Die erste Welle der Überwachungstechnik war reagierend: Man überprüfte, was geschehen war. Die neue Welle ist präventiv: Sie arbeitet mit Wahrscheinlichkeiten, Prognosen, algorithmischen Entscheidungen – etwa mit „AIP“ der US-Firma Palantir. Politiker, die kaum IT-Kompetenz haben, bejubeln Verfahrensplattformen und KI-Unterstützung, ohne zu erkennen, dass sie damit ein Instrument erlauben, das den Staat zum allumfassenden Datenapparat wandelt. Wir müssen den Rechtsstaat auch im digitalen Raum verteidigen! Von **Günther Burbach**.

Dieser Beitrag ist auch als Audio-Podcast verfügbar.

https://www.nachdenkseiten.de/upload/podcast/251020_Die_zweite_Welle_Wie_KI_Deutschlands_Sicherheitsapparat_veraendert_NDS.mp3

Podcast: Play in new window | Download

Stell dir vor: Du bewegst dich durch den Alltag, du rufst ein Taxi, surfst im Netz, besuchst Freunde, postest Sprüche auf Social Media, bekommst eine Rechnung zugeschickt. All das hinterlässt digitale Spuren. Nun stell dir vor, ein System zieht all diese Spuren zusammen, bewertet, verknüpft, prognostiziert und entscheidet leise mit, wohin dein Leben steuert. Das klingt wie Science-Fiction? Nein, genau darauf zielt die „zweite Welle der Überwachung“.

Deutschland steht gerade mitten in dieser Welle. Wir haben bereits die erste Phase hinter uns: klassische Überwachungstechnik wie Vorratsdatenspeicherung, Videoüberwachung, Telefonabhörungen. Doch sie war reagierend: Man überprüfte, was geschehen war. Die neue Welle ist präventiv: Sie arbeitet mit Wahrscheinlichkeiten, Prognosen, algorithmischen Entscheidungen. Und das zentrale Werkzeug, mit dem sie in deutschen Polizeien, Ministerien und Behörden Einzug hält, trägt den stolzen Namen „Analysesoftware“. Doch in Wahrheit ist sie ein Entscheidungsinstrument.

In Ländern wie Bayern, Hessen und Nordrhein-Westfalen sitzt die US-Softwarefirma Palantir längst im Maschinenraum der Sicherheitspolitik. Politiker, die kaum IT-Kompetenz haben, bejubeln Verfahrensplattformen und KI-Unterstützung, ohne zu erkennen, dass sie damit ein Instrument erlauben, das den Staat zum allumfassenden Datenapparat wandelt.

Wenn wir jetzt zulassen, dass Palantir mit KI-Modulen in bestehende Polizeisysteme eingebettet wird, dann geben wir Kontrolle ab, bevor wir wissen, wozu. Wir riskieren, dass wir zu Objekten eines Systems mutieren, das „uns“ bewacht, statt „für uns“ da zu sein.

Dies ist der Kampf um Freiheit im digitalen Zeitalter und wir haben nicht mehr viel Zeit.

Palantir 2.0 – Wenn KI das Kommando übernimmt

Was bislang als Datenplattform galt, wird gerade zu einem System, das selbstständig denkt. Palantir nennt es „AIP", die Artificial Intelligence Platform. Das klingt harmlos, ist aber ein Quantensprung. Denn das System kann mittlerweile Zusammenhänge erkennen, die kein Mensch mehr nachvollzieht. Es verknüpft Gesichter mit Aufenthaltsorten, Kontakte mit Geldströmen, Bewegungen mit Kommunikationsmustern. Und es schlägt von selbst vor, wo als Nächstes zu ermitteln wäre.

Damit verändert sich die Rolle des Menschen. Der Ermittler wird zum Bediener einer Maschine, die längst gelernt hat, was er sucht. Ein Befehl genügt: *„Zeig mir alle Personen, die letzte Woche im Umkreis von 500 Metern um X waren und in Verbindung zu Y stehen."* Sekunden später erscheint ein Netz aus Linien, Punkten und Querverbindungen, das digitale Abbild einer Gesellschaft.

