https://farid.ps/articles/industrialization_of_profiling/de.html

Von Personen von Interesse zu Bevölkerungen: Die Industrialisierung des Profilings

Das Aufkommen des Profilings – vom gezielten, manuellen Prüfen spezifischer „Personen von Interesse“ hin zur automatisierten, kontinuierlichen Überwachung ganzer Bevölkerungen – stellt eine der tiefgreifendsten Transformationen in der Ausübung von Macht, der Rolle der Technologie und den Grenzen individueller Autonomie dar. Was einst erheblichen menschlichen Aufwand, institutionelle Priorisierung und bewusste Auswahl erforderte, hat sich zu einer nahtlosen Infrastruktur entwickelt, die Verhaltensdaten von Milliarden Menschen in Echtzeit erzeugt, aggregiert und analysiert – oft als zufälliges Nebenprodukt des alltäglichen Lebens.

Diese Transformation war nicht allein durch die Technologie vorbestimmt. Sie entstand aus dem Zusammenspiel bürokratischer Expansion, wiederholter Sicherheitskrisen, wirtschaftlicher Anreize durch die Monetarisierung von Daten und dem unaufhaltsamen Rückgang der Grenzkosten für Datenerfassung, -speicherung und -auswertung. Das Ergebnis ist nicht einfach „mehr Überwachung“, sondern ein qualitativ anderes Regime: eines, das natürliche Reibung durch reibungslose Skalierung, menschliches Ermessen durch algorithmische Automatisierung und die Ausnahmeverdächtigung Weniger durch die grundlegende Beobachtung Vieler ersetzt.

Im Kern liegt eine fundamentale Metamorphose: Das Profiling hat sich von einem **handwerklichen Handwerk** – selektiv, arbeitsintensiv und erklärend – zu einem **industriellen Prozess** – universal, automatisiert und prädiktiv – gewandelt. Das Folgende zeichnet diese Transformation nach und identifiziert die Momente, in denen Beschränkungen erodierten und neue Fähigkeiten zu einem System kontinuierlicher, bevölkerungsweiter Inferenz kristallisierten.

I. Grundlagen: Profiling als selektive, manuelle Praxis

Profiling umfasst in seiner grundlegendsten Form die systematische Sammlung und Interpretation von Informationen, um Eigenschaften zu erschließen, Verhalten vorherzusagen oder Risikokategorien zuzuweisen. Seine Ursprünge reichen tief in die Antike zurück.

Antike Reiche führten Volkszählungen nicht nur zur Besteuerung oder Rekrutierung durch, sondern auch zur Klassifizierung. Römische Behörden und chinesische kaiserliche Administratoren sortierten Bevölkerungen nach Beruf, Loyalität und Status und erstellten frühe relationale Karten, die potenzielle Bedrohungen identifizieren konnten. Religiöse Institutionen führten Aufzeichnungen über Geburten, Eheschließungen, Beichten und morali-

sches Verhalten und schufen proto-soziale Graphen, die Netzwerke von Einfluss und Abweichung offenbarten.

Diese Systeme teilten jedoch eine entscheidende Beschränkung: **Information war teuer**. Das Sammeln, Überprüfen, Speichern und Interpretieren von Daten erforderte erhebliche menschliche Arbeit. Infolgedessen blieb Profiling **selektiv, episodisch und begrenzt**. Es konzentrierte sich auf Eliten, Dissidenten oder strategisch relevante Gruppen – nicht auf ganze Bevölkerungen.

In der frühen Neuzeit in Europa hielt diese Selektivität an, selbst als Staaten ihren Überwachungsapparat ausweiteten. Nachrichtendienste zielten auf Ketzer, politische Rivalen, Schmuggler und ausländische Agenten ab, mittels Informanten, abgefangener Korrespondenz und physischer Überwachung. Die *Cabinets noirs* – oder Schwarzen Kammern – Frankreichs und anderer Staaten verkörperten diesen Ansatz: Teams von Schreibern öffneten Briefe manuell, kopierten sie und versiegelten sie erneut für die Zustellung. Diese Operationen waren von Natur aus beschränkt. Sie konzentrierten sich auf hochwertige Ziele, da alles Breiteres logistisch unmöglich war.

