

## Menschenrechtsgerichtshof schränkt Massenüberwachung der Geheimdienste ein

Der Europäische Menschenrechtsgerichtshof in Straßburg hat heute die britische geheimdienstliche Massenüberwachung als Verstoß gegen Menschenrechte gebrandmarkt. Mit dem Urteil der Großen Kammer kommen neue Anforderungen auf die Gesetzgeber aller europäischen Staaten zu, die solche Massenüberwachung betreiben. Auch der Schutz von Journalisten muss sich verbessern. Ein Kommentar.



Europäischer Gerichtshof für Menschenrechte (Straßburg) – Foto: CherryX, CC BY-SA 3.0

Der Europäische Menschenrechtsgerichtshof<sup>1</sup> in Straßburg hat heute<sup>2</sup> sein Urteil zur geheimdienstlichen Massenüberwachung bekanntgegeben. Da ich einer der Beschwerdeführer in diesem Fall war, kann ich nicht objektiv über die Entscheidung schreiben. Einen Kommentar aber muss ich loswerden.

Zunächst das heutige Urteil des Menschenrechtsgerichtshofs<sup>3</sup> in aller Kürze: Artikel 8 der Europäischen Menschenrechtskonvention (Menschenrecht auf Achtung des Privat- und Familienlebens) sowie Artikel 10 (Menschenrecht auf Freiheit der Meinungsäußerung) wurden beide durch die Massenüberwachung der britischen Geheimdienste verletzt. Die Richter legten wegen des Verstoßes gegen die Menschenrechte und um dem Missbrauch der Datenhalden entgegenzuwirken neue Anforderungen fest, die künftig für alle Staaten gelten, die der Konvention beigetreten sind.

Das massenhafte Abgreifen von Kommunikationsdaten geschieht innerhalb und teilweise auch außerhalb Großbritanniens an den Glasfaserkabeln. Dass dieser Zugriff durch den Geheimdienst GCHQ stattfindet und die Daten auch massenhaft ausgewertet werden, ist vom britischen Intelligence and Security Committee (ISC) eingeräumt worden und wird auch von der britischen Regierung nicht mehr bestritten. In den Snowden-Papieren befand sich der mittlerweile auch nicht mehr bestrittene Nachweis, dass vom GCHQ eine Operation namens *Tempora*<sup>4</sup>

durchgeführt wurde, bei der riesige Datenmengen abgeschmorpft und durchsucht wurden.

Die Massenüberwachung der Kommunikation an sich bleibt nach dem Urteil prinzipiell weiterhin möglich. Wie schon im ersten Urteil<sup>5</sup> wird sie eben nur beschränkt und eingehegt. Das kann die Beschwerdeführer zwar nur enttäuschen, aber nicht wirklich überraschen. Vielleicht war dafür die Zeit (noch) nicht reif.

### Die Begründung des Gerichts

Die erste der Beschwerden (unter dem Motto „Privacy not Prism“<sup>6</sup>) wurde bereits am 29. September 2013 eingereicht und später mit weiteren Verfahren zusammengelegt. Diese breit angelegten Beschwerden liefen also über sieben Jahre.

Es ging darin nicht nur um die breite Überwachung von Kommunikation an sich, sondern auch um die Kontrolle und Aufsicht dieser Praxis und um die Weitergabe von Daten an weitere Geheimdienste. Denn die teilweise nicht öffentlich verfügbaren Regeln, nach denen britische Geheimdienststellen Datensätze aus der Massenüberwachung an Partnergeheimdienste ohne eine richterliche Prüfung weitergeben, oder gar die fehlenden Vorschriften zur Kontrolle und zur Verwendung der Selektoren wa-

ren ebenfalls bemängelt worden. Hierzu finden sich in dem Urteil erhebliche neue Anforderungen, die künftig zu erfüllen sind.

