NEUE CYBERCRIME-REGELN

Russland: Menschenrechte sind ein „Fehltritt“

Fünf Jahre dauernde Verhandlungen kamen vergangene Woche zum Abschluss.(Bild: UN Photo Manuel Elias)

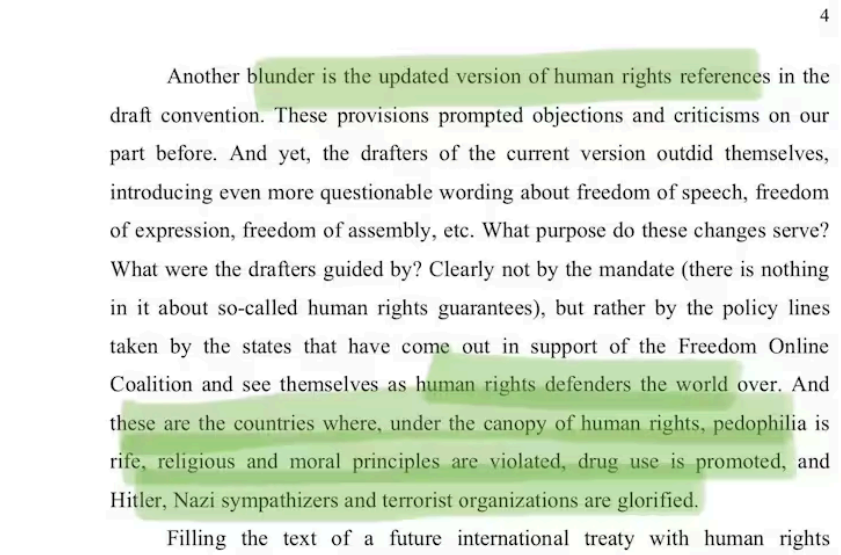
Auf Initiative Russlands beschlossen UN-Gremien vergangene Woche neue schärfere Regeln zu Bekämpfung von Cybercrime. Kritiker befürchten, dass diese Regeln nun zur Einschränkung von Meinungsfreiheit und Verfolgung von Oppositionellen eingesetzt werden. Und: Muss der Westen russische oder iranische Spionage unterstützen?

Russland hat sich kein Blatt vor den Mund genommen. Man brauche schärfere Überwachungsgesetze, denn „unter dem Deckmantel der Menschenrechte“ würden Pädophilie, Drogenhandel und Hitlerverehrung geschützt. Das zuständige UN-Gremium hat diesen Antrag vergangenen Freitag für viel Beobachter überraschend durchgewunken. Liest jetzt Putin auf Ihrem Smartphone mit?

Der Entscheidung waren jahrelange Diskussionen vorangegangen. Russland hatte die Diskussion 2019 initiiert. Seither laufen digitale Bürgerrechtsorganisationen gegen die Pläne Sturm. NGOs gaben in seltener Einigkeit mit Big-Tech-Unternehmen negative Stellungnahmen ab und zuletzt zeigte sich sogar der UN-Menschenrechtskommissar besorgt über die Pläne des UN-Cybercrime-Komitees.

„Fehltritt“ Menschenrechte

Was ruft Kritiker hier auf die Barrikaden? Einige nicht gerade für Menschenrechte bekannte UN-Mitgliedsstaaten wie Russland, Iran oder Venezuela hatten aktiv darauf hingearbeitet, Hinweise auf Menschenrechte aus der Konvention zu entfernen. Möglichkeiten zur Verfolgung von Cybercrime sollten nicht durch Menschenrechte behindert werden. Russland bezeichnete das Beharren auf Menschenrechten sogar als Fehltritt.



4

Another blunder is the updated version of human rights references in the draft convention. These provisions prompted objections and criticisms on our part before. And yet, the drafters of the current version outdid themselves, introducing even more questionable wording about freedom of speech, freedom of expression, freedom of assembly, etc. What purpose do these changes serve? What were the drafters guided by? Clearly not by the mandate (there is nothing in it about so-called human rights guarantees), but rather by the policy lines taken by the states that have come out in support of the Freedom Online Coalition and see themselves as human rights defenders the world over. And these are the countries where, under the canopy of human rights, pedophilia is rife, religious and moral principles are violated, drug use is promoted, and Hitler, Nazi sympathizers and terrorist organizations are glorified.