Selbst in dieser Phase war die Macht der **Metadaten** klar verstanden. Informationen über die Kommunikation – Absender, Empfänger, Zeitpunkt und Route – konnten Netzwerke und Absichten offenbaren, ohne Zugang zum Inhalt zu erfordern. Der britische Postspionageskandal von 1844 brachte dies scharf ins öffentliche Bewusstsein. Der italienische Revolutionär Giuseppe Mazzini, ein Exilant in London, vermutete, dass seine Briefe von den Behörden auf Ersuchen ausländischer Mächte geöffnet wurden. Er und seine Anhänger legten Mohnsamen und Sandkörner in die Umschläge als Markierungen; als die Briefe gestört ankamen, veranlasste Mazzini den radikalen Abgeordneten Thomas Duncombe, die Angelegenheit im Parlament zur Sprache zu bringen. Der daraus resultierende Skandal enthüllte systematische Brieföffnung aufgrund von Anordnungen des Innenministers Sir James Graham, löste Empörung, parlamentarische Untersuchungen und schließlich die Abschaffung der geheimen Abteilung des Postamts aus. Er markierte eine der ersten modernen Datenschutzpaniken und unterstrich, wie relationale Daten allein Assoziationsnetzwerke zerschlagen konnten.

Als Reaktion entstanden rechtliche Normen wie die „Briefgeheimnis“ (*Briefgeheimnis*, *secret de la correspondance*). Diese Prinzipien beschränkten die Nutzung von Kommunikationsdaten strikt auf betriebliche Zwecke wie die Zustellung und verboten die sekundäre Ausbeutung zur Überwachung oder zum Profiling. Die zugrunde liegende Idee war einfach, aber tiefgreifend:

> Daten, die für einen bestimmten Zweck erzeugt wurden, sollten nicht umgewidmet werden, um breitere Profile von Personen oder Netzwerken zu erstellen.

Dieses Prinzip sollte sich über Jahrhunderte hinweg wiederholen – doch letztlich unter technologischem und institutionellem Druck erodieren.

II. Das bürokratische Jahrhundert: Skalierung ohne Automatisierung

Das 20. Jahrhundert erweiterte das Profiling dramatisch, während es viele seiner früheren Beschränkungen beibehielt. Die Anforderungen des totalen Krieges erforderten eine beispiellose Informationsbeschaffung. Postzensur, Signalaufklärung und Codeknacken dehnten die Überwachung über Eliten hinaus auf breitere Bevölkerungsgruppen aus. Institutionen wie die National Security Agency institutionalisierten großflächige Abfangmaßnahmen, während inländische Behörden umfangreiche Akten über politische Gruppen, mutmaßliche Radikale und kriminelle Netzwerke anlegten.

Dennoch blieb Profiling **grundsätzlich gezielt**. Abhöraktionen waren an bestimmte Personen oder Leitungen gebunden. Geheimdienstakten wurden von menschlichen Analysten kuratiert. Selbst bei steigendem Volumen blieb **menschliche Aufmerksamkeit der Engpass**.

Frühe Computersysteme (1950er–1970er Jahre) begannen, den Umfang der Aktenführung zu verändern. Regierungen und Unternehmen digitalisierten Sozialhilferollen, Kreditgeschichten und Strafregister und ermöglichten schnellere Abfragen und Querverweise. Doch diese Systeme arbeiteten weiterhin mit **diskreten Datensätzen**, nicht mit kontinuierlichen Verhaltensströmen.

Bis in die 1970er Jahre führten Bedenken gegenüber zentralisierten „Datenbanken“ zu rechtlichen Reaktionen. Der US-Privacy Act von 1974 und frühe europäische Datenschutzgesetze führten Prinzipien der Zweckbindung, Datenminimierung und Transparenz ein. Diese Rahmenwerke erweiterten die Logik der Briefgeheimnis auf das digitale Zeitalter.

Sie basierten jedoch auf einer entscheidenden Annahme: dass die Datenerhebung **begrenzt und episodisch** sei. Sie regelten Datensätze – nicht Flüsse. Diese Annahme sollte bald zusammenbrechen.