Die Begründung in den Worten des Gerichts (in Absatz 425), warum die britische Massenüberwachung gegen den Artikel 8 der Menschenrechtskonvention verstößt:

*[...] the Court recalls that there is considerable potential for bulk interception to be abused in a manner adversely affecting the rights of individuals to respect for private life [...] Therefore, in a State governed by the rule of law [...] section 8(4) regime [...] did not contain sufficient „end-to-end“ safeguards to provide adequate and effective guarantees against arbitrariness and the risk of abuse. In particular, it has identified the following fundamental deficiencies in the regime: the absence of independent authorisation, the failure to include the categories of selectors in the application for a warrant, and the failure to subject selectors linked to an individual to prior internal authorisation [...] These weaknesses concerned not only the interception of the contents of communications but also the interception of related communications data [...].*

Der Schutz der Millionen Betroffenen gegen Missbrauch der Daten ist also nicht ausreichend, es existiert keine unabhängige Institution zur Autorisierung der Überwachung und es mangelt dabei auch an einer sinnvollen Kategorisierung bei den Selektoren. Das gilt sowohl für Inhaltsdaten als auch für die Metadaten der Kommunikation.

### Wichtige Verbesserungen eingefordert

Die erste Anforderung, die mit dem Urteil der Großen Kammer des Gerichtshofs nun allen Staaten der Konvention auferlegt wurde, betrifft die unabhängige Autorisierung der Massenüberwachung: Ein Richter oder eine andere unabhängige Stelle soll eine aussagekräftige und präzise Ermächtigung erteilen, die einen „Ende-zu-Ende“-Schutz („end-to-end“ safeguards) enthält. Der „Ende-zu-Ende“-Schutz bezieht sich auf die verschiedenen Stufen der Datenerfassung und -auswertung, die vom Gericht unterschieden werden. In allen diesen Stufen müssen also künftig Sicherungen gegen Missbrauch vorgesehen werden, beginnend von der ersten Datensammlung über den Einsatz der Selektoren bis zum Speichern in den Datenhalten.

Für Großbritannien wird diese Neuanforderung eine Gesetzesänderung nötig machen, da die Ermächtigung zur Massenüberwachung bisher der Innenminister erteilt. Da der Minister schon keine unabhängige Institution ist, wird der britische Gesetzgeber tätig werden müssen. Aber auch der neue „Ende-zu-Ende“-Schutz in allen Stufen wird allen Staaten, die Massenüberwachung betreiben, zu denken geben müssen – inklusive Deutschland. Das BND-Gesetz<sup>7</sup> muss also auch abgeklopft werden.

Neu ist zudem eine weitere Anforderung, die auch für die Kategorien der Selektoren eine unabhängige Autorisierung vorschreibt. Es kann in Zukunft keine Allgemeinplätze mehr geben, die faktisch der Art der Selektoren keine Grenzen setzen:

Einfach nur „nationale Sicherheit“ dranschreiben, wird künftig nicht mehr ausreichen. Die Selektoren sind deswegen von besonderer Bedeutung, weil sie letztlich darüber entscheiden, welche Inhalte aus den massenhaften Daten technisch ausgewählt und dann von Analysten wahrgenommen, gelesen oder angehört werden.

Beide Neuerungen bedeuten eine erhebliche Verbesserung für die Menschenrechte von mehr als 820 Millionen Europäern<sup>8</sup>, da solche höchstrichterlichen Anforderungen von allen 47 Staaten des Europarats umzusetzen sind.

Neben den beiden wichtigen Verbesserungen – aus Sicht der von Massenüberwachung Betroffenen – gegenüber dem ersten Urteil des Gerichts vom September 2018 betonen die Richter der Großen Kammer die Wichtigkeit des Schutzes von Journalisten. Auch hier muss künftig eine unabhängige Prüfung stattfinden, bevor auf journalistische Quellen zugegriffen werden darf. In seiner Pressemitteilung fasst das Gericht zusammen:

*The Court also found that the bulk interception regime had breached Article 10, as it had not contained sufficient protections for confidential journalistic material.*

Der Schutz von Journalisten muss also künftig besser berücksichtigt werden.

### Viele Jahre lang schlicht illegal

Die juristische Aufarbeitung der Veröffentlichungen aus den Snowden-Papieren kommt mit dem heutigen Urteil in gewisser Weise zu einem Ende. Zwar laufen weitere innerbritische IPT-Verfahren (Investigatory Powers Tribunal)<sup>9</sup>, aber keine höchstrichterlichen Verfahren in Europa mehr. In den Vereinigten Staaten wurde die Rechtswidrigkeit der geheimdienstlichen Massenüberwachung von US-Amerikanern im Jahr sieben nach Snowden<sup>10</sup> bereits gerichtlich festgestellt. In Europa haben wir durch den Menschenrechtsgerichtshof nun die unzweifelhafte Feststellung, dass die vormals geheimen britischen Operationen des massenhaften Abgriffs von Kommunikationsdaten nach menschenrechtlichen Standards viele Jahre lang schlicht illegal waren.

