Der neue Überwachungsstaat braucht keine Uniformen mehr, keine Zensoren, keine Stasi-Akten. Er braucht nur noch Algorithmen. Wer entscheidet, wann ein Text „radikal“ ist? Wer legt fest, wann Kritik an Regierungspolitik „systemfeindlich“ klingt? Solche Wertungen entstehen heute nicht mehr im Gerichtssaal, sondern im Code. Am Ende stehen nicht selten Hausdurchsuchungen, Beschlagnahmungen von Geräten oder Kontosperrungen. Der Einschüchterungseffekt ist enorm. Von **Günther Burbach**.

Dieser Beitrag ist auch als Audio-Podcast verfügbar.

https://www.nachdenkseiten.de/upload/podcast/251031_Die_neue_Angstmaschine_Wie_Staat_KI_und_Plattformen_Kritik_kriminalisieren_NDS.mp3

Podcast: Play in new window | Download

Die neue Macht der digitalen Denunziation

Inzwischen reichen ein getippter Satz, ein geteilter Link oder ein Video-Upload, damit staatliche Ermittlungen in Gang gesetzt werden. Was früher mühsam über Anzeigen, Prüfungen und öffentliche Debatten angestoßen wurde, läuft heute weitgehend automatisiert. Unsichtbare digitale Filter und algorithmische Warnsysteme entscheiden, was auffällt und was anschließend juristisch verfolgt wird. Am Ende stehen nicht selten Hausdurchsuchungen, Beschlagnahmungen von Geräten oder Kontosperrungen. Das Ergebnis ist immer dasselbe: Menschen, die nach eigener Darstellung nichts anderes wollten als informieren oder kritisieren, stehen plötzlich mit Ermittlungsakten und durchwühlten Schreibtischen da. Der Einschüchterungseffekt ist enorm.

In den vergangenen Wochen wurde etwa bekannt, dass der Medienwissenschaftler Norbert Bolz Ziel einer Hausdurchsuchung wurde. Nach Angaben von Medien erfolgte der Einsatz wegen des Verdachts auf Verwendung verfassungsfeindlicher Symbole, ein Vorwurf, der bereits durch seine bloße Existenz Rufschaden erzeugt, ganz gleich, ob er sich am Ende als haltbar erweist oder nicht. Solche Verfahren wirken längst über ihren juristischen Rahmen hinaus. Sie senden eine Botschaft: Kritik kann Konsequenzen haben, auch wenn sie rechtlich zulässig ist.

Ähnlich erging es in den letzten Jahren mehreren Medienschaffenden, die wegen angeblicher Verbreitung von Desinformation oder unliebsamer Positionen ins Visier der Behörden gerieten. In den Schlagzeilen genügt meist schon der Satz „Gegen XY wird ermittelt“. Die Unschuldsvermutung, einst ein Grundpfeiler des Rechtsstaats, verliert in

dieser neuen Medienlogik an Gewicht. Der Verdacht wird zur Nachricht und die Nachricht zur Verurteilung im öffentlichen Bewusstsein.

Die Erklärung für diese Entwicklung liegt nicht in einer plötzlichen Willkür einzelner Staatsanwälte. Sie liegt in einem System, das technische Datenanalyse, politische Prioritäten und juristische Abläufe miteinander verknüpft. In vielen Fällen beginnt der Vorgang nicht mit einer Anzeige, sondern mit einem digitalen Hinweis: einer Meldung aus einem Plattform-Algorithmus, einer Risikobewertung aus einer automatisierten Überwachung oder einer Anomalie in Text- und Kommunikationsmustern. Diese Systeme durchforsten Netzwerke, Beiträge und Metadaten nach „auffälligen“ Inhalten, eine Art Frühwarnsystem, das ständig nach Abweichungen vom digital definierten Normalzustand sucht. Wird eine Häufung bestimmter Begriffe, Quellen oder Vernetzungen erkannt, erzeugt das System einen sogenannten Alert, der bei zuständigen Stellen landet. Dort entscheidet dann ein Mensch, oft unter Zeitdruck, über das weitere Vorgehen. Die Entscheidung wirkt formal juristisch, beruht aber auf maschinell vorbereiteten Verdachtsmomenten.

Die neue Art von Strafverfolgung beginnt mit Datenanalyse

So entsteht eine neue Art von Strafverfolgung, die nicht mehr mit polizeilicher Recherche beginnt, sondern mit Datenanalyse. Der richterliche Beschluss wird in vielen Fällen nur noch zur Formsache. Was wie eine unabhängige Entscheidung aussieht, ist häufig das Endprodukt einer Kette, die längst vorher festgelegt wurde. Der Algorithmus definiert den Verdacht, die Behörde bestätigt ihn, das Gericht nickt ihn ab. Die Verhältnismäßigkeit wird zur juristischen Vokabel ohne praktische Bedeutung.

Die Folgen für die Betroffenen sind verheerend: Wohnungsdurchsuchungen, beschlagnahmte Computer, gesperrte Konten, monatelange Verfahren, selbst wenn am Ende kein strafbares Verhalten nachgewiesen wird. Die Botschaft dahinter ist unmissverständlich: Wer öffentlich kritisch auftritt, lebt gefährlich. Und genau das ist Teil des Problems. Der Staat selbst muss sich fragen lassen, ob er noch die Grenze zwischen legitimer Gefahrenabwehr und politisch motivierter Einschüchterung kennt.

Diese neue Realität ist kein Unfall. Sie ist das Resultat einer schleichenden Verschmelzung von staatlicher Macht, technischer Infrastruktur und privaten Zensurmechanismen. Plattformen wie *YouTube*, *Meta* oder *X* liefern die Daten, private Analysefirmen werten sie aus, und staatliche Institutionen greifen darauf zurück, wenn sie es brauchen. Der Kreislauf schließt sich dort, wo aus einem Datensatz eine Maßnahme wird, aus einer Maßnahme ein Präzedenzfall und aus einem Präzedenzfall ein neues Normal.

