Donnerstag, 23. Juli 2026, 17:00 Uhr
~10 Minuten Lesezeit

Die Überwachungsparanoia

Der beschlossene Angriff auf Datenschutz und Privatsphäre schürt die Angst vor einem aufziehenden Überwachungsstaat — dabei ist dieser längst Realität. Teil 1 von 2.

von Simone Hörrlein
Bild: Collage mit Foto von Shutterstock.com (DacologyPhoto, FOTOGRIN)

Die Aufregung ist groß: Die jüngst von der Europäischen Union (EU) im dritten Anlauf verabschiedete Chat-Kontrolle erhitzt die Gemüter ebenso wie der am 22. April 2026 verabschiedete ***Gesetzesentwurf*** *(https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/2025_IP_Sp der Internetanbieter verpflichtet, IP-Adressen und die zugehörigen Port-Nummern für drei Monate vorsorglich zu speichern. Dabei ist die Überwachung und langfristige Speicherung privater Kommunikation im Internet schon seit vielen Jahren traurige Realität. Was gerade in der EU und in Deutschland ganz offiziell geschieht, ist nichts anderes als die schrittweise Legalisierung der Massenüberwachung, welche der „Sicherheitsapparat" schon seit Jahrzehnten illegal betreibt. Die totale Überwachung kommt nicht mit der Chat-Kontrolle und anderen aktuell aufflackernden Überwachungsmaßnahmen und*

sie dient auch nicht primär dem Schutz von Kindern, Jugendlichen und anderen vulnerablen Gruppen. Ginge es um Pädophile und andere Perverse, dann würde man ganz andere Techniken einsetzen und auch die Epstein-Clique rigoros ausräuchern. Die Tatsache, dass das nicht getan wird, zeigt ganz deutlich, dass es um etwas anderes geht — nämlich darum, die totale Überwachung unter dem Vorwand von Schutz und Sicherheit Schritt für Schritt mehrheitsfähig zu machen. Es geht um den Übergang von einer „freundlichen Diktatur", auch Demokratie genannt, in eine weit weniger freundliche Technokratie, in der die totale Kontrolle des Einzelnen durch künstliche Intelligenz zur „Neuen Normalität" werden soll. Wer das nicht versteht, lebt in einer Traumwelt.

Datenschutz — nur noch Orwell'sche Verdrehung

Die Demokratiesimulation hat ausgedient und mit ihr auch der sogenannte Datenschutz. Zwar findet man die Definition des Datenschutzes noch immer auf der Website (https://www.bfdi.bund.de/DE/Buerger/Inhalte/Allgemein/Datenschutz/GrundlagenDatenschutzrecht.html) „des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit", doch was dort geschrieben steht, ist nicht viel mehr als hohle Phrasen. Vor dem Hintergrund der seit Jahrzehnten erfolgenden Massenüberwachung sind die dort erwähnten Dokumente zum Datenschutz blanker Hohn:

EU-Grundrechtecharta: Personenbezogene Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit der Einwilligung des Betroffenen oder auf gesetzlichen Grundlagen verarbeitet werden. Nach Artikel 8 der Grundrechtecharta hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

Grundgesetz-Bezug: Auf nationaler Ebene fußt der Datenschutz auf dem durch das Grundgesetz geschützten Recht auf informationelle Selbstbestimmung. Das Recht auf informationelle Selbstbestimmung wird aus dem allgemeinen Persönlichkeitsrecht und der Menschenwürde hergeleitet.

Datenschutzgrundverordnung: Zentraler Grundsatz der DSGVO und des gesamten Datenschutzrechts ist das sogenannte Verbotsprinzip. Dies bedeutet, dass die Verarbeitung personenbezogener Daten grundsätzlich verboten und ausnahmsweise nur dann gestattet ist, wenn die Voraussetzungen

einer der Erlaubnisnormen der DSGVO greifen (Art. 6 Abs. 1 DSGVO).

Nichts als schöne Worte. Worte, die vorspiegeln, dass ausschließlich das Individuum ein Recht an seinen Daten besitzt, was mitnichten der Fall ist.