Das sollte man erstmal sacken lassen.

Aber ignorieren kann man leider auch nicht: Die Aufmerksamkeit für die Machenschaften der Geheimen ist über die Jahre merklich abgeebbt oder von anderen politischen Problemen überlagert. Dass die Geheimdienste der Five Eyes<sup>11</sup> und weiterer Staaten weiterhin massenweise Daten horten, auswerten und in ihnen schürfen, ist zwar vielen bekannt, aber oftmals kein drängendes Ärgernis mehr.

Das britische GCHQ und die US-amerikanische NSA und mit ihnen weitere Geheimdienste haben seit dem elften September 2001 eine Vielzahl an Überwachungsprogrammen gestartet, sind mit Hunderten Millionen aus dem Säckel der Steuerzahler in den jeweiligen Ländern ausgestattet worden und nutzen die technologische Revolution, die in die Hosentaschen, Büros und Wohnungen der Menschen einzog, auf ihre Weise. Snowden hat uns seltene Einblicke in diese Programme gewährt und

Verfahren wie das mit dem heutigen Urteil beendete erst möglich gemacht.

Aber auch im Rahmen der Schriftsätze und bei den beiden Anhörungen<sup>12</sup> des Gerichtshofs haben die Vertreter der britischen Regierung über die Durchführung der technisierten Massenüberwachung mit sehr wenigen Ausnahmen nur eingeräumt, was nicht mehr abzustreiten war. Wie genau die automatisierten Filterprozesse, die in nahezu Echtzeit über die riesigen Datenmassen laufen, in der Praxis funktionieren, liegt noch immer nur teilweise offen.

## Der Massenüberwachung weiterhin die Stirn bieten

Mehr als zweihundert Seiten Text umfasst die Entscheidung, denn rechtlich und technisch ist die Materie komplex. Auch wenn der Schriftsatz mit Sicherheit in den kommenden Tagen noch sehr detailliert analysiert wird, so steht eines fest: Die Massenüberwachung wird mit dem Urteil nicht beendet.

In der Parallelwelt der Geheimdienste, in der eigene Regeln gelten und in der trotz zahlreicher Skandale der politische Schutzschirm noch immer recht sicher war, wird das Urteil dennoch nicht nur Freude hervorrufen. Daran zu rütteln, dass die riesigen Behörden jeden Tag Millionen Datenhäppchen einsammeln und auswerten, dürfte nicht nur in Großbritannien und nicht nur unter Geheimdienstlern aufmerksam verfolgt werden. Denn gegen die Massenüberwachung als solche anzukämpfen, muss auch jene interessieren, die sonst noch an die Datentöpfe wollen: Das sind neben den Geheimen nämlich auch Strafverfolgungsbehörden in den Ländern, in denen die Menschenrechtskonvention gilt. Wenn das Gericht nun also schärfere Regeln vorschreibt, müssen sich alle daran messen lassen.

Es lohnt sich, der Massenüberwachung auch weiterhin die Stirn zu bieten – rechtlich, technisch und politisch. Ein paar mehr Leute vom Schlag eines Snowden könnten wir da übrigens ganz gut gebrauchen.

Quelle: <https://netzpolitik.org/2021/snowden-enthuellungen-menschenrechtsgerichtshof-schraenkt-masseneueberwachung-der-geheimdienste-ein/>