III. Der Wendepunkt: Von Datensätzen zu Datenschutt

Der entscheidende Bruch erfolgt Ende der 1990er und Anfang der 2000er Jahre mit dem Aufstieg des Internets – nicht nur als Kommunikationsmedium, sondern als Infrastruktur, die kontinuierlich Daten erzeugt.

Digitale Systeme erzeugen **Datenschutt**: Metadaten, die automatisch als Nebenprodukt gewöhnlicher Aktivitäten entstehen. Jede Verbindung, Abfrage, jeder Klick und jede Bewegung erzeugt Spuren, die mit vernachlässigbaren Kosten protokolliert, gespeichert und analysiert werden können.

Dies markiert den entscheidenden Wandel:

> Profiling hört auf, eine Tätigkeit zu sein, die *auf* Daten ausgeübt wird, und wird zu einer Infrastruktur, die sie kontinuierlich *erzeugt*.

Internetdienstanbieter erfassen Verbindungsprotokolle, DNS-Abfragen und Routing-Informationen und offenbaren Verhaltensmuster, selbst ohne Zugriff auf Inhalte. Im Gegensatz zu postalischen Metadaten – flüchtig und dezentralisiert – sind digitale Metadaten persistent, zentralisiert und trivial durchsuchbar.

Auf dieser Infrastruktur bauten Plattformen wie Google und Meta das Profiling zu einem zentralen Wirtschaftsmodell aus. Suchmaschinen erfassen Absichten; soziale Netzwerke kartieren Beziehungen; mobile Ökosysteme verfolgen Bewegungen. Eingebettete Tracker erweitern die Sichtbarkeit über weite Teile des Webs. Metas Tracking-Pixel, die auf etwa einem Drittel der weltweit populären Websites vorhanden sind, überwachen Aktivitäten weit über die eigenen Plattformen hinaus und erfassen oft sensible Signale aus Gesundheits-, Finanz- oder politischen Kontexten.

In dieser Umgebung entsteht eine entscheidende Erkenntnis:

> Inhalt wird weitgehend redundant. In vielen Fällen sind relationale Muster nicht nur Stellvertreter für Bedeutung – sie sind analytisch nützlicher als der Inhalt selbst.

Metadaten zeigen nicht nur an, dass Kommunikation stattfand; sie ermöglichen die **probabilistische Rekonstruktion von Inhalten**. Wer mit wem kommuniziert, wann, wie oft und in welchem breiteren Kontext, kann stark einschränken, was kommuniziert wird. Öffentlich verfügbare Informationen – geteilte Zugehörigkeiten, berufliche Rollen, politische Positionen, soziale Bindungen – verengen den Raum plausibler Interpretationen weiter.

Mit der Zeit werden diese Einschränkungen prädiktiv. Metadaten sind nicht nur deskriptiv; sie sind generativ. Sie begleiten Inhalte nicht nur – sie können sie oft **annähern oder ableiten**, insbesondere bei Aggregation in großem Maßstab.

Suchanfragen offenbaren Absichten. Kommunikationshäufigkeit offenbart Beziehungsstärke. Co-Location offenbart Assoziation. Bei ausreichendem Maßstab konvergieren diese Signale zu hochpräzisen Verhaltensmodellen, die den direkten Zugriff auf Inhalte häufig überflüssig machen.

Unternehmenssysteme optimieren Verhalten zur Monetarisierung; Staatssysteme beschränken es zur Kontrolle – doch beide stützen sich auf dieselbe zugrunde liegende Maschinerie: **Vorhersage durch großflächige Verhaltensinferenz**.

IV. Identität ohne Flucht: Persistente Anker

Ein definierendes Merkmal des industriellen Profilings ist das Entstehen einer **persistenten Identität**.

Frühere Systeme verließen sich auf veränderliche Identifikatoren – Namen, Dokumente, Adressen –, die geändert oder verschleiert werden konnten. Moderne Systeme rekonstruieren Identität durch überlappende Signale:

- Geräte-Fingerprints

- Verhaltensmuster
- Soziale Graphen
- Biometrische Marker (Gesichter, Gang, Stimme)

Öffentlich geteilte Bilder dienen als dauerhafte Anker. Selbst wenn Personen Konten wechseln oder Pseudonyme annehmen, können Gesichtserkennