2001/01 Ausland

https://shop.jungle.world/artikel/2001/01/fahrenheit-2001

Europäische Konvention gegen »Cyberkriminalität«

Fahrenheit 2001

Von **lucien maigret**

Mit einer Konvention gegen so genannte Cyberkriminalität will der Europarat dem unkontrollierten Treiben im Internet ein Ende bereiten.

Luis, ein Internet-Nutzer aus Portugal, sucht im Netz für seinen kleinen Sohn nach Kinderwäsche aus zweiter Hand. Als er in einer Suchmaschine »Baby + Panties« eingibt, gerät er auf eine Seite, die zunächst recht geheimnisvoll aussieht. Er meint Kleinkinder zu erkennen und klickt eines der winzigen Bildchen an. Als sich das Bild vor ihm aufbaut, schließt er entsetzt seinen Browser: Er ist auf einer Seite gelandet, die Kinderpornografie zeigt.

Luis ist über den Schrecken kaum hinweg, als die Polizei an seiner Haustür läutet. Die Beamten beschlagnahmen seinen Computer, Luis wird nach der Aufnahme seiner Personalien zunächst wieder auf freien Fuß gesetzt.

Was wie eine Szene aus dem unveröffentlichten zweiten Band von »Fahrenheit 451« wirkt, könnte bald schon Wirklichkeit sein, wenn eine Konvention des Europarats zur so genannten Cyberkriminalität umgesetzt wird. Etwa so: Luis ist auf einem in Dänemark beheimateten Server gelandet, der Pädofilen eindeutige Angebote macht. Der Betreiber, ein in Kanada lebender Österreicher, ist in beiden Ländern den Behörden bekannt, lebt aber auf freiem Fuß, weil die österreichische und die kanadische Internetpolizei hoffen, über ihn einen Pädophilenring aufzudecken.

Weil einige der dargestellten Kinder und Jugendlichen offenbar aus Osteuropa stammen, liegt außerdem ein Rechtshilfe-Ersuchen aus der Ukraine vor, zunächst die persönlichen Daten eines jeden Besuchers der Website zu übermitteln. Bei einigen verdächtigen Besuchern in Norwegen, Deutschland und Italien hat die Cyberpolizei in Kiew auch schon per Eilbefehl den Computer beschlagnahmen lassen. »Handeln in Echtzeit«, heißt das im Jargon der Sicherheitsfachleute.

In den USA ist Luis bereits gespeichert, weil eine diskrete Funktion in einem Programm eines großen Softwareherstellers ihn als jemanden meldete, der wahrscheinlich eine illegale Kopie dieser Software benutzt. Und auch in der Datenbank der britischen Webpolizei ist Luis vertreten. Dort wurde er automatisch eingetragen, als er als Mitglied einer lokalen Antifa-Gruppe verschiedene geschichtsrevisionistische Websites absurfte. Also geht eine Kopie seiner Festplatte zu Prüfzwecken auch über den Kanal.

Die Grundlage für solche länderübergreifenden Datenpolizei-Aktionen soll nach ihrer Ratifizierung noch in der ersten Jahreshälfte 2001 die Convention on Cybercrime bilden, die zur Zeit von zwei Expertengruppen des Europarates erarbeitet wird. Das Papier liegt mittlerweile in der vierundzwanzigsten Entwurfsversion vor, genauer gesagt: in deren zweiter Überarbeitung. Der Vermerk »Declassified PC-CY« verrät, dass es eine Version gibt, die der Geheimhaltung unterliegt und wohl noch weiter gehende Angriffe auf die Privatsphäre enthält. »Polizeibefugnisse werden ausgeweitet«, fasst die grüne Europa-Abgeordnete Ilka Schröder das Papier zusammen, »Datenschutz eingeschränkt und Provider zu Kollaborateuren des Überwachungsstaates gemacht.«

Die Konvention trägt die Handschrift derjenigen Vertreter der Inneren Sicherheit, die das Heil der Menschheit vor allem in immer mehr staatlicher und zunehmend auch transnationaler Kontrolle sehen. Diese Ideologie hat unter den vierzig Mitgliedsstaaten des Europarats ihre vehementesten Fürsprecher in den Regierungen so unterschiedlicher Staaten wie der USA, Großbritanniens, Schwedens und Russlands gefunden.