In diesem Artikel wollen wir zeigen, wie dieser Mechanismus funktioniert: Wer über welche Daten verfügt, wie Plattformen, Sicherheitsbehörden und Justiz miteinander verbunden sind, auf welcher Grundlage Entscheidungen getroffen werden und warum all das für den Rechtsstaat gefährlicher ist, als viele glauben. Denn der eigentliche Schaden entsteht nicht erst bei einer Verurteilung. Er entsteht dort, wo die Angst beginnt, überhaupt noch zu sprechen.

Wie unsere Daten kontrolliert und wie sie sortiert werden

Wer die Kontrolle über Daten hat, kontrolliert letztlich auch die Deutung der Realität. Diese einfache Wahrheit beschreibt den Kern des modernen Überwachungsstaats: Derjenige, der sieht, was andere sagen, schreiben und teilen, kann bestimmen, was sichtbar bleibt und was verschwindet. Heute ist diese Kontrolle auf mehrere Schultern verteilt: auf Plattformkonzerne, Cloud-Anbieter, Sicherheitsbehörden und private Datenanalysefirmen. Doch am Ende greifen ihre Systeme ineinander wie Zahnräder eines einzigen Apparats.

Die meisten digitalen Spuren, die ein Bürger in Deutschland hinterlässt, passieren mindestens drei Ebenen der Kontrolle: die Plattform, die Infrastruktur und die staatliche Schnittstelle. Plattformen wie *YouTube*, *Meta* oder *X* speichern und analysieren jede Aktivität, nicht nur sichtbare Beiträge, sondern auch Klickpfade, Scrollbewegungen, Zeitverläufe und Kontaktbeziehungen. Diese Daten liegen meist auf Servern von Amazon Web Services (AWS), Google Cloud oder Microsoft Azure. Ein Großteil dieser Server steht zwar physisch in Europa, doch die Unternehmen unterliegen US-Recht, was bedeutet: Auf Anforderung US-amerikanischer Behörden müssen sie Daten herausgeben, auch wenn sie aus Deutschland stammen.

Auf der zweiten Ebene befinden sich die staatlich beauftragten Cloud- und Sicherheitsdienstleister. In Deutschland ist das vor allem T-Systems, die im Auftrag von Bund und Ländern sogenannte „Sovereign Clouds“ betreiben, also angeblich besonders geschützte Datennetze für Behörden. Tatsächlich aber laufen auch dort viele Dienste über Kooperationen mit denselben US-Anbietern. Das Bundesinnenministerium nutzt beispielsweise Microsoft-Dienste in einer angepassten Variante, die offiziell „DSGVO-konform“ sein soll, in Wahrheit aber nur eine juristische Zwischenschicht darstellt.

Die dritte Ebene schließlich ist die der Datenanalyse und hier beginnt der politische Teil der Kontrolle. Systeme wie Palantir Gotham oder Foundry verknüpfen Datenquellen aus Polizei, Nachrichtendiensten und offenen Netzen. Das Projekt „Hessendata“, vom hessischen Innenministerium in Zusammenarbeit mit Palantir aufgebaut, ist ein Beispiel dafür, wie aus heterogenen Daten ein Gesamtbild entsteht. Offiziell soll die Software Kriminalitätsmuster

erkennen. In der Praxis aber lassen sich mit denselben Werkzeugen auch Kommunikationsnetzwerke auswerten, wer mit wem interagiert, welche Inhalte geteilt, welche Begriffe gehäuft verwendet werden.

Diese Technologien können in Echtzeit Bewegungs- und Meinungsmuster analysieren. Sie erkennen Trends, Themen, Einflusspunkte. Genau das macht sie so wertvoll für Sicherheitsbehörden, aber auch so gefährlich für die Meinungsfreiheit. Denn wer die Kommunikationsströme der Gesellschaft kartografieren kann, kann auch gezielt eingreifen: einzelne Kanäle drosseln, Accounts markieren, Narrative verstärken oder schwächen. Die Grenze zwischen Sicherheitspolitik und Informationslenkung wird damit unscharf.

Hinzu kommt ein kaum beachteter Akteur: die privaten Datenbroker. Sie sammeln, kaufen und verkaufen Daten aus nahezu allen Lebensbereichen, Einkaufsverhalten, Standortverläufe, Webseitenaufrufe, selbst Gesundheitsdaten. Diese Informationen fließen nicht direkt an den Staat, aber sie landen bei Firmen, die wiederum mit Behörden kooperieren. Damit entsteht eine parallele Informationsinfrastruktur, die staatliche Kontrolle nicht mehr braucht, weil sie längst ausgelagert ist.

Die Maschine liefert die Begründung gleich mit

Im juristischen Alltag bedeutet das: Wenn eine Staatsanwaltschaft einen Verdacht verfolgt, stehen bereits vorformulierte Datensätze bereit. Verbindungen zwischen Personen, Kommunikationshäufigkeit, Schlüsselwörter, sogar emotionale Tonalitäten in Texten, alles lässt sich automatisiert auswerten. So wird eine Ermittlungsakte nicht mehr von Hand aufgebaut, sondern algorithmisch erzeugt. Und genau hier kippt der Rechtsstaat: Wo früher ein Anfangsverdacht begründet werden musste, liefert heute die Maschine die Begründung gleich mit.

Dass solche Systeme in Deutschland im Einsatz sind, ist kein Geheimnis. In mehreren Bundesländern laufen Pilotprojekte zur KI-gestützten Strafverfolgung. Die Polizei Nordrhein-Westfalen experimentiert mit automatisierter „Gefährdungserkennung“, das BKA nutzt textanalytische Verfahren zur Einschätzung „digitaler Risikopotenziale“, und auf EU-Ebene wird eine gemeinsame Plattform zur Terrorismusbekämpfung vorbereitet, in der auch Inhalte aus sozialen Medien analysiert werden sollen. Der Begriff „Prävention“ dient dabei als Schutzschild für Überwachung.

Doch Prävention ist ein dehnbarer Begriff. Wer entscheidet, wann ein Text „radikal“ ist? Wer legt fest, wann Kritik an Regierungspolitik „systemfeindlich“ klingt? Solche Wertungen entstehen nicht mehr im Gerichtssaal, sondern im Code. Und dieser Code gehört nicht dem

Staat, sondern privaten Unternehmen, deren Modelle weder öffentlich noch kontrollierbar sind.

So verschiebt sich Macht leise, technisch, unsichtbar, weg von den demokratisch legitimierten Institutionen hin zu einem Netz aus Plattformen, Softwarekonzernen und Sicherheitsapparaten. Der Bürger sieht davon nichts. Er klickt, schreibt, teilt, löscht und ahnt nicht, dass seine Daten längst nicht mehr ihm gehören.

Diese Unsichtbarkeit ist die gefährlichste Form der Kontrolle. Sie schafft ein Klima der Selbstzensur, in dem Menschen beginnen, sich selbst zu beobachten, bevor es jemand anderes tut. Der neue Überwachungsstaat braucht keine Uniformen mehr, keine Zensoren, keine Stasi-Akten. Er braucht nur noch Algorithmen, die entscheiden, wessen Meinung sichtbar bleibt und wessen Haus durchsucht wird.

Der Schatten der Plattformen: Wie digitale Reputationssysteme arbeiten

Wer heute glaubt, Zensur sei nur ein staatliches Phänomen, hat das System der modernen Plattformökonomie nicht verstanden. Die Macht, Themen zu verschweigen, ist längst privatisiert. Sichtbarkeit ist zur Währung geworden und wer darüber entscheidet, was sichtbar bleibt, übt politische Macht aus, ohne gewählt zu sein.

Plattformen wie *YouTube*, *X* oder *Facebook* sind nicht bloß Kommunikationsräume. Sie sind algorithmische Filtermaschinen. Jede Äußerung wird dort zunächst technisch bewertet, bevor sie einem Publikum überhaupt gezeigt wird. Dabei geht es nicht mehr nur um Klickzahlen oder Reichweite, sondern um „Vertrauensmetriken“, interne Reputationswerte, die bestimmen, ob ein Beitrag hochgestuft, neutral behandelt oder in den digitalen Schatten geschickt wird. Der Begriff „Shadowban“ ist längst kein Mythos mehr. Millionen Nutzer erleben ihn täglich: Beiträge werden nicht gelöscht, aber unsichtbar gemacht, Videos erscheinen nicht in der Suche, Kommentare werden ausgeblendet, Followerzahlen stagnieren plötzlich ohne erkennbaren Grund.

Offiziell erklären die Konzerne, dies geschehe, um „toxische Inhalte“ zu bekämpfen oder Desinformation einzudämmen. In Wahrheit werden algorithmische Eingriffe zunehmend politisiert. Die Definition, was „Desinformation“ ist, verschiebt sich ständig, oft parallel zu den Kommunikationslinien westlicher Regierungen. Was gestern noch legitime Kritik war, gilt heute als potenzielle Gefahr für die „öffentliche Sicherheit“. Plattformrichtlinien orientieren sich dabei an den Vorgaben des EU-Digital Services Act oder an den sogenannten Codes of Practice on Disinformation. Dahinter steht ein europaweites Netz aus Aufsichtsbehörden, Kommissionen und externen „Faktenprüfern“, deren Zusammensetzung

kaum transparent ist.

Entscheidend ist: Diese Eingriffe geschehen automatisiert. Kein Mensch liest und urteilt, sondern ein KI-System bewertet Wahrscheinlichkeiten. Schlagwörter, Stimmungen, Quellen, alles wird in Echtzeit gescannt. Inhalte, die bestimmte semantische Muster enthalten, werden herabgestuft, andere dagegen priorisiert. Der Algorithmus wird so zum unsichtbaren Redakteur, der keine Verantwortung kennt.

Für Journalisten, Künstler oder Wissenschaftler hat das fatale Folgen. Sichtbarkeit entscheidet heute über Existenz. Wer seine Arbeit online publiziert, ist auf Reichweite angewiesen. Wenn diese Reichweite verschwindet, verliert man nicht nur Publikum, sondern auch Glaubwürdigkeit und Einkommen. Und weil die Plattformen keine konkreten Gründe nennen, bleibt der Betroffene im Dunkeln. Die Verantwortung verschiebt sich still vom Unternehmen zum Betroffenen selbst: „Vielleicht war dein Ton zu scharf, vielleicht dein Thema zu riskant." So entsteht die perfideste Form der Zensur, die Selbstzensur.

Der Staat löscht nicht selbst, er lässt löschen

Besonders brisant wird es, wenn staatliche Stellen und Plattformen zusammenarbeiten. Schon heute gibt es offizielle Meldewege zwischen Ministerien und Social-Media-Unternehmen. Die EU-Kommission unterhält eigene Taskforces, in denen Regierungsvertreter Hinweise auf angeblich „gefährliche" Inhalte direkt an die Plattformen weitergeben können. Diese wiederum agieren formal „freiwillig", handeln aber de facto im Auftrag politischer Vorgaben. Das Ergebnis ist eine neue Form indirekter Zensur: Der Staat löscht nicht selbst, er lässt löschen.

Auch auf nationaler Ebene existieren inzwischen Strukturen, die weit über den ursprünglichen Schutzbereich des NetzDG hinausgehen. Beim Bundeskriminalamt, im Auswärtigen Amt und in mehreren Landesministerien arbeiten spezialisierte Teams, die Inhalte beobachten, klassifizieren und bei Bedarf an Plattformen melden. Was mit der Bekämpfung von Hassrede begann, hat sich zu einem Informationslenkungssystem entwickelt. Dabei werden Plattformregeln und Rechtsnormen miteinander verschränkt, ein gefährlicher Graubereich zwischen privatem Unternehmensrecht und öffentlichem Strafrecht.

Währenddessen werden die technischen Systeme immer präziser. Moderne KI-Modelle analysieren nicht nur Wörter, sondern auch Tonlage, Kontext und Bildinhalte. Sie erkennen Ironie, Emotionen und politische Frames. Damit entsteht ein digitales Reputationssystem, das jede Äußerung in einen sozialen Kontext einordnet. Wer wiederholt Inhalte teilt, die als

„grenzwertig“ gelten, verliert automatisch Sichtbarkeit, ganz ohne gerichtliches Verfahren, ohne Verteidigungsmöglichkeit, ohne Transparenz.

Diese automatisierte Form der Diskurssteuerung erzeugt eine neue Gesellschaftsstruktur: eine, in der Macht nicht mehr sichtbar ausgeübt, sondern statistisch verteilt wird. Wer innerhalb der Grenzen spricht, wird belohnt. Wer sie überschreitet, verschwindet. Nicht im Gefängnis, sondern im Algorithmus.

Die klassische Pressezensur hatte wenigstens Zensoren mit Namen. Heute weiß niemand mehr, wer entscheidet. Das ist das eigentlich Gefährliche an der Gegenwart: Die Grenze zwischen freier Meinung und digitalem Delikt ist nicht mehr erkennbar und sie lässt sich täglich verschieben.

Vom Verdacht zur Hausdurchsuchung: Wie Justiz und KI zusammenwirken

In der klassischen Vorstellung des Rechtsstaats steht zwischen Verdacht und Hausdurchsuchung eine Hürde: die richterliche Kontrolle. Sie soll sicherstellen, dass nur dort eingegriffen wird, wo tatsächliche Anhaltspunkte für eine Straftat bestehen. Doch in der Praxis hat sich diese Kontrolle in vielen Fällen zu einer Formalie entwickelt. Der digitale Verdacht entsteht längst nicht mehr im Kopf eines Ermittlers, sondern im Code einer Maschine und wird dann durch einen juristischen Stempel legitimiert.

Der Weg von einem kritischen Text bis zur Hausdurchsuchung ist oft kürzer, als man glaubt. Ein Beitrag wird auf einer Plattform gemeldet oder von einem automatisierten System als „auffällig“ markiert. Der Plattformbetreiber erstellt einen Bericht, oft ergänzt durch maschinell erzeugte Risikoeinschätzungen. Diese landen bei einer Behörde oder einer Staatsanwaltschaft, die sich auf solche Berichte beruft, um Ermittlungen einzuleiten. Anschließend wird ein richterlicher Beschluss beantragt, häufig auf Grundlage von Screenshots, automatisierten Analysen oder aus dem Kontext gerissenen Zitaten.

Die richterliche Entscheidung erfolgt meist schriftlich, innerhalb weniger Stunden. Die vorgelegten Unterlagen enthalten selten eine vollständige Darstellung des Falls, sondern nur die relevanten Ausschnitte, die den Verdacht stützen. In Zeiten digitaler Überlastung und politischer Sensibilität wird kaum jemand das Risiko eingehen, einen Antrag abzulehnen. Ein Beschluss ist schnell unterschrieben und der Eingriff damit rechtskonform, zumindest auf dem Papier.

Was folgt, ist Routine: frühmorgendliche Durchsuchung, Beschlagnahme aller elektronischen Geräte, Spiegelung von Festplatten, Mitnahme von Smartphones, Notizen

und Datenträgern. Die Polizei handelt auf richterliche Anweisung, die Staatsanwaltschaft beruft sich auf „Pflicht zur Ermittlungsführung“, und am Ende hat niemand die Verantwortung. Der Schaden aber ist real, beruflich, psychologisch, gesellschaftlich. Selbst wenn das Verfahren später eingestellt wird, bleibt der Makel. Der Betroffene steht als jemand da, „gegen den ermittelt wurde“.

Man muss kein Jurist sein, um zu erkennen, dass hier ein Grundprinzip ausgehöhlt wird: der Schutz vor willkürlicher Durchsuchung. In Artikel 13 des Grundgesetzes ist die Unverletzlichkeit der Wohnung verankert, einst eine Lehre aus den totalitären Erfahrungen des 20. Jahrhunderts. Doch dieser Schutz wird löchrig, wenn digitale Verdachtskonstrukte als Beweisgrundlage genügen. Ein Algorithmus kann keine Verhältnismäßigkeit abwägen. Er kennt keine Ironie, keinen Kontext, keine journalistische Satire. Er errechnet Wahrscheinlichkeiten und produziert damit Verdachtsmomente, die Menschen in echte Bedrängnis bringen.

„Präventive Maßnahmen“

Besonders problematisch ist die zunehmende Nutzung sogenannter „präventiver Maßnahmen“. In mehreren Bundesländern dürfen Polizei und Staatsanwaltschaft Daten auswerten oder Wohnungen durchsuchen, ohne dass eine konkrete Straftat vorliegt, allein aufgrund einer prognostizierten Gefahr. Solche Prognosen entstehen durch KI-gestützte Musteranalysen. Der Mensch wird damit nicht mehr wegen seiner Taten verfolgt, sondern wegen seiner statistischen Ähnlichkeit zu jemandem, der etwas getan haben könnte.

Wie konnte es so weit kommen? Der Grund liegt im Zusammenspiel von technischer Machbarkeit und politischer Opportunität. Behörden sind längst überfordert mit der Flut digitaler Inhalte. KI-Systeme versprechen Entlastung, Geschwindigkeit, Effizienz. Gleichzeitig wächst der politische Druck, „gegen Hass und Hetze“ oder „Desinformation“ vorzugehen. Was daraus entsteht, ist eine gefährliche Allianz: Technische Vereinfachung trifft auf politische Erwartung. Das Ergebnis sind Ermittlungen, die sich eher nach Stimmungswellen als nach Rechtsnormen richten.

Richter und Staatsanwälte geraten dabei selbst in ein System stiller Lenkung. Niemand befiehlt ihnen, kritisch denkende Journalisten zu verfolgen oder oppositionelle Stimmen zu überwachen. Aber sie handeln in einem Klima, in dem Vorsicht als Schwäche gilt und Härte als Pflicht. Wer ablehnt, riskiert Kritik, wer zustimmt, erfüllt Erwartungen. Auf diese Weise entstehen Entscheidungen, die formal korrekt sind und inhaltlich dennoch Unrecht schaffen.

Und es gibt einen weiteren Aspekt: die Kosten. Jede Hausdurchsuchung, jede digitale Forensik, jede Auswertung von Geräten verschlingt enorme Summen. Sie bindet Ermittler, Techniker, Richter, Gutachter. Ressourcen, die an anderer Stelle fehlen, bei echter Kriminalität, bei Wirtschaftsdelikten, bei Gewaltverbrechen. Doch diese Prioritätensetzung findet kaum öffentliche Beachtung. Der spektakuläre Eingriff in ein Wohnzimmer erzielt mehr Wirkung als ein stilles Ermittlungsverfahren im Hintergrund. Abschreckung ist Teil der Strategie.

Diese Art von Einschüchterung funktioniert, weil sie individuell trifft, aber kollektiv wirkt. Sie erzeugt Angst, nicht durch Verurteilungen, sondern durch Verfahren. Es reicht, dass Menschen wissen, dass es passieren *kann*. Damit hat der Staat ein Werkzeug geschaffen, das subtiler und wirkungsvoller ist als jede offene Zensur. Denn wo Angst regiert, schweigt der Verstand zuerst.

Politische Sprache als Delikt, vom Guten Tag zum Gedankenverbrechen

Sprache war in jeder Epoche ein Gradmesser der Freiheit. Wenn Wörter selbst zum Risiko werden, ist das ein Warnsignal. Deutschland erlebt derzeit genau das: eine schleichende Kriminalisierung von Sprache, in der der Kontext keine Rolle mehr spielt, sondern nur noch der Verdacht, ein bestimmtes Wort könne „falschen Gruppen“ gefallen oder „falsche Assoziationen“ wecken.

Was vor wenigen Jahrzehnten als normale politische Zuspitzung galt, wird heute als potenziell gefährlich eingestuft. Wer etwa Begriffe wie „Systemversagen“, „Widerstand“ oder „Lügenpresse“ verwendet, gerät in Verdacht, extremistischen Sprachgebrauch zu übernehmen, selbst wenn der Inhalt sachlich und unaufgeregt formuliert ist. Der Übergang vom legitimen Protest zur angeblich staatsgefährdenden Rhetorik ist fließend geworden. Entscheidend ist nicht mehr, *was* gesagt wird, sondern *wer* es sagt.

Diese Entwicklung zeigt sich besonders drastisch an der öffentlichen Behandlung älterer Zitate. Aussagen, die früher selbstverständlich waren, wirken heute plötzlich wie Provokationen. Ein Franz Josef Strauß, der einst den „linken Meinungsterror“ anprangerte, würde heute wohl als Populist gelten. Angela Merkel sprach noch 2010 von der „Multikulti-Gesellschaft als gescheitertem Experiment“, ein Satz, der in heutiger Zeit möglicherweise eine Empörungswelle auslösen würde. Selbst Helmut Schmidt äußerte sich kritisch über Einwanderung, über transatlantische Abhängigkeiten und militärische Aufrüstung, Positionen, die heute in den Mainstream-Medien sofort in die Nähe von „rechts“ gerückt würden.

Begriffe werden gemieden, weil sie „gefährlich“ klingen könnten

Das Problem liegt nicht allein im Wandel gesellschaftlicher Normen, sondern im Verlust semantischer Präzision. Wörter werden zu Signalen, zu Marken, die eine Zugehörigkeit markieren. Wer ein „falsches“ Wort benutzt, verliert Reputation, unabhängig vom Inhalt. So entsteht ein Klima, in dem sich viele nicht mehr trauen, ungeschützt zu sprechen. Begriffe werden gemieden, weil sie „gefährlich“ klingen könnten. Die Folge ist ein sprachlicher Selbstschutzmechanismus, der die öffentliche Debatte verflacht.

Hinzu kommt, dass digitale Überwachungssysteme Sprache nicht verstehen, sondern nur vermessen. Algorithmen erkennen keine Ironie, keine Satire, keine historischen Bezüge. Wenn sie auf bestimmte Wörter trainiert sind, reagieren sie wie Spürhunde auf Reizgerüche: bedingungslos. Wird ein Beitrag markiert, folgt oft eine automatische Kette von Überprüfungen, vom Plattformfilter über Meldestellen bis zur Staatsanwaltschaft. Dort wird das maschinelle Ergebnis häufig als objektiver Hinweis behandelt, obwohl es nur eine statistische Wahrscheinlichkeit abbildet.