Wer jetzt glaubt, das diene nur der Kriminalitätsbekämpfung, irrt. Solche Systeme funktionieren umso besser, je mehr Daten man hineinschüttet. Das bedeutet: Je umfassender die Erfassung, desto größer ist die Versuchung, sie für andere Zwecke zu nutzen – Gefahrenabwehr, Migration, politische Analyse, Krisenmanagement. Der Schritt von der Polizeiarbeit zur sozialen Steuerung ist dann kein Sprung mehr, sondern ein Schieberegler.

Und während die Öffentlichkeit noch diskutiert, ob man Überwachungskameras an jeder Ecke braucht, haben die Behörden längst eine andere Waffe in der Hand: eine künstliche Intelligenz, die jeden Bürger als Datencluster begreift. Sie unterscheidet nicht zwischen Täter und Unbeteiligtem, sondern zwischen relevant und irrelevant. Das ist eine gefährliche Verschiebung: Schuld wird durch Wahrscheinlichkeit ersetzt.

Noch bedenklicher ist, dass niemand mehr weiß, wie das System zu seinen Schlüssen kommt. Palantir AIP ist eine Blackbox, ein mathematischer Nebel, in dem Datenflüsse Entscheidungen formen, ohne dass jemand den Weg nachvollziehen kann. Wenn eine KI eine Person als „auffällig" markiert, ist das keine Justizhandlung mehr, sondern eine maschinelle Bewertung. Aber sie wird behandelt, als käme sie von oben: neutral, sachlich, unfehlbar.

In Wahrheit steckt hinter jeder künstlichen Intelligenz ein politischer Wille, die Entscheidung, Kontrolle über Unsicherheit zu stellen. Das ist menschlich nachvollziehbar,

aber gesellschaftlich fatal. Denn ein Staat, der sich auf Software verlässt, verlernt das Denken in Zweifeln. Und genau das ist die Essenz von Rechtsstaatlichkeit: Zweifel, Prüfung, Verantwortung.

Politischer Leichtsinn – Digitalisierung um jeden Preis

In den Landesregierungen wird der Einsatz solcher Systeme oft als Fortschritt verkauft. „Effizienzsteigerung", „Modernisierung der Ermittlungsarbeit", „digitale Souveränität", das sind die Schlagworte, mit denen Minister ihre Pressemitteilungen schmücken. Dahinter steckt selten böser Wille, aber oft schlichte Ahnungslosigkeit.

Viele Innenpolitiker wissen nicht, was sie da genehmigen. Sie lassen sich Vorführungen zeigen, auf denen Palantir-Mitarbeiter beeindruckende Visualisierungen präsentieren: farbige Linien, blitzende Netzwerke, Live-Simulationen. Man sieht Daten fließen und fühlt sich, als hätte man das Chaos im Griff. Das ist der Moment, der für die Demokratie am gefährlichsten ist: wenn Technik Vertrauen ersetzt.

In Bayern zum Beispiel wurde die Einführung von VeRA mit großem Pathos angekündigt. Man sprach von einem „wichtigen Schritt in die Zukunft" und davon, dass „alle Datenschutzfragen geklärt" seien. Kaum jemand fragte nach, was im Hintergrund passiert, wenn diese Software arbeitet. Wie viele Bürgerdaten werden einbezogen? Wie lange bleiben sie gespeichert? Wer überprüft, ob der Algorithmus verzerrt urteilt? Keine Antwort, nirgends.

