Wenn durch die Verschiebung staatlicher Funktionslogik jeder Bürger zu einem potenziellen Verdachtsfall wird, erodiert das Gerüst der liberalen Demokratie – nicht laut, nicht revolutionär, nicht mit dem Pathos einer neuen Verfassung, sondern mit Schnittstellen, Registern, „Matching-Diensten” und Datenhäusern. Die Frage lautet deshalb nicht mehr, ob der Staat digital wird, sondern mit welcher Durchdringung er unser Leben überwacht, interpretiert und vorherzusagen versucht. Wer diesen Umbau bloß für ein Modernisierungsprojekt hält, verkennt seine politische Tragweite und Brisanz. Von **Detlef Koch**.

*Dieser Beitrag ist auch als Audio-Podcast verfügbar.*

https://www.nachdenkseiten.de/upload/podcast/260419_Technofeudalismus_der_Plattform_Staat_Wenn_jeder_Buerger_zu_einem_potentiellen_Verdachtsfall_wird_Teil_3_NDS.mp3

Podcast: Play in new window | Download

*Den ersten Teil der Serie finden Sie unter diesem Link, den zweiten Teil unter diesem Link.*

Das Programm *(P20)* [1] entwirft für die deutschen Polizeien eine *„single digital network“*-Architektur mit zentralem *„data house“*. Auf europäischer Ebene sind biometrische Interoperabilitätsdienste wie der *Shared Biometric Matching Service* (sBMS)[2], das *Entry/Exit System* (EES)[3] und das *European Travel Information and Authorisation System* (ETIAS)[4] Teil der Grenzverwaltung, das Identitäten, Reisen und Risiken schon vor der Bewegung selbst prüft (Interoperabilität ist die Fähigkeit unterschiedlicher IT-Systeme, Daten automatisiert, standardisiert und nahtlos auszutauschen sowie effektiv zusammenzuarbeiten). Parallel entstehen im zivilen Bereich Plattformen wie *Telematikinfrastruktur* (TI)[5], *elektronische Patientenakte* (ePA), *Deutsches Elektronisches Melde- und Informationssystem für den Infektionsschutz* (DEMIS) oder die Analyse- und Datenhaushalte der *Bundesagentur für Arbeit* (BA)[6]. Die operative Frage lautet deshalb nicht mehr, ob der Staat digital wird, sondern mit welcher Durchdringung er unser Leben überwacht, interpretiert und vorherzusagen versucht.

Wer diesen Umbau bloß für ein Modernisierungsprojekt hält, verkennt seine politische Tragweite und Brisanz. P20 will die heterogene IT-Landschaft der Polizeien durch standardisierte Dienste und ein zentrales Datenhaus ersetzen, in dem Informationen zusammengeführt, verknüpft und – soweit rechtlich zulässig – anderen Polizeien sowie Justiz- und Ausländerbehörden zugänglich gemacht werden. Bis 2030 sollen verschiedene Informationssysteme, Anwendungen und Prozesse unter dem Dach dieses Ökosystems

zusammenlaufen. Das ist mehr als digitale Aktenpflege. Es ist der Übergang von Fachverfahren zu Infrastruktur – und damit zu einer Form von Macht, die nicht mehr nur über Weisungen, sondern über Architektur ausgeübt wird.

Gerade die Polizei zeigt, wie weit dieser Übergang bereits fortgeschritten ist. Seit 2015 lässt sich ein klarer Trend von ortsbezogenen Prognosewerkzeugen wie *Predictive Monitoring / Analysis / Prediction*(PreMAP)[7], *Kriminalitätsprognose* (KrimPro)[8], *Kriminalitätslagebild*(KLB-operativ)[9], *System zur Kriminalitätsauswertung und Lageantizipation* (SKALA)[10] oder *Pre Crime Observation System* (PRECOBS) hin zu verfahrensübergreifenden Analyseplattformen beobachten.