In Putins Reich werden Internetprovider gezwungen, eine Software in ihre Server einzubauen, die alle relevanten Verkehrsdaten ständig an die Zentrale des Geheimdienstes FSB weitermeldet. Die USA verschaffen sich mithilfe des unter ihrer Regie stehenden weltumspannenden Abhör-Systems Echelon sowieso schon Zugriff auf einen Großteil der elektronischen Kommunikation und haben vor allem ein Interesse daran, die Verbreitung von Kryptografie zu unterbinden. Darin werden sie vom Echelon-Partner Großbritannien unterstützt. Das Geburtsland der Bürgerrechte ist längst zum europäischen Spitzenreiter auf fast allen Feldern der Überwachungstechnologie geworden und pflegt eine unter anderem den Bereich der Internetkriminalität umfassende Sicherheitspartnerschaft mit Schweden.

So ist es kein Wunder, dass die Verschlüsselung von Datenverkehr mithilfe mächtiger Algorithmen wie PGP in dem 21seitigen Papier keinerlei Erwähnung findet. Schließlich ist der Inhalt einer mit PGP verschlüsselten Mail nach bisheriger Kenntnis selbst für den US-Geheimdienst NSA unbrauchbar.

Doch was dem normalen E-Mail-Nutzer und auch der Industrie Vertraulichkeit verschafft, ist selbstverständlich auch jedem nützlich, der das Internet für illegale Zwecke gebraucht. Deswegen heißt es in der Konvention, dass »jede Person, die Kenntnis hat von den Funktionen eines Computersystems oder von Maßnahmen, die getroffen wurden, um die darin enthaltenen Daten zu schützen, alle nötigen Informationen (...) preisgeben muss, um die Maßnahmen zu ermöglichen, die in den Paragrafen 1 und 2 behandelt werden«. Im Klartext: Wer seine Daten vor fremdem Zugriff schützen will, muss seine Passwörter und Kryptographieschlüssel preisgeben, wenn ihn die Cyberpolizei dazu auffordert.

In seltener Eintracht befürchten Industrievertreter und Datenschützer, dass in der klassifizierten Version der Konvention auch die Aufforderung an Hersteller von Kryptografie-Software enthalten sein könnte, künftig einen Nachschlüssel bei Abhör-Behörden zu hinterlegen. Eine solche eingebaute Schwachstelle käme nicht nur Geheimdiensten zupass, sondern auch Crackern, die sich, sobald sie die Sicherheitslücke entdeckt hätten, den Zugriff auf den vertraulichsten Teil des Datenverkehrs im Internet sichern könnten.

Akribisch listet die Konvention vier Arten von Verstößen auf, bei denen die Unterzeichnerstaaten sich verpflichten müssen, neue Strafrechtsklauseln einzuführen. Das reicht von der Zerstörung

von Computeranlagen über Betrug mithilfe von Computern bis zur Kinderpornografie, die immer dann herangezogen wird, wenn es die besondere Verwerflichkeit des Treibens im virtuellen Raum zu geißeln gilt: alles Straftaten, die auch bisher schon straf- wie zivilrechtlich zu ahnden waren. Warum nun Sondergesetze nötig sein sollen, um zu betonen, dass diese Delikte auch strafbar sind, wenn sie unter Benutzung eines Computers begangen werden, das erklärt die Konvention nicht.

Neu eingeführt werden in der Konvention allein »Vergehen gegen das Urheber- und verwandte Rechte«, also etwa das Herunterladen schwarz kopierter MP3-Files oder gecrackter Computerprogramme, das künftig auch als Straftat bewertet werden soll. Hier gilt wie für alle anderen in der Konvention erwähnten Delikte, dass Verstöße durch »effektive, angemessene und überzeugende Sanktionen geahndet werden« sollen, »welche Freiheitsentzug einschließen«.

Schlechte Aussichten für Luis: Mit dem Vorwurf der Kinderpornografie, des Ideologie-Vergehens und der Verletzung des Urheberrechts dürfte er kaum Aussicht auf eine milde Beurteilung haben. Ein typischer Cyberkrimineller eben.