Auch in Hessen, wo Palantir zuerst eingeführt wurde, hat sich kaum jemand getraut, das System zu hinterfragen. Die wenigen, die es taten, wurden als Fortschrittsverweigerer abgestempelt. Dabei hat das Bundesverfassungsgericht 2023 eindeutig gewarnt: Eine solche Datenanalyse ist nur in engen Grenzen zulässig, und nur, wenn sie sich auf konkrete Gefahren bezieht. In der Praxis aber werden immer mehr Datenquellen angezapft, um den „Erkenntnisgewinn" zu steigern. Das Ziel wird zur Rechtfertigung der Mittel.

Diese politische Naivität hat System. Man will zeigen, dass man „digital denkt". Man will modern wirken, innovationsfreudig, sicherheitspolitisch stark. Aber man versteht nicht, dass man in Wahrheit Machtstrukturen importiert, die man nie wieder loswird. Wer einmal einen Algorithmus entscheiden lässt, wird ihn nicht mehr stoppen, weil jedes Abschalten als Sicherheitsrisiko gilt. So wächst ein Apparat, der sich selbst legitimiert.

Das juristische Feigenblatt – Wenn Gesetze der Technik folgen

Früher war es so: Die Technik musste sich den Gesetzen beugen. Heute werden die Gesetze an die Technik angepasst. Genau das passiert gerade in Deutschland. Nach den Urteilen des Bundesverfassungsgerichts, die den Einsatz automatisierter Polizeianalyse in Hessen und Hamburg als verfassungswidrig einstuften, hätte man meinen können: Schluss, Stopp, Neuorientierung. Doch das Gegenteil trat ein.

Statt die Systeme zu pausieren, wurden Gesetze nachgeschärft. Die Lücken, auf die Karlsruhe hingewiesen hatte, schließt man nun mit neuen Formulierungen. Die Botschaft lautet: Wir wollen diese Werkzeuge, koste es, was es wolle. Datenschutz wird zur Randnotiz, Grundrechte werden in Paragrafen gegossen, die den digitalen Ausnahmezustand legalisieren.

Es ist ein stiller Umbau des Rechtsstaats. Nicht frontal, nicht laut, sondern durch kleine, technokratische Eingriffe. Ein neues Wort hier, ein neuer Absatz da, und schon ist erlaubt, was gestern verboten war. Das nennt man „Modernisierung“. In Wahrheit ist es eine stille Verschiebung der Machtbalance zwischen Bürger und Staat.

Wo früher der Richter-Vorbehalt galt, genügt jetzt eine „automatisierte Analyse zur Gefahrenprognose“. Wo früher der Einzelfall zählte, zählt heute die Datenlage. Der Mensch als Individuum wird durch Wahrscheinlichkeitscluster ersetzt.

Diese Entwicklung ist gefährlicher als jede sichtbare Kamera an der Straßenecke. Denn sie findet unsichtbar statt, im Inneren von Behörden, Rechenzentren, Cloud-Servern. Und sie wird abgesichert durch Politiker, die von Technik reden, aber Macht meinen.

Leben unter dem Algorithmus – Was es für jeden bedeutet

Was bedeutet das alles konkret, für dich, für mich, für jeden einzelnen Menschen? Es bedeutet, dass der Staat dich kennt, lange bevor du ihn triffst.

Wenn du morgens dein Handy einschaltest, weiß ein System, wo du bist. Wenn du online einkaufst, erkennt es deine Vorlieben. Wenn du dich in der Nähe eines Tatorts bewegst, landet dein Standort im Raster. Und wenn jemand in deinem Umfeld auffällig wird, bist du automatisch ein „Beziehungsobjekt“, ein Punkt in einem Netz, das du nie betreten hast.

Das alles passiert nicht, weil jemand dich gezielt überwachen will. Es passiert, weil du in einem System lebst, das alles wissen will, für den Fall der Fälle. Aus Sicherheitsgründen, versteht sich. Aus „Verantwortung“. Und weil niemand mehr unterscheiden kann, was sinnvoll ist und was Missbrauch, wächst eine Kultur der Dauererfassung.