In Hessen, Nordrhein-Westfalen und Bayern laufen mit hessenDATA, *Datenbankübergreifende Analyse und Recherche* (DAR)[11] und *Verfahrensübergreifende Recherche- und Analyseplattform* (VeRA) Palantir-basierte Systeme; parallel existieren mit Gesichtserkennungssystem (GES) und Radar Islamistisch-Terroristische Gefährderbewertung (RADAR-iTE)[12] bundesweite Infrastrukturen. Der entscheidende Punkt ist nicht der Name der Software. Entscheidend ist der Funktionswandel: weg von der einzelnen Spur, hin zum verknüpfbaren Datenraum.

Die Hamburger Forschungsgruppe um Simon Egbert und Susanne Krasmann hat diesen Wandel präzise beschrieben. Predictive Policing sei keine totale Revolution, wohl aber eine Zäsur, weil Polizeiarbeit datafiziert und plattformisiert werde. Vorhersagen, Ermittlungsunterstützung und Prävention werden in dieselbe datengetriebene Logik eingespannt; die Zukunft der Polizeiarbeit liege in der Verknüpfung vielfältiger Datensätze, auch aus polizeiexternen Quellen.[13] Damit verschiebt sich der Modus staatlichen Wissens: von der fallbezogenen Rekonstruktion zum vorausschauenden Vergleich von Zusammenhängen, in Fachkreisen auch antizipative Korrelation genannt. Nicht Gewissheit, sondern Relevanz wird zur operativen Währung.

Im Bereich Grenzschutz erscheint dieselbe Logik in größerem Maßstab und mit geringerer Sichtbarkeit. Das operative Gefüge aus Schengener Informationssystem (SIS), Visa Information System (VIS), Eurodac, EES und sBMS verschiebt die Kontrolle von der physischen Grenze auf vorgelagerte Datenprüfungen. EES registriert Ein- und Ausreisen biometrisch; ETIAS[14] soll visumfreie Reisende anhand von Screening-Regeln, Risikoindikatoren und Watchlists vorab bewerten; das European Search Portal (ESP) und das Common Identity Repository (CIR) sollen getrennte Register in Richtung einer übergreifenden Suche und konsolidierten Identität verschieben. Hinzu kommen die Dienste des European Border Surveillance System (EUROSUR) Fusion Services, die Anomalien erkennen und Schiffspositionen prognostizieren. So entsteht kein digitaler Schlagbaum,

sondern ein dichtes Vorfeld aus Verifikation, Priorisierung und Verdachtsproduktion.

Auch die zivile Verwaltung folgt dieser Plattformlogik. Im Gesundheitsbereich[15] koppeln TI, ePA, E-Rezept, DEMIS, SurvNet@RKI, *Surveillance Outbreak Response Management and Analysis System* (SORMAS) und *Elektronisches Melde- und Informationssystem Gesundheitsämter* (EMIGA) Versorgung, Meldewesen und Sekundärnutzung zu zentral oder zentral koordinierten Infrastrukturen. Besonders folgenreich ist die Opt-out-Logik der ePA: Sie verlagert den Schwerpunkt von individueller Einwilligung zur populationsweiten Bereitstellung. In der Arbeits- und Sozialverwaltung bilden Vermittlungs-, Beratungs- und Informationssystem (VerBIS), Arbeitslosengeld II/Sozialgeld-Leistungsverfahren (ALLEGRO), das Data Warehouse der BA, Datenbasierte operative Ressourcenallokation (DORA) und der Grundsicherungsdatenabgleich einen stark zentralisierten Komplex aus Fallbearbeitung, Auswertung und Kontrolle. Selbst kommunale Datenhubs und digitale Zwillinge in Städten wie Hamburg, Leipzig oder München folgen diesem Muster: Daten werden nicht bloß gesammelt, sondern als administrativ wirksame Infrastruktur für Zuteilung, Priorisierung, Monitoring und Ressourcensteuerung eingerichtet.