Filling the text of a future international treaty with human rights

Russland bezeichnet Menschenrechte als „Fehltritt“ und Tarnung für Pädophile, Drogenhändler und Nazis. (Bild: Screenshot)

Muss der Westen russische Spionage unterstützen?

Ein zweiter Kritikpunkt besteht im Anwendungsgebiet der Konvention. Wieder auf Betrieben Russlands sollte die Konvention auf zukünftige, jetzt noch nicht definierbare Cyber-Verbrechen angewendet werden können. Das öffne, so Kritiker, viel Spielraum für die Verfolgung politischer Kritik im Namen einer UN-Konvention. Westliche Staaten müssten dann zum Beispiel Russland oder den Iran bei der Spionage gegen politische Dissidenten unterstützen.

Vertreter der russischen Delegation bei den letzten Verhandlugen (Bild: Screenshot)

Erweiterte Haftung für Internetanbieter

Ein dritter großer Kritikpunkt betrifft die Ausdehnung der Haftung von Inhalteanbietern. Ginge es nach Russland, dann wären nicht nur Medien, die Inhalte veröffentlichen, haftbar. Es könnten auch Betreiber von Internetcafés zur Verantwortung gezogen werden, wenn über deren Infrastruktur Cyberverbrechen begangen werden.

Tanja Fachathaler begleitete die Verhandlungen für die NGO Access Now. „Die Entscheidung, diese Konvention anzunehmen, ist schwer nachvollziehbar.“ Es lagen viele Bedenken auf dem Tisch, viele Staaten haben sich Kritikern angeschlossen. Dennoch gab es keine Mehrheit für Änderungen an der zuletzt diskutierten Version.

„Großer Fehler“

Der wesentliche Grund für Beobachterin Fachathaler: „Einige Staaten wollten ein Zeichen setzen, dass man auch heute noch mit Russland verhandeln kann.“ Nachsatz: „Ich halte das für einen großen Fehler.“ Denn Russland habe nun gelernt, wie sich in UN Gremien Mehrheiten gegen den Westen finden lassen. Und weitere relevante Konventionen zur Cybersicherheit oder zu Künstlicher Intelligenz stünden bereits im Raum.

Der Weg zum UN-Recht

Die Konvention wurde von einem sogenannten Adhoc-Kommitee beschlossen. Bis daraus geltendes Recht wird, fehlen noch einige Schritte.

Die UN Generalversammlung muss der Konvention zustimmen. Nächster Termin dafür ist im Herbst.

Eine Anzahl von Mitgliedsstaaten müssen die Konvention ratifizieren, also in nationales Recht übersetzen. Diese Zahl ist

von Mal zu Mal verschieden, in diesem Fall müssen 40 Länder
diesen Beschluss fassen.
Erst danach ist die Konvention geltendes Recht.

Österreich hat bereits angekündigt, die Konvention in nationales Recht umsetzen zu wollen. „Wir haben uns erfolgreich dafür eingesetzt, dass keine sehr vagen Strafbestimmungen aufgenommen wurden, die zu Einschränkung der Meinungsfreiheit durch autoritäre Länder führen könnten“, sagt eine Sprecherin des Außenministeriums.

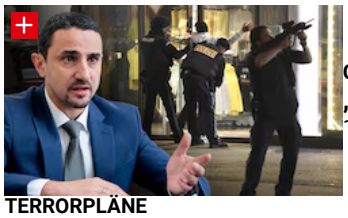
Verbesserungsbedarf
Das ist möglicherweise nicht für alle so eindeutig. Mit der Konvention wurden zugleich erklärende Anmerkungen veröffentlicht. Diese weisen darauf hin, dass die Konvention wenig Hinweise auf die Einhaltung von Menschenrechten enthält, weil diese ohnehin einzuhalten wären. Die Notizen weisen ebenso darauf hin, dass die neue Cybercrime-Konvention nicht zur Verfolgung „politischer oder moralischer“ Vergehen missbraucht werden möge.