> ***Denn für die Zukunft gilt: Sie können zwar die Freigabe Ihrer Daten verweigern, doch dann wird Ihnen der Zugang zu vielen Dingen einfach verwehrt bleiben.***

Die wohlklingenden Ausführungen zum Datenschutz sind in Wahrheit nur Schall und Rauch. Denn in der Realität wird alles, was wir online tun, abgefangen, analysiert und gegebenenfalls jahrelang gespeichert, und das nicht erst seit gestern. Der Rechtsstaat, dessen Aufgabe es ist, die gesetzlich verbrieften Rechte der Bürger zu schützen, versagt hier nicht nur jämmerlich, er ist aktiver Teil dieser Rechtsverstöße. Ein derartiges Staatsversagen sollte Konsequenzen nach sich ziehen. Tut es aber nicht, weil auch der Rechtsstaat nichts anderes als eine Fata Morgana ist, ein Vehikel, das dort versagt, wo es eigentlich tätig werden müsste, und dort tätig wird, wo es sich herauszuhalten hat.

Schon Edward Snowden warnte uns vor diesem Konstrukt, er nannte es eine „supranationale Organisation, die nicht den Gesetzen ihrer eigenen Länder unterliegt". Er meinte damit die Geheimdienste der beteiligten Staaten, welche de facto über dem Gesetz stehen. Die nachfolgenden Fakten wurden zu einem großen Teil von Snowden aufgedeckt. Die Aufregung damals war groß, dennoch hat sich an der Praxis bis heute nichts geändert. Die Empörung verschwand nach und nach, die illegale Überwachung ging nahtlos weiter. Schuld daran sind auch wir.

Die umfassende Überwachung im Netz, die tagtäglich stattfindet, betrifft leider nicht nur Terroristen, Kriminelle und „echte" Staatsfeinde, sie betrifft uns alle. Und jeder, der seine Privatsphäre schützen möchte, gilt bereits als verdächtig. Es geht um eine Massenüberwachung, die sowohl Metadaten — wer kommuniziert mit wem, wann, wo — als auch Inhalte von E-Mails, E-Mail-Anhängen, Telefonaten, Chat-Nachrichten, ja sogar Browserverläufe abfängt, analysiert und gegebenenfalls speichert. Mithilfe von Systemen wie PRISM, das heißt Zugriff auf Server von Google, Apple, Microsoft und so weiter, TEMPORA, also das Anzapfen von Unterseekabeln, und die globale Satellitenüberwachung, um nur einige der Überwachungsinstrumente zu nennen, wird der gesamte Internetverkehr in jeder Sekunde bis ins Detail überwacht. Später mehr dazu, wie das in etwa funktioniert.

Überwachung früher und heute

Die Überwachung von Verdächtigen ist nicht neu, neu ist aber, dass heute jeder als verdächtig gilt. Initiatoren der totalen Überwachung waren im Rahmen des Zweiten Weltkrieges die angelsächsischen Länder USA, Vereinigtes Königreich (UK), Kanada, Australien und Neuseeland, auch unter der Bezeichnung **„Five Eyes" (5 Eyes)** (https://en.wikipedia.org/wiki/UKUSA_Agreement) bekannt. Das Konstrukt, das eigentlich zur Bekämpfung der Sowjetunion im Kalten Krieg gedacht war, hat seine Ziele heute grundlegend gewandelt. Auch wenn primär mit Terrorabwehr und Spionagebekämpfung argumentiert wird, so werden zunehmend auch Dissidenten, Journalisten und Whistleblower, wobei Julien Assange das wohl gravierendste Beispiel darstellt, ins Visier genommen.

> ***Jeder der das System kritisiert, der seine Ungerechtigkeiten oder sein Versagen anprangert, wird ganz einfach zum Staatsfeind erklärt und gerät ins Visier der Geheimdienste. Zuerst bist du nur ein Verschwörungstheoretiker, dann ein Extremist und schließlich mutierst du zum gefährlichen Terroristen.***

Und Terroristen haben keine Rechte.

