für die von ihren Nutzer:innen verbreiteten Informationen haftbar gemacht werden können, auch wenn sie keine Kenntnis von der Rechtswidrigkeit des Inhalts haben. Dies steht einerseits im Widerspruch zum „Digital Services Act" der EU, in dem durchgehend tatsächliche Kenntnis oder Bewusstsein als Standard genannt sind. Andererseits schafft es den Anreiz für übermäßig umfassende Moderationsbemühungen der Plattformen zum Nachteil der Meinungsäußerungsfreiheit.

Unzureichender Schutz für gutgläubige Akteure

Der Übereinkommensentwurf enthält keine ausreichenden Formulierungen zum Schutz gutgläubiger Akteure, wie z.B. Sicherheitsforscher:innen (unabhängig davon, ob es sich um das autorisierte Testen oder den proaktiven Schutz eines Informations- und Kommunikationstechnologiesystems handelt), Hinweisgeber:innen, Aktivist:innen und Journalist:innen, vor einer übermäßigen Kriminalisierung. Es riskiert damit, seinen eigenen Existenzzweck – nämlich die Bekämpfung von Computerkriminalität – zu unterminieren.

Fehlen von spezifischen Menschenrechtsgarantien

Das Abkommen enthält keine spezifischen Menschenrechtsgarantien, wie sie von zivilgesellschaftlichen Organisationen und dem UN-Hochkommissariat für Menschenrechte gefordert wurden, um Klarheit und Rechtssicherheit unter den Mitgliedstaaten zu schaffen und die Anwendung des Vertrags ohne unrechtmäßige Einschränkung der Menschenrechte und Grundfreiheiten zu erleichtern.[6]

Weiters sind die zahlreichen Verweise auf nationales Recht sowie das Fehlen folgender Sicherheitsmaßnahmen in einer Schlüsselbestimmung bedenklich:[7]

- Richtervorbehalt sowie die Prüfung der Verhältnismäßigkeit während der gesamten Anwendung der (teilweise überschießenden) Überwachungsmaßnahmen;
- Anwendbarkeit zentraler Menschenrechtsgrundsätze der Rechtmäßigkeit, Notwendigkeit und Nichtdiskriminierung;

registriert
4 Artikel 18.
5 Artikel 19.
6 Artikel 6.
7 Artikel 24 (2).

- Angemessene Unterrichtung der betroffenen Personen über deren Überwachung, sobald dies die Ermittlungen nicht mehr gefährdet (aktuell erfolgt die Überwachung unter dauerhafter Geheimhaltung), um das im Vertragstext genannte Recht auf einen wirksamen Rechtsbehelf überhaupt erst zu ermöglichen;
- Regelmäßige Berichte, einschließlich statistischer Daten über den Einsatz solcher Maßnahmen.

Auch beziehen sich die Menschenrechtsgarantien nur auf Teile des Abkommens, aber nicht auf den gesamten Text, wie etwa auch – und wohl besonders wichtig - auf die internationale Zusammenarbeit. Dies bedeutet in der Praxis, dass ein Großteil des grenzüberschreitenden Austauschs von Beweismitteln im Rahmen des Übereinkommens ohne sinnvolle Bedingungen und Schutzmaßnahmen erfolgen kann.

Verfahrensrechtliche Maßnahmen und Strafverfolgung

Das Übereinkommen erweitert den Anwendungsbereich der verfahrensrechtlichen Maßnahmen auf die Untersuchung von Straftaten, die über jene, die in dem Übereinkommen aufgeführt sind, hinaus, was auch ihre Eingriffsintensität und das Missbrauchspotenzial erhöht. Diese Gefahr wird durch überschießende Überwachungsmaßnahmen – wie etwa die Echtzeitüberwachung von Inhalts- und Verkehrsdaten - verstärkt,[8] die Eingriffe in die Privatsphäre ohne ausreichende Garantien ermöglichen und möglicherweise die Cybersicherheit und Verschlüsselung unterminieren, sowie zu einer Proliferation von Spyware führen.