Damit entstehen paradoxe Situationen: Ein Journalist zitiert in kritischer Absicht eine Passage aus dem Dritten Reich und gerät selbst in Verdacht, diese Ideologie zu verbreiten. Eine Satirikerin nutzt provokante Sprache, um Missstände zu entlarven und sieht sich plötzlich strafrechtlichen Vorwürfen ausgesetzt. Der Kontext, der Sinn, die Absicht werden ausgeblendet. Entscheidend ist allein das Vorkommen eines markierten Wortes.

Diese Entwicklung hat gravierende Folgen für die Meinungsfreiheit. Wenn Sprache selbst als potenzielle Gefahr gilt, verliert der Diskurs seine Elastizität. Politik wird zum Sprachspiel ohne Risiko, Medien zum Echo einer vorsichtigen Mehrheit. Der öffentliche Raum schrumpft auf das, was niemanden stört und damit verschwindet genau das, was Demokratie lebendig macht: die Reibung.

Die Beweislast kehrt sich um

Besonders bedenklich ist die juristische Dimension. In mehreren Verfahren wurde in den letzten Jahren deutlich, dass Ermittlungen aufgrund von Zitaten, Symbolen oder Schlagwörtern eingeleitet wurden, ohne dass ein strafbarer Kontext vorlag. Der Tatbestand der „Verwendung verfassungsfeindlicher Symbole“ wird zunehmend extensiv ausgelegt. Ein Zitat, eine ironische Grafik reichen aus, um Ermittlungen zu rechtfertigen. Die Beweislast kehrt sich um: Nicht der Staat muss nachweisen, dass eine Absicht bestand, der Beschuldigte muss beweisen, dass keine bestand.

Das alles geschieht in einer Zeit, in der staatliche Stellen selbst die Bedeutung von Begriffen verschieben. Worte wie „Resilienz“, „Kampfbereitschaft“ oder „Zeitenwende“ sind in den politischen Wortschatz eingegangen, sie klingen nach Modernisierung, meinen aber Aufrüstung, Anpassung und Kontrolle. Die Sprache der Macht bleibt unantastbar, während die Sprache der Kritik kriminalisiert wird.

Der vielleicht größte Schaden aber ist psychologisch. Wer ständig überlegen muss, welche Wörter er verwenden darf, verliert die innere Freiheit des Denkens. Sprache wird dann nicht mehr Werkzeug, sondern Fessel. Der Weg vom „Guten Tag“ zum Gedankenverbrechen ist kein Sprung, er ist eine Serie kleiner Schritte, die man kaum bemerkt, weil sie alle im Namen der Vernunft geschehen.

Der Rechtsstaat in der Filterblase, warum Richter und Staatsanwälte mitspielen

Wenn man verstehen will, warum die Justiz in Deutschland in manchen Fällen mitspielt, wo sie eigentlich bremsen müsste, muss man die Mechanik dahinter kennen. Kein Richter bekommt eine politische Order, keine Staatsanwaltschaft einen geheimen Befehl, kritische Stimmen mundtot zu machen. Doch das System erzeugt eine Eigendynamik, die es ermöglicht, dass genau das geschieht, ganz ohne Zensurgesetz und ganz ohne formellen Druck.

Der Rechtsstaat lebt vom individuellen Gewissen, aber er funktioniert durch Hierarchie. Und diese Hierarchie ist empfindlich gegenüber Erwartungen. In einer Atmosphäre permanenter „Krisenbewältigung“, ob Pandemie, Krieg oder Desinformation, wird der Druck, „auf der richtigen Seite“ zu stehen, immens. Niemand will als derjenige gelten, der zu milde urteilte, zu spät reagierte oder einen „Gefährder“ laufen ließ. Das Ergebnis ist eine vorsorgliche Konformität, ein reflexartiges Mitziehen im Namen der Sicherheit.

Hinzu kommt ein strukturelles Problem: Staatsanwälte in Deutschland sind weisungsgebunden. Sie unterstehen den jeweiligen Justizministerien. Diese können, formal legal, Anweisungen geben, Verfahren aufzunehmen, zu unterbrechen oder Prioritäten zu setzen. In der Praxis bedeutet das: Wenn ein Thema politisch sensibel ist, wissen auch ohne ausdrückliche Anweisung alle Beteiligten, wie erwartet wird zu handeln. Niemand muss etwas sagen; das System kommuniziert nonverbal.

Richter wiederum sind formal unabhängig, aber sie arbeiten innerhalb eines Rahmens aus politischen Signalen, medialem Druck und institutioneller Routine. Die richterliche Unabhängigkeit endet oft dort, wo Zeit und Ressourcen fehlen. Wer täglich Dutzende Anträge auf Durchsuchung, Beschlagnahme oder Telekommunikationsüberwachung

abzeichnet, prüft wahrscheinlich nicht mehr die Verhältnismäßigkeit jedes einzelnen Falles. Viele Beschlüsse werden im Eilverfahren erlassen, formal korrekt, materiell zweifelhaft.

Parallel dazu verändert sich die Arbeitsweise der Justiz selbst. Digitale Fallmanagementsysteme, KI-gestützte Aktenanalysen und semantische Suchfunktionen sind längst Alltag. Was als Arbeitserleichterung gedacht war, hat Nebenwirkungen: Fälle werden nach Schlagworten priorisiert, Risikoeinstufungen automatisiert übernommen. Die Datenbanken, aus denen solche Einschätzungen stammen, speisen sich teils aus denselben Quellen wie die Überwachungssysteme der Polizei oder der Plattformen. So entstehen stille Rückkopplungen: Der Algorithmus, der eine Person auffällig findet, liefert gleichzeitig die Grundlage, auf der über deren strafrechtliche Relevanz entschieden wird.