Die 5/9/14 Eyes

Was als „5 Eyes" begann, wurde im Laufe der Zeit zu den **„5/9/14 Eyes"** (https://en.wikipedia.org/wiki/UKUSA_Agreement), worunter man internationale Geheimdienstallianzen versteht, die sich den Austausch von Signal Intelligence (SIGINT) — also abgefangenen Kommunikationsdaten — auf die Fahnen geschrieben haben. Diese Struktur ermöglicht es, nationale Datenschutzgesetze auszuhebeln, ohne rechtliche Konsequenzen fürchten zu müssen. Die Zusammenarbeit der **„5 Eyes"** (https://stateofsurveillance.org/articles/surveillance/five-eyes-alliance-mutual-surveillance-explained/) basiert auf dem geheimen UKUSA-Abkommen von 1946. Dieses Abkommen, damals noch **BRUSA** (https://en.wikipedia.org/wiki/1943_BRUSA_Agreement), war jahrzehntelang streng geheim. Es wurde erst im Juni 2010 offiziell von der US-amerikanischen **NSA** (https://web.archive.org/web/20130805231226/http://www.nsa.gov/public_info/declass/ukusa.shtml) und dem britischen Nationalarchiv freigegeben.

Die Angelsachsen teilen seither alle gesammelten Daten in Echtzeit. Dazu wurde ein globales Netzwerk aus gemeinsamen Einrichtungen und nationalen Hauptquartieren etabliert, die eng miteinander verzahnt sind. Die Hauptquartiere befinden sich bei der National Security Agency (NSA) in Fort Meade, USA, bei den Government Communications Headquarters (GCHQ) in Cheltenham, UK, beim Communications Security Establishment (CSE) in Ottawa, Kanada, dem Australian Signals Directorate (ASD) in Canberra, Australien,

und dem Government Communications Security Bureau (GCSB) in Wellington, Neuseeland.

Ein gemeinsamer Standort ist **Pine Gap** (https://en.wikipedia.org/wiki/Pine_Gap) in Australien, nahe Alice Springs, wo die USA und Australien eine gemeinsame Satellitenüberwachung unterhalten. Der *Guardian* berichtete 2025 in einem **Artikel** (https://www.theguardian.com/australia-news/2025/oct/27/pine-gap-protests-spy-base-gaza-war-australia-complicity) darüber, dass Australien über Pine Gap am Krieg in Gaza beteiligt sei. Und in **Menwith Hill (UK)** (https://en.wikipedia.org/wiki/RAF_Menwith_Hill) arbeiten NSA und GCHQ Hand in Hand. Die geografische Lage der fünf Länder ermöglicht die Überwachung rund um die Uhr; wenn in den USA und Kanada Nacht ist, übernehmen die Partner in Australien oder Neuseeland die Beobachtung derselben Ziele.

Die „9 Eyes" sind eine Erweiterung der „5 Eyes" um die Länder Dänemark, Frankreich, Niederlande und Norwegen. Diese Länder pflegen zwar eine enge Zusammenarbeit mit den „5 Eyes" und es gibt auch feste Kooperationsstrukturen, allerdings fehlt ein formaler Vertrag wie das UKUSA-Abkommen. Die **„14 Eyes"** (https://worldpopulationreview.com/country-rankings/14-eyes-countries), die zusätzlich die Länder Deutschland, Belgien, Italien, Schweden und Spanien einschließen, sind auch unter der Bezeichnung **„SIGINT Seniors Europe"** (https://cyberinsider.com/5-eyes-9-eyes-14-eyes/) bekannt. Diese Länder dienen primär dem Austausch von Informationen auf europäischer Ebene und der technischen Unterstützung. Die Zusammenarbeit ist weniger „intim" als bei den „5 Eyes", umfasst aber dennoch den regelmäßigen Datenaustausch.

Nationale Sicherheit als Vorwand für Massenüberwachung

Primär geht es dieser Geheimdienstallianz um die Überwachung der eigenen Bevölkerung, welche ohne richterlichen Beschluss aufgrund von Gesetzen zum Datenschutz verboten ist. Die nationalen Spionageverbote werden durch einen Trick umgangen: Ein Geheimdienst, zum Beispiel britischer GCHQ, überwacht die Bürger eines Partnerlandes, beispielsweise USA, was für ihn legal ist, da es sich um „Ausländer" handelt. Diese Daten werden dann an den Partner, zum Beispiel NSA, weitergegeben. Da der Datenschutz in den USA nur das Sammeln, nicht aber das Empfangen von Daten verbietet, ist beispielsweise die NSA durch dieses Konstrukt rechtlich nicht angreifbar.