## Constanze Kurz

**Constanze Kurz**<sup>13</sup> ist promovierte Informatikerin, Autorin und Herausgeberin<sup>14</sup> von mehreren Büchern<sup>15</sup>, zuletzt zum *Cyberwar*<sup>16</sup>. Ihre Kolumne *Aus dem Maschinenraum*<sup>17</sup> erschien von 2010 bis 2019 im Feuilleton der FAZ. Sie ist Aktivistin<sup>18</sup> und ehrenamtlich Sprecherin<sup>19</sup> des *Chaos Computer Clubs*. Sie forschte an der Humboldt-Universität zu Berlin am Lehrstuhl „Informatik in Bildung und Gesellschaft“ und war Sachverständige der Enquête-Kommission *Internet und digitale Gesellschaft* des Bundestags. Sie erhielt den *Werner-Holtfort-Preis*<sup>20</sup> für bürger- und menschenrechtliches Engagement<sup>21</sup>, den *Toleranz-Preis*<sup>22</sup> für Zivilcourage und die *Theodor-Heuss-Medaille* für vorbildliches demokratisches<sup>23</sup> Verhalten. Kontakt: [constanze\(at\)netzpolitik.org](mailto:constanze(at)netzpolitik.org) (PGP<sup>24</sup>).

## Anmerkungen

- 1 [https://www.echr.coe.int/Documents/Court\\_in\\_brief\\_ENG.pdf](https://www.echr.coe.int/Documents/Court_in_brief_ENG.pdf)
- 2 *Der Beitrag wurde am 25. Mai 2021 veröffentlicht (d. Red.).*
- 3 [https://hudoc.echr.coe.int/eng#%7B%22documentcollectionid%22:%22GRANDCHAMBER%22,%22CHAMBER%22,%22itemid%22:\[%22001-210077%22\]%7D](https://hudoc.echr.coe.int/eng#%7B%22documentcollectionid%22:%22GRANDCHAMBER%22,%22CHAMBER%22,%22itemid%22:[%22001-210077%22]%7D)
- 4 <https://netzpolitik.org/2013/tempora-neue-snowden-dokumente-nennen-weitere-von-grossbritannien-angepfunden-glasfaser-kabel-auch-deutsche/>
- 5 <https://netzpolitik.org/2018/nach-dem-urteil-die-europaeische-menschenrechtskonvention-auf-den-stand-der-digitalen-revolution-bringen/>
- 6 <https://netzpolitik.org/2019/wieder-vor-gericht-geheimdienstliche-masseneueberwachung-und-das-menschenrecht-auf-privatheit/>
- 7 <https://netzpolitik.org/2020/zugestaendnisse-die-keine-sind/>
- 8 <https://de.wikipedia.org/wiki/Europarat>
- 9 <https://www.ipt-uk.com/content.asp?id=11?id=11>
- 10 <https://www.reuters.com/article/us-usa-nsa-spying/u-s-court-mass-surveillance-program-exposed-by-snowden-was-illegal-idUSKBN25T3CK>
- 11 [https://de.wikipedia.org/wiki/Globale\\_Überwachungs-\\_und\\_Spionageaffäre#Five\\_Eyes\\_\(UKUSA\)](https://de.wikipedia.org/wiki/Globale_Überwachungs-_und_Spionageaffäre#Five_Eyes_(UKUSA))
- 12 <https://netzpolitik.org/2019/masseneueberwachung-der-kommunikation-anhoerung-beim-menschenrechtsgerichtshof/>
- 13 [https://de.wikipedia.org/wiki/Constanze\\_Kurz](https://de.wikipedia.org/wiki/Constanze_Kurz)
- 14 <https://nowyouknow.eu/>
- 15 <http://gewissensbits.gi.de/constanze-kurz/>
- 16 <https://www.randomhouse.de/Buch/Cyberwar-Die-Gefahr-aus-dem-Netz/Constanze-Kurz/C.-Bertelsmann/e537921.rhd>
- 17 <http://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/>
- 18 <https://www.privacynotprism.org.uk/>
- 19 <https://www.youtube.com/watch?v=hj3gAsqrB18>
- 20 [https://de.wikipedia.org/wiki/Werner\\_Holtfort#Holtfort-Stiftung](https://de.wikipedia.org/wiki/Werner_Holtfort#Holtfort-Stiftung)
- 21 <https://media.ccc.de/search?q=Constanze+Kurz>
- 22 <http://www.ev-akademie-tutzing.de/toleranz-preis-fuer-christian-wulff-und-constanze-kurz/>
- 23 <https://www.jungundnaiv.de/2020/05/03/constanze-kurz-ueber-die-corona-app-folge-460/>
- 24 <https://pgp.mit.edu/pks/lookup?op=get&search=0x4A13B8EE269F8A45>