Internationale Zusammenarbeit

Der Anwendungsbereich der internationalen Zusammenarbeit der Strafverfolgungsbehörden beschränkt sich nicht auf die im Übereinkommen selbst genannten Straftaten, was möglicherweise verstärkt zu Missbrauch führen wird. Auch sind die ohnehin mangelhaften Menschenrechtsgarantien auf diesen Teil der Konvention nicht anwendbar und auch der Artikel zum Datenschutz ist unzureichend, um Missbrauch der Konvention vorzubeugen.[9]

Das Übereinkommen ermutigt die Vertragsstaaten etwa, auch bilaterale und multilaterale Vereinbarungen zu treffen, um die Übermittlung personenbezogener Daten zu erleichtern, wodurch die Gefahr besteht, dass das durch EU-Recht garantierte Datenschutzniveau untergraben wird.[10]

Aber auch betreffend die Übermittlung personenbezogener Daten in voller Übereinstimmung mit dem Datenschutzrahmen des ersuchten Staates fehlt es an klaren, präzisen, unzweideutigen und wirksamen Normen zum Schutz personenbezogener Daten im ersuchenden Staat und um zu

8 Insbesondere Artikel 28 (4), 29 und 30.

9 So verlangt etwa Artikel 40 das „größtmögliche Maß an Rechtshilfe“ für Straftaten, die Straftaten, die im Einklang mit dem Übereinkommen festgelegt sind, sowie für jede schwere Straftat nach dem innerstaatlichen Recht des ersuchenden Staates. Insbesondere in den Fällen, in denen kein Rechtshilfevertrag zwischen den Vertragsstaaten gilt zwischen den Vertragsstaaten kein Vertrag über die Rechtshilfe besteht, enthalten die Absätze 8 bis 31 umfassende Vorschriften über die Verpflichtungen zur Rechtshilfe mit einem Vertragsstaat mit allgemein unzureichenden Menschenrechtsgarantien Garantien und Ablehnungsgründen. Zum Beispiel legt Absatz 22 eine hohe Messlatte von „stichhaltige Gründe für die Annahme“, dass der ersuchte Staat die Rechtshilfe verweigern kann.
Wenn die Vertragsstaaten personenbezogene Daten nicht in Übereinstimmung mit ihren geltenden Rechtsvorschriften übermitteln können, wie dem EU-Datenschutzrahmen, kann die widersprüchliche Verpflichtung in Artikel 40, dem ersuchenden Staat „das größtmögliche Maß an Rechtshilfe“ zu gewähren, einen unangemessenen Anreize für die Übermittlung personenbezogener Daten unter angemessenen Bedingungen gemäß Artikel 36 Absatz 1 Buchstabe b, z. B. durch Ausnahmeregelungen für bestimmte Situationen in Artikel 38 der EU-Rechtsdurchsetzungsrichtlinie Durchsetzungsrichtlinie.

10 Artikel 36 Absatz 1 lit. c.

verhindern, dass personenbezogene Daten in einer Weise weiterverarbeitet und an andere Staaten übermittelt werden, die die das Grundrecht auf Privatsphäre und Datenschutz verletzen können.[11]

Lösungen

1. Österreich soll bei der **Abstimmung in der UN-Generalversammlung** zwischen 15. und 20. Dezember 2024 über die Annahme der Konvention als Übereinkommen der Vereinten Nationen **gegen dieses stimmen bzw. sich zumindest der Stimme enthalten** und darauf hinwirken, dass andere Staaten (vor allem Mitgliedsstaaten der Europäischen Union) es ihm gleichtun.
2. Sollte die Konvention dennoch als Übereinkommen der Vereinten Nationen angenommen werden, soll Österreich sie in weiterer Folge und so lange die vorstehend genannten, schwerwiegenden Mängel fortbestehen **nicht unterschreiben und nicht ratifizieren**.
3. Schwerpunktsetzung auf die fortlaufenden Verhandlungen zur Konvention
    1. Österreich soll sich allerdings weiterhin **proaktiv in den Verhandlungen zu einem ergänzenden Protokoll zur Konvention beteiligen**, die zwei Jahre nach Annahme des Übereinkommens beginnen und in demselben Format geführt werden, wie bereits die Verhandlungen über das Übereinkommen selbst. Eine Ratifikation wäre daher nicht Voraussetzung dafür, um weiterhin involviert sein zu können.
    2. In diesen Verhandlungen soll sich Österreich proaktiv und nachhaltig in Koordination mit den Mitgliedsstaaten der Europäischen Union sowie mit der Europäischen Kommission dafür einsetzen, dass die vorstehend genannten, **schwerwiegenden Mängel im Text des Übereinkommens korrigiert** werden. Insbesondere soll der Fokus auf den Menschenrechtsgarantien – deren Stärkung und Anwendbarkeit auf das gesamte Übereinkommen - liegen.
    3. Österreich soll sich auch proaktiv **gegen** eine mit dem Übereinkommen **drohende Proliferation von Spyware** einsetzen.
    4. Erst nach einer signifikanten Verbesserung des Vertragstextes unter Behebung der dargestellten Mängel soll Österreich eine **Neubewertung vornehmen, ob ein Beitritt zur Konvention erfolgen kann**. Dabei sollen insbesondere und vorrangig menschenrechtliche Überlegungen den Ausschlag geben.

11 Artikel 36 (2).