Gerade darin liegt der Kern des Problems. Diese Systeme treffen meist nicht das letzte Urteil. Sie ordnen Aufmerksamkeit. Sie markieren Zonen, Personen, Fahrzeuge, Reisen oder Fallkonstellationen als relevant. Genau darin besteht ihre Macht. Wer Aufmerksamkeit sortiert, verschiebt faktisch Verdacht, Ressourcen und Eingriffsintensität. Die entscheidende politische Frage lautet daher nicht, ob Maschinen „intelligent“ sind, sondern wer durch ihre Risikologik sichtbarer, verdächtiger oder kontrollierbarer wird. Das Europäische Netzwerk gegen Rassismus (ENAR)[16] spricht von einem „hardwiring“ diskriminierender Polizeipraktiken, wenn historische Verzerrungen in technische Verfahren eingeschrieben werden. Amnesty International[17] beschreibt predictive policing als Form massenhafter Überwachung mit „chilling effects“ (abschreckende Wirkung), Transparenzdefiziten und fehlenden Rechtsbehelfen.

Der Bürgerrechtsabbau vollzieht sich in diesem Modell nicht als dramatische Suspendierung, sondern als strukturelle Verschiebung.

Erstens wird der Eingriff zeitlich vorverlagert: Nicht erst die Tat oder der konkrete Antrag, sondern bereits Risikozuordnung, Anomalie oder Korrelation können operative Reaktionen auslösen. Zweitens wird die Person funktional entgrenzt: Wer in solchen Architekturen erscheint, ist nicht mehr nur Reisender, Patient, Leistungsbezieher oder Beschuldigter, sondern ein verknüpfbarer Datenpunkt in mehreren Systemen zugleich. Drittens wird Rechtsschutz asymmetrisch: Betroffene wissen oft nicht, dass sie profiliert wurden, auf welcher Datenbasis dies geschah und wie sie eine maschinell vermittelte Einschätzung

wirksam anfechten könnten. Das ist kein Randproblem technischer Verwaltung. Das ist die stille Verschiebung vom liberalen Rechtsstaat der Akte zum präventiven Plattformstaat der Korrelation.

Die Informationsasymmetrie ist dabei kein Begleitschaden, sondern Funktionsbedingung. Der Staat – oft zusammen mit privaten Anbietern – weiß immer mehr über die Verknüpfbarkeit von Daten, die Herkunft von Signalen und die Logik ihrer Bewertung; der Einzelne weiß immer weniger darüber, wann er von diesen Prozessen erfasst, gerankt oder weitergereicht wird. Selbst dort, wo Transparenz versprochen wird, bleiben Datenquellen, Schnittstellen und Erfolgsmaße häufig unklar.[18][19]

Die Kartierung operativer Polizeisoftware nennt als wiederkehrende Probleme unklare Quellsysteme, den Blackbox-Charakter proprietärer Plattformen und die Nichtveröffentlichung von Erfolgs- und Fehlschlagsdaten aus ermittlungstaktischen Gründen. Kommunale Plattformdokumente wiederum lassen Hosting, Echtzeitkopplung und Entscheidungsautomatisierung oft im Ungefähren. Das Machtgefälle entsteht also nicht nur aus mehr Daten, sondern aus ungleichem Wissen über die Regeln ihrer Verknüpfung.

Dass diese Entwicklung mit dem Rechtsstaat kollidiert, ist längst sichtbar. Der zentrale Bruch verläuft dort, wo aus klassischer Datenverarbeitung für konkrete Zwecke eine zweckändernde, verfahrensübergreifende Analyse wird, die „neues Wissen“ generiert. Das Bundesverfassungsgericht hat 2023 die damaligen Normen in Hessen und Hamburg zur automatisierten Datenanalyse wegen unzureichender Eingriffsschwellen, mangelnder Normenklarheit und fehlender Verhältnismäßigkeit beanstandet; die Länder reagieren nun mit neuen Rechtsgrundlagen. Aber gerade dieser Vorgang zeigt, wie der Abbau von Freiheitsgarantien heute funktioniert: nicht primär durch den offenen Bruch, sondern durch die nachträgliche Legalisierung eines technisch bereits eingeschliffenen Modus. Erst wird die Infrastruktur geschaffen. Dann ringt das Recht um Anschluss.