Auch das Sprachklima in der Justiz hat sich gewandelt. Begriffe wie „Gefährder“, „radikalisierte Meinungsträger“ oder „Desinformationsakteur“ sind inzwischen Teil interner Dokumente und Fortbildungen. Sie klingen technisch, sind aber hochpolitisch. Denn wer so bezeichnet wird, verliert automatisch seine Unschuldsvermutung, er wird nicht mehr als Bürger, sondern als Risiko betrachtet. Das verändert die Perspektive der Ermittler. Aus dem Verdacht wird eine Bedrohung, aus der Bedrohung ein Fall, aus dem Fall eine Hausdurchsuchung.

Viele Richter und Staatsanwälte erkennen die Problematik durchaus. Doch sie befinden sich in einem System, das kaum Widerspruch zulässt. Wer zu oft nachfragt, gilt als schwierig. Wer auf die Einhaltung rechtsstaatlicher Grundsätze pocht, wird als realitätsfern bezeichnet. Der moralische Druck, „das Richtige zu tun“, ersetzt die rechtliche Abwägung. So entsteht schleichend ein Klima der stillen Zustimmung, nicht aus Bosheit, sondern aus Bequemlichkeit, Angst oder Karrieredenken.

Der Rechtsstaat verliert seine Rolle als Schutzschild des Bürgers

Die Folgen sind gravierend. Der Rechtsstaat verliert seine Rolle als Schutzschild des Bürgers und wird zum Vollstrecker eines diffusen Sicherheitsnarrativs. Statt die Grundrechte gegen Übertreibungen der Exekutive zu verteidigen, legitimiert er sie. Der Prozess läuft leise, fast unmerklich. Kein Gesetz wird gebrochen, kein Grundsatz offiziell aufgehoben. Alles bleibt formal in Ordnung, nur die innere Substanz schwindet.

Und über all dem schwebt die Technik. Die neuen juristischen Tools, die digitalen Justizakten und die automatisierten Fallanalysen schaffen eine neue Art der Abhängigkeit. Sie suggerieren Objektivität, wo in Wahrheit politische Vorannahmen eingebaut sind. Wenn ein System lernt, dass bestimmte Begriffe, Themen oder Quellen häufiger mit Ermittlungen

in Verbindung stehen, beginnt es, genau diese Muster zu verstärken. Die Justiz bewegt sich dann in einer algorithmischen Filterblase, in der sie nur noch das bestätigt, was sie ohnehin schon vermutet.

So entsteht ein Paradox: Der Rechtsstaat, der geschaffen wurde, um den Einzelnen vor der Willkür der Macht zu schützen, wird zum Werkzeug eben dieser Macht, nicht, weil er autoritär wäre, sondern weil er automatisiert wurde. Der Mensch verschwindet aus der Entscheidungskette, ersetzt durch Zahlen, Wahrscheinlichkeiten und Signale. Der Rechtsstaat bleibt auf dem Papier bestehen, aber sein Geist verflüchtigt sich, Byte für Byte.

Die Angstmaschine – wie Kontrolle zur Methode wird

Am Ende bleibt die Angst. Sie ist das unsichtbare Produkt eines Systems, das sich selbst als rational und notwendig beschreibt. Angst ist kein Zufall, sondern ein Werkzeug und sie funktioniert besser als jede offene Zensur. Wer sich fürchtet, beobachtet sich selbst. Wer sich selbst beobachtet, schweigt.

Diese Logik prägt inzwischen den politischen und medialen Alltag. Nicht die spektakulären Verbote, sondern die leisen Mechanismen halten die Gesellschaft in Schach. Eine Hausdurchsuchung hier, eine Sperrung dort, ein mediales Exempel zwischendurch, das genügt, um eine Botschaft zu senden: Wir sehen alles. Wir wissen alles. Und wir handeln, wenn es uns nötig erscheint. Der Rest erledigt sich von selbst.

So entsteht ein Klima der permanenten Vorsicht. Menschen überlegen, ob sie einen bestimmten Artikel teilen sollen, ob eine Kritik missverstanden werden könnte, ob sie in der falschen Gruppe stehen. Es ist die gleiche Logik, die einst in totalitären Systemen herrschte, nur ohne deren Brutalität. Heute reicht das Wissen, *dass* man beobachtet wird. Kontrolle ersetzt Gewalt.

Das Besondere an dieser neuen Angst ist ihre Sanftheit. Niemand schreit, niemand droht. Alles geschieht formal korrekt, eingebettet in Gesetze, Verordnungen und „Nutzungsbedingungen“. Jeder Eingriff lässt sich begründen: Schutz der Demokratie, Bekämpfung von Hass, Wahrung der Sicherheit. Doch die Summe dieser Begründungen ergibt eine Gesellschaft, in der das freie Wort nur noch geduldet wird, solange es nicht stört.

Die digitale Zensur tarnt sich als Verantwortung

Die klassische Zensur schützte sich durch Verbote. Die digitale Zensur tarnt sich als

Verantwortung. Sie löscht nicht mehr den Satz, sondern die Reichweite. Sie verfolgt keine Gedanken, sie verhindert ihre Verbreitung. Der neue Zensor trägt keinen Uniformrock, sondern schreibt Code. Er bestimmt, was sichtbar bleibt und wer im Schatten verschwindet.