„Es sind auch bereits weitere Zusätze abgekündigt. Auch ein Hinweis, dass das Ergebnis doch nicht für alle passt, die jetzt aus diplomatischen Gründen zugestimmt haben“, meint Expertin Fachathaler.

Was bedeutet die Cybercrime-Konvention für Messenger-Überwachung?
In Österreich wird nach den jüngst vereitelten Anschlagsplänen auf die Taylor-Swift-Konzerte viel über neue digitale Überwachungsregeln debattiert. Ganz oben auf der Wunschliste: die Überwachung von Messengerdiensten.

Innenminister Gerhard Karner (ÖVP) hatte sich zuletzt wieder neue Überwachungsbefugnisse gewünscht. Alle anderen Parteien stehen dem ablehnend gegenüber. Eine unter dem damaligen Innenminister Herbert Kickl (FPÖ) verabschiedete Regelung zur Messengerüberwachung war 2019 vom Verfassungsgerichtshof gekippt worden.

Lesen Sie auch:



GEHEIMDIENST-CHEF
„Attentat verhindert und stehen trotzdem im Fokus“
14.08.2024

TERRORPLÄNE
ÖVP beharrt trotz Abfuhr auf Messenger-Überwachung
14.08.2024

NACH ALARM IN WIEN
Terrorexperte: „Wir können so nicht weitermachen!“
09.08.2024

Zu effizienten Messengerüberwachung werden in der Regel staatliche Überwachungstools, auch Staatstrojaner genannt, auf Smartphones und Laptops installiert. Diese lesen jede Kommunikation mit und erlauben auch andere Eingriffe. Das Problem: Dazu werden Sicherheitslücken ausgenützt, die nicht nur Behörden, sondern auch Kriminellen offenstehen.

Messengerüberwachung gegen Politiker und Journalisten
Die Softwarelösungen werden von vielen Seiten kritisch betrachtet, über ihren konkreten Einsatz ist öffentlich wenig bekannt. Ein Bericht des Europarats zeichnet nach, in welchen europäischen Ländern Spuren staatlicher Messengerüberwachung festgestellt wurden. Offenbar setzen praktisch alle europäischen Länder Staatstrojaner ein. Die in dem Bericht aufgedeckten Fälle erzählen allerdings mehr von überwachten Politikern und Journalisten als von aufgedeckten Verbrechensplänen.

Auch auf den Smartphones von Emmanuel Macron und anderen französischen Regierungsmitgliedern soll Spionagesoftware gefunden worden sein. Vermuteter Auftraggeber in diesem Fall ist Marokko.

WER STAATSTROJANER VERWENDET

Eine Untersuchung des Europarats zur Verbreitung von Überwachungssoftware in europäischen Staaten.

ja keine Daten nein

Grafik: Stand Ende 2023 • **Krone** KREATIV | Quelle: Europarat

„Das ist staatliches Hacking“, meint Tanja Fachathaler von Access Now. „Das ist immer mit Risiken verbunden.“ Es gebe keine Möglichkeit, sicherzustellen, dass diese Tools und Lücken nur von den richtigen Stellen verwendet werden. Und: „Österreich ist ja ein schönes Beispiel dafür, dass es auch ohne Messengerüberwachung und Staatstrojaner geht.“

Kein Rückenwind für Karner

Rückendeckung für Karners Wünsche gibt es mit der neuen Cybercrime-Konvention nicht. Denn diese richtet sich, stellt auch das Außenministerium fest, an Diensteanbieter. Messengerüberwachung müsse allerdings beim Nutzer und dessen Endgeräten ansetzen. Dazu regelt die neue Konvention noch nichts.

Michael Hafner