Der Beamte, der dich früher kontrollierte, war sichtbar, ansprechbar, menschlich. Der Algorithmus ist unsichtbar. Er prüft, vergleicht, bewertet und du erfährst es nicht. Du weißt nicht, ob du auf einer Liste stehst, ob du einen Risikowert hast, ob dein Name in einem Zusammenhang auftaucht, der dich eines Tages blockiert. Vielleicht bekommst du einfach keinen Kredit, keine Wohnung, keine Sicherheitsfreigabe. Vielleicht wirst du nur langsamer durchsucht, weil dich das System als harmlos markiert hat. Oder schneller, weil nicht.

Unsichtbare Kontrolle

Und das ist der Kern dieser zweiten Welle: Sie verändert nicht nur die Polizei, sondern die Wahrnehmung von Normalität. Wenn Kontrolle unsichtbar wird, wird sie auch unwidersprochen. Man gewöhnt sich daran, dass alles registriert, verknüpft, ausgewertet wird. Man nennt das dann Effizienz, Sicherheit, Fortschritt. Und übersieht, dass die Freiheit leise verschwindet, nicht mit einem Schlag, sondern mit jedem Software-Update ein Stück mehr.

Am Ende steht kein Polizeistaat alter Prägung, sondern ein digitaler Verwaltungsstaat, der alles weiß und nichts mehr erklären muss. Ein Staat, der Bürger nicht mehr beschützt, sondern berechnet. Und das ist vielleicht die gefährlichste Form von Kontrolle, weil sie sich als Vernunft tarnt.

Staat und Mensch

Wenn man also heute in den Innenministerien über KI in der Sicherheit redet, dann redet man in Wahrheit über das Verhältnis zwischen Staat und Mensch. Über Vertrauen, über Grenzen, über Verantwortung. Und darüber, ob wir noch selbst bestimmen, was wir wissen dürfen, oder ob künftig ein Algorithmus entscheidet, wer wir sind.

Das ist keine Zukunftsangst, sondern Gegenwart. Die zweite Welle der Überwachung rollt und sie rollt nicht über Daten, sondern über Menschen.

Wenn Politiker über Digitalisierung reden, denken sie an Bürokratieabbau, schnellere Verfahren, moderne Verwaltungen. Doch im Innern der Sicherheitsapparate hat Digitalisierung längst eine andere Bedeutung: Sie ist der Schlüssel zur Kontrolle. Nicht durch Gewalt, sondern durch Berechnung.

Während das Land über Energiesparen, Migration oder den Haushalt streitet, rollt eine zweite Welle der Überwachung heran, getragen von Software, gespeist von Daten, angetrieben von Künstlicher Intelligenz. Ihr Motor heißt Palantir. Und ihre Wirkung reicht

weit über Polizei und Justiz hinaus: Sie verändert das Verhältnis zwischen Staat und Bürger.

In Bayern, Hessen und Nordrhein-Westfalen laufen die Systeme bereits. Die Politiker nennen das „effizient“. Die Datenschützer nennen es „riskant“. Und viele Bürger merken es gar nicht. Doch hinter den schönen Worten von Modernisierung, KI und digitaler Sicherheit verbirgt sich ein tiefgreifender Umbau, ein technischer, juristischer und kultureller.

Die zweite Welle der Überwachung kommt als Software-Update

Die zweite Welle der Überwachung kommt ohne Sirenen. Sie braucht keine Kameras, keine Blockwarte, keine Mauern. Sie kommt als Software-Update. Als KI-Modul. Als Routinefunktion. Und genau das macht sie so gefährlich: Sie verändert die Gesellschaft nicht durch Zwang, sondern durch Gewöhnung.

Am Ende dieser Entwicklung steht kein Diktator und keine sichtbare Zensur. Am Ende steht eine Infrastruktur, die alles weiß, bevor jemand fragt, und alles bewertet, bevor jemand denkt.