Die Justiz, die Medien, die Politik, sie alle haben sich in diesem System eingerichtet. Die einen, weil sie glauben, damit Stabilität zu sichern. Die anderen, weil sie Angst haben, ausgeschlossen zu werden. Was dabei verloren geht, ist das Fundament einer offenen Gesellschaft: Vertrauen. Vertrauen in die Rechtsstaatlichkeit, in die Pressefreiheit, in das Recht auf Irrtum. Ohne Vertrauen bleibt nur Kontrolle und Kontrolle erzeugt Misstrauen.

Das ist der eigentliche Teufelskreis unserer Zeit: Ein System, das im Namen der Sicherheit immer neue Kontrollmechanismen schafft, produziert die Unsicherheit, vor der es zu schützen vorgibt. Je mehr Daten gesammelt, je mehr Inhalte gesperrt, je mehr Verdächtige konstruiert werden, desto größer wird das Misstrauen zwischen Bürger und Staat.

Wer heute den Mut hat, diese Entwicklung zu kritisieren, tut es meist unter dem Vorwurf, selbst ein Teil des Problems zu sein. So wird die Kritik an der Kontrolle selbst wieder kontrolliert. Das ist der Punkt, an dem Freiheit nicht mehr durch Gesetze bedroht wird, sondern durch Stimmungen.

Die Angstmaschine lebt von Schweigen

Doch noch ist nichts verloren. Der Rückweg beginnt mit Aufklärung und mit dem Mut, über diese Dinge offen zu sprechen. Die Angstmaschine lebt von Schweigen. Sie verliert an Kraft, sobald man sie benennt. Das ist die Aufgabe von Journalisten, Künstlern, Juristen und Bürgern zugleich: sichtbar machen, was unsichtbar geworden ist.

Denn es geht nicht um Technik, nicht um Algorithmen, nicht einmal um Daten. Es geht um das Menschenbild, das dahintersteht. Um die Frage, ob der Staat seinen Bürgern vertraut oder sie nur verwaltet. Ob er ihre Freiheit schützt oder sie dosiert. Der Rechtsstaat war nie perfekt, aber er war auf der Idee gebaut, dass der Mensch mehr ist als ein Risiko.

Wenn diese Idee fällt, fällt alles andere mit ihr. Deshalb ist jetzt die Zeit, das Prinzip Freiheit neu zu behaupten – gegen den Strom der Angst, gegen die Versuchung der Bequemlichkeit. Nicht durch Widerstand im heroischen Sinne, sondern durch Beharrlichkeit. Durch das einfache, unbeugsame Wort.

Denn Worte, so klein sie auch scheinen, sind das Letzte, was einem Menschen bleibt, wenn der Algorithmus schon längst entschieden hat, dass er besser schweigen sollte.

Mehr zum Thema:

Schon wieder Hausdurchsuchung wegen „falscher“ Meinung: Diese Einschüchterungen müssen aufhören!

Unsichtbar gemacht – Wie die EU kritische Medien zum Schweigen bringt

Die zweite Welle – Wie KI Deutschlands Sicherheitsapparat verändert

Chatkontrolle: Der größte Angriff auf unsere Privatsphäre seit der Vorratsdatenspeicherung

Quellen:

- Polizei durchsucht Wohnung von Norbert Bolz in Berlin – „Hausdurchsuchung wegen Tweet: Der Medienwissenschaftler hatte einen ironischen Kommentar gepostet, der laut Staatsanwaltschaft auf ein Verbot verfassungsfeindlicher Symbole hindeuten könnte.“
- „Fast alle Meldungen ans BKA erfolgen durch ‚Trusted-Flaggers‘“ – Artikel über die Zentrale Meldestelle für strafbare Inhalte im Internet (ZMI) beim BKA: „Die Meldestelle existiert seit 1. Februar 2022 und sammelt Hinweise zu Hass, Hetze und strafbaren Inhalten im Netz, die dann an Strafverfolgungsbehörden weitergeleitet werden.“
- „Strafbare Inhalte im Internet: BKA erhält 13.730 Meldungen“ – Zwischenbilanz der ZMI: „Über 13.700 Meldungen von Juni 2021 bis September 2023; rund 80 % davon an Strafverfolgungsbehörden weitergeleitet.“
- „Datenschutz: Diskussion um Palantir – Was soll die Polizei dürfen?“ Handelsblatt. Zum Einsatz von Palantir-Software in Deutschland und den datenschutzrechtlichen Risiken.
- „Palantir: US-Software zum Überwachen auch in Deutschland?“ Deutschlandfunk. Analyse über Einsatz und Kritik der Software im Polizeikontext.

- Zentrale Meldestelle für strafbare Inhalte im Internet (ZMI) beim Bundeskriminalamt Offizielle Seite: „Zentrale Meldestelle für strafbare Inhalte im Internet (ZMI) – BKA“. Informationen zur Einrichtung und Aufgabe der Meldestelle.

- Zwischenbilanz: „Strafbare Inhalte im Internet: BKA erhält 13.730 Meldungen“ Heise. Detaillierte Zahlen und Einschätzung zur Tätigkeit der ZMI.

- Kritik an Datenanalyse-Software / Überwachungspotenzial
Heise Background: „Palantir-Software für die Polizei: Ermittlung oder Überwachung?“ Detaillierte Kritik am Einsatz in deutschen Bundesländern.

- Zusammenarbeit Staat / Plattformen / Meldestellen
Pressemitteilung der Medienanstalten & BKA: „Zum 9. Aktionstag zur Bekämpfung von Hasspostings – BKA & Medienanstalten arbeiten bundesweit …“

- Netzpolitik.org: „Zentrale Meldestelle: Bundeskriminalamt plant jetzt ohne Zuarbeit der sozialen Netzwerke“. Hintergrundartikel zur Praxis der Meldestelle und Plattformbeteiligung.

Titelbild: Ana Rosa D. Ribeiro/shutterstock.com