Wer diese Entwicklung nur national betrachtet, unterschätzt ihre Reichweite. Für Polizei, Grenze und Militär ist nicht überall eine gemeinsame Führungsstruktur sichtbar, sehr wohl aber eine funktionale Konvergenz: Datenfusion, Sensorik, Interoperabilität und „Data-to-Decision“ prägen die operative Grammatik aller drei Felder. Im militärischen Bereich ist öffentlich vor allem assistierte, nicht vollautonome Nutzung künstlicher Intelligenz (KI) dokumentiert; gerade deshalb ist der Befund so aufschlussreich. Die Macht liegt weniger in der automatisierten Wirkauslösung als in „digitalen Backbones“ (digitales Rückgrat), Mission Networks, Lagebildsystemen und der Transparenzasymmetrie, die sie erzeugen.

Die politische Pointe ist unangenehm schlicht: Selbst wo Menschen formell entscheiden,

entscheiden sie zunehmend in Räumen, deren Relevanzen, Prioritäten und Sichtbarkeiten technisch vorstrukturiert sind.

Hier helfen die Begriffe der Plattformtheorie weiter. José van Dijck und ihre Co-Autoren schreiben, Plattformen bildeten soziale Strukturen nicht bloß ab, sondern produzierten sie. Vili Lehdonvirta beschreibt digitale Plattformen als regelsetzende Autoritäten, die staatliche Funktionen nachbilden. Auf die aktuelle Entwicklung übertragen heißt das: Die zentrale Bewegung ist keine Entstaatlichung, sondern eine Neuformatierung staatlicher Macht in Plattformform. Macht organisiert sich weniger über sichtbare Hierarchie und mehr über Zugang zu Infrastrukturen, Standards, Daten und Matching-Diensten. Gerade Palantir in der Polizei, sBMS im Grenzschutz oder TI und ePA im Gesundheitssektor zeigen, dass operative Steuerung an technische Ökosysteme gebunden wird – und damit oft auch an private Mitsteuerung.

Deshalb reicht die übliche Debatte über „mehr Effizienz“ oder „mehr Datenschutz“ nicht aus. Effizienz ist in diesen Infrastrukturen nie neutral; sie entscheidet darüber, welche Daten anschlussfähig werden, welche Stellen Zugriff erhalten und welche Lebensbereiche in dieselbe operative Logik gezogen werden. Datenschutz wiederum bleibt notwendig, aber er greift zu kurz, wenn die eigentliche Machtverschiebung in Architekturen, Standards, Beschaffungslogiken und unsichtbaren Bewertungsroutinen liegt.

Der Bericht zu algorithmic accountability im öffentlichen Sektor nennt dafür die naheliegenden, bisher aber auffallend schwach institutionalisierten Gegenmittel: Transparenz, Folgenabschätzungen, Audits, unabhängige Aufsicht, Anhörungsrechte und Beschaffungsbedingungen. Dass solche Instrumente heute wie Notmaßnahmen wirken, ist bereits Teil der Diagnose.

Nicht einzelne KI-Tools verändern den Staat, sondern die Tatsache, dass Polizei, Grenze, Militär und zivile Verwaltung ihre operative Arbeit zunehmend als Plattformbetrieb organisieren. Was als technischer Fortschritt verkauft wird, ist in Wahrheit ein Umbau des Regierens selbst: weg von punktueller Reaktion, hin zu permanenter Verknüpfung, Vorprüfung und Priorisierung. Der moderne Staat verschwindet nicht im Digitalen. Er wird dort neu gebaut. Die offene Frage ist nicht, ob er dadurch leistungsfähiger wird, sondern ob eine Demokratie, die sich immer tiefer in unsichtbare Infrastrukturen einlässt, am Ende noch weiß, wie sie sich selbst vor der totalitären Übernahme schützen soll.