Es beginnt harmlos: Daten sollen helfen, Leben zu retten, Kriminalität zu bekämpfen, Gefahren zu verhindern. Doch was als Schutz gedacht ist, wird schnell zur Logik des Verdachts. Die Maschine unterscheidet nicht mehr zwischen Täter und Zeuge, zwischen relevant und zufällig. Sie erkennt Muster, nicht Menschen. Und aus diesen Mustern entstehen Entscheidungen, die niemand mehr hinterfragt, weil sie „objektiv“ erscheinen.

Das ist der Punkt, an dem ein demokratischer Staat sich selbst gefährdet. Nicht, weil er böse Absichten hätte, sondern weil er glaubt, Kontrolle sei gleich Sicherheit. Dabei ist Kontrolle das Gegenteil von Vertrauen und Vertrauen das Fundament jeder freien Gesellschaft.

Die zweite Welle der Überwachung ist keine ferne Zukunft. Sie ist längst da. Sie steckt in den neuen Polizeigesetzen, in den Cloud-Verträgen, in den unscheinbaren Phrasen über „digitale Resilienz“. Sie wächst in Serverräumen, Ministerien und Rechenzentren. Und sie wird bleiben, solange niemand fragt, wer sie steuert und wem sie dient.

Wir müssen den Rechtsstaat im digitalen Raum verteidigen

Wer also glaubt, dass all das nur Fachpolitik betrifft, der täuscht sich. Es betrifft uns alle. Es entscheidet darüber, ob der Staat in Zukunft Bürger schützt oder Bürgerprofile. Ob Freiheit ein Risiko bleibt, das wir eingehen dürfen, oder ein Restwert, den die Algorithmen noch tolerieren.

Es gibt keinen lauteren Weckruf als diesen: Wenn wir den Rechtsstaat erhalten wollen, müssen wir ihn auch im digitalen Raum verteidigen. Nicht mit Technikgläubigkeit, sondern mit Bewusstsein. Nicht mit Paragrafen, sondern mit Haltung.

Denn die zweite Welle rollt und es bleibt zu befürchten, dass niemand da ist, der einen Schutzwall aufbaut, oder auch nur bemerkt, dass wir alle einen Schutzwall benötigen.

Quellen

- „Federal Council calls for rapid deployment for the police“ – Heise, 2025: Pilotbetrieb von **VeRA** in Bayern, Verbindung mehrerer Polizeisysteme zur Analyseplattform (Heise)
- „Palantir und Polizei: Hessendata als Vorbild für ganz Deutschland?“ – FAZ: über Einsatz in Hessen, Anpassung an Landesverhältnisse (FAZ)
- „Analyse-Software der Hessischen Polizei vor dem Bundesverfassungsgericht“ – Webseite Landesdatenschutz Hessen: Rechtliche Auseinandersetzungen um Hessendata / Gotham in Hessen (Datenschutz Hessen)
- „Verfassungsbeschwerde gegen umstrittene Polizei-Software“ – Legal Tribune Online, 2025: Beschwerde gegen Palantir-Einsatz in Bayern wegen „massenhafter Datenauswertung“ (LTO)
- „Besuch bei Vera: Wie Bayerns Polizei Palantir nutzt“ – Golem: Reportage, wie die Plattform VeRA tatsächlich funktioniert (Golem)
- „Regelungen für Palantir-Einsatz verfassungswidrig“ – Behörden Spiegel, 2023: Rechtliche Einwände gegen automatisierte Auswertung in Hessen (Behörden Spiegel)
- „Palantir: Warum die Polizei-Software umstritten ist“ – Deutschlandfunk: Hintergrund, Datenschutzbedenken, technische und politische Aspekte (Deutschlandfunk)
- „KI bei der Polizei: Vera, übernehmen Sie!“ – Zeit Online, 2025: über KI-Ambitionen der bayerischen Polizei mit Palantir (Zeit Online)

Titelbild: APChanel / Shutterstock