Das Ausspionieren jedes einzelnen Individuums und das Aushebeln des Datenschutzes, der in Wahrheit überhaupt nicht existiert, stützen sich auf drei Hauptargumente der Geheimdienste und

Regierungen:

1. Nationale Sicherheit und Terrorabwehr. Das Argument lautet, man müsse „die Nadel im Heuhaufen“ finden, wofür man erst den ganzen Heuhaufen, also alle Daten, durchsuchen müsse.
2. Man unterscheidet zwischen Inhalt einer Nachricht, also was Sie schreiben, und den Metadaten, wer, wann, wo. Metadaten, so die Argumentation, seien weniger schützenswert, obwohl sie Bewegungsprofile und soziale Netzwerke exakt abbilden.
3. Die Daten werden von Algorithmen lediglich gescannt, nur bei Verdachtsmomenten übernimmt ein Mensch die finale Analyse. Für den Einzelnen gilt: Solange Sie nicht „auffällig“ werden, sind Sie nur eine Nummer in der Datenbank.

Bestehende Gerichtsurteile werden von den beteiligten Organisationen einfach ignoriert. Kritiker und auch der Europäische Gerichtshof für Menschenrechte (EGMR) sehen in diesem Vorgehen einen unverhältnismäßigen Eingriff, der das Grundrecht auf Privatsphäre pauschal aushebelt. Schon in einem der ersten Grundsatzurteile des EGMR zur geheimen Überwachung in der Sache „Klass und Andere gegen Deutschland vom 6. September 1978“ (**Beschwerde Nr. 5029/71** (https://www.legal-tools.org/doc/f46bdd/)) stellte das Gericht fest:

„*Der Gerichtshof ist sich der Gefahr bewusst, dass ein solches Gesetz die Demokratie unter dem Vorwand ihrer Verteidigung untergräbt oder sogar zerstört.*“

Zudem argumentierte das Gericht, „dass die vertragschließenden Staaten im Namen des Kampfes gegen Spionage und Terrorismus nicht beliebige Maßnahmen ergreifen dürfen, die sie für angemessen halten“.

Das Problem ist eine schleichende Erosion der Privatsphäre unter dem Deckmantel von nationaler Sicherheit. In einem anderen Urteil vom 13. September 2018, Rechtssache „Big Brother Watch and Others v. the United Kingdom“ **(Beschwerde Nr. 58170/13 unter anderem** (https://epic.org/documents/big-brother-watch-v-uk-bureau-of-investigative-journalism-v-uk-10-human-rights-organizations-v-uk/)), warnte der EGMR erneut explizit:

„*Ein System geheimer Überwachung, das zum Schutz der nationalen Sicherheit eingerichtet wurde, kann die Demokratie unter dem Vorwand, sie zu verteidigen, untergraben oder sogar zerstören.*“

Dass solche Urteile einfach ignoriert werden können, zeigt eines: Diese Gerichte sind zahnlose Tiger, ihre Urteile sind obsolet. **Privacy International** (https://privacyinternational.org/learn/mass-surveillance) stellt fest, dass Massenüberwachung das Prinzip der Unschuldsvermutung aufhebt. In einer Demokratie gilt: Der Staat darf nur bei konkretem Verdacht eingreifen. Bei der

Massenüberwachung gilt jedoch: Jeder ist verdächtig, bis das Gegenteil bewiesen ist.

Massenüberwachung erstickt den Diskurs und kriminalisiert den Schutz der Privatsphäre

> ***Es ist bekannt, das alleine das Wissen darüber, „überwacht zu werden", zur Selbstzensur führt, der sogenannte „Chilling Effect". In Deutschland zeigt dieser Effekt bereits Wirkung, das bestätigen offizielle Umfragen.***

Menschen trauen sich nicht mehr, frei zu sprechen, zu recherchieren oder zu protestieren, aus Angst, falsch verstanden zu werden. Das erstickt nicht nur den demokratischen Diskurs im Keim. Es verhindert auch die Aufklärung von Korruption, Staatsversagen und illegalen staatlichen Übergriffen auf fälschlicherweise als verdächtig eingestufte Individuen. Eine **Umfrage** (https://www.welt.de/politik/deutschland/article68f11916cdf2d9fc0bea1883/umfrage-nur-46-prozent-der-deutschen-glauben-ihre-meinung-frei-aeussern-zu-koennen.html) des Institut für Demoskopie Allensbach kommt zu dem Ergebnis, dass nur noch 46 Prozent der Befragten der Ansicht sind, man könne seine politische Meinung frei äußern. Eine Bankrotterklärung für einen Rechtsstaat. Der Originalbericht steht **hier** (https://www.ifd-allensbach.de/fileadmin/kurzberichte_dokumentationen/FAZ_Oktober2025_Freiheit.pdf).