Akteure, die den Staat schleichend übernehmen, brauchen Zugang zu Parteien, Ministerien, Aufsichtsbehörden und öffentliche Deutungsmilieus. Wie Wahlkampfspenden, Think-Tank-Netzwerke, Personalverflechtungen, regulatorische Einflussnahme und die Nähe zu

bestimmten politischen Lagern – bis hin zu den religiös aufgeladenen Weltbildern des christlichen Fundamentalismus die Macht der Tech-Giganten festigen und sich exzessiver Reichtum in politische Strukturmacht übersetzt, davon handelt der 4. Teil dieser Serie.

Titelbild: wacomka/shutterstock.com

**Mehr zum Thema:**

„Technofeudalismus” – das Weltbild: Freiheit, Mensch und Macht (Serie, Teil 1)

„Technofeudalismus“ – das Geschäftsmodell der Macht: Monopol, Risiko-Kapital und Plattformökonomie (Serie, Teil 2)

---

[«1] P20/20 Im Ergebnis des Programms P20 sollen die circa 320.000 Polizeibeschäftigten jederzeit und überall Zugriff auf die Informationen haben.

[«2] Shared Biometric Matching Service (sBMS) ist nur einer der Bausteine der vorgesehenen Interoperabilitätsarchitektur. Es ist ein gemeinsamer biometrischer Abgleichdienst, der horizontale, standardisierte biometrische Funktionen für verschiedene groß angelegte Informationssysteme bereitstellt – die totale Vernetzung.

[«3] EES – Das europäische Ein- und Ausreisesystem – EU-Datenbank als grund- und menschenrechtliche Herausforderung

[«4] ETIAS – Automatisierte Verdächtigung

[«5] Die Telematikinfrastruktur (TI) soll alle Beteiligten im Gesundheitswesen miteinander vernetzen.

[«6] AW – Automatisierte Entscheidungen und Teilhabe in Deutschland (2019)

[«7] PreMAP – Software zur Vorhersage von Einbruchskriminalität (wo könnte als Nächstes etwas passieren?)

[«8] KrimPro – Allgemeines System für statistische Vorhersagen von Straftaten

[«9] KLB-operativ Tool zur aktuellen Lageanalyse (wo passiert gerade was, wo muss Polizei hin?

[«10] SKALA – Prognose von Kriminalitätsbrennpunkten sowie die Effizienz und Effektivität polizeilicher Interventionen

[«11] DAR – Gotham basiert (Analysetool der US-Firma Palantir)

[«12] iTE = *Islamist Terrorists in Europe* – *Automatisierte Ungerechtigkeit*

[«13] Egbert, S.; Krasmann, S. (2019): *Predictive Policing. Eine ethnographische Studie…*, Universität Hamburg.

[«14] Das gesamte ETIAS-Ökosystem ist komplex und besteht aus der von Frontex betriebenen ETIAS-Zentrale, den ETIAS-Nationalstellen in 30 europäischen Ländern und dem von eu-LISA entwickelten und gepflegten groß angelegten Informationssystem.

[«15] CCC: Ohne Transparenz kein Vertrauen in elektronische Patientenakte

[«16] ENAR Ethnische Profilerstellung führt zu übermäßiger Polizeipräsenz gegenüber Minderheiten und deren Gemeinschaften.

[«17] AI-Report Automated Racism: Der Einsatz von Vorhersage- und Profilingsystemen zur gezielten Überwachung geografischer Gebiete sowie von Einzelpersonen und Gemeinschaften kann die Fähigkeit und Bereitschaft der Menschen, ihr Recht auf Vereinigungs- und Versammlungsfreiheit wahrzunehmen, erheblich beeinträchtigen.

[«18] GPAI (2024): “Algorithmic Transparency in the Public Sector: A state-of-the-art report of algorithmic transparency instruments”. Report, May 2024, Global Partnership on Artificial Intelligence

[«19] Transparency International: Algorithmic transparency and accountability