Dieses Umfrageergebnis wurde oft mit Verweis auf die Meinungsfreiheit, die durch das Grundgesetz garantiert sei, relativiert. Doch was die Befragten meinen, ist der oben beschriebene „Chilling-Effect". Das Wissen darüber, dass alles, was man im Netz sagt und tut, überwacht wird, führt dazu, lieber nichts mehr zu sagen oder zu schreiben. Man wird nicht buchstäblich mundtot gemacht, etwa durch ein Gesetz, noch nicht. Man wird mundtot gemacht durch den Druck des öffentlichen Raumes, die Totalkontrolle, die Vorverurteilung und Diffamierung durch die Medien, die Sanktionierung durch Politik und Staat, und neuerdings durch die Legalisierung von Überwachung, die sich langsam aber sicher durch alle Bereiche der Gesellschaft frisst. Damit wird ein gefährlicher Weg beschritten, der erneut in einem System enden könnte, für das hinterher niemand verantwortlich gewesen sein will.

Trotz aller Warnungen von Kritikern und Gerichtsurteilen hat sich an der Massenüberwachung im Internet bis heute nichts geändert, im Gegenteil, sie wird immer übergriffiger. Um ihre Machenschaften weiter zu betreiben, gehen Geheimdienste und Staat sogar so weit, Gesetze im Nachhinein zu ändern, um ihre illegale Praxis zu

legalisieren. Ein Beispiel ist der „**Investigatory Powers Act** (https://en.wikipedia.org/wiki/Investigatory_Powers_Act_2016)“ in Großbritannien, oft „Snooper's Charter“ genannt. Hinzu kommt, dass Geheimdienste und Regierungen Verschlüsselung, also bisher der einzige effektive Schutz vor dem illegalen Ausspionieren, offen bekämpfen.

Der Schutz der Privatsphäre, der das Recht eines jeden Bürgers ist, wird auf diese Weise sogar kriminalisiert. Dabei geht es nicht nur um Chats, es geht um die gesamte Kommunikation im Netz. Und während Politiker öffentlich fordern, „Hintertüren“ in die Verschlüsselung einzubauen, versuchen sie zu legalisieren, was Geheimdienste längst tun.

> ***Wer seine Privatsphäre aus Prinzip effektiv schützen will, wozu er das Recht hat, weil sich der Staat aus dem Privatleben der Bürger herauszuhalten hat, gilt als verdächtig oder handelt in einer Grauzone, während der Staat das Grundrecht auf Privatsphäre systematisch auszuhöhlen versucht.***

Das System ist krank, es leidet an einer schweren Schizophrenie. Während nach außen Freiheit, Menschenrechte und Demokratie gepredigt werden, agiert im Inneren eine Infrastruktur, die totale Kontrolle ermöglicht, kontinuierlich ausgebaut wird und nur auf den „guten Willen“ von Geheimdienstchefs und Politikern vertraut, ihre Macht nicht zu missbrauchen. Es ist ein System, das darauf setzt, dass die meisten Bürger sich anpassen und sich mit der Phrase „wer nichts zu verbergen hat, hat nichts zu befürchten“ sedieren lassen. Für Journalisten, die system- und gesellschaftskritisch arbeiten, ist es ein feindliches Umfeld, in dem Privatsphäre nicht mehr als Recht, sondern als Verdachtsmoment behandelt wird.

Simone Hörrlein ist Lebensmittelchemikerin und Wissenschaftsjournalistin. Nach ihrem Studium an der **TU München** war sie mehrere Jahre in der medizinischen Forschung tätig und arbeitete zuletzt in der Wissenschaftskommunikation des **Kompetenzzentrums für Ernährung**. Neben den Naturwissenschaften interessiert sie sich für Finanz- und Geopolitik. Aktuell lebt sie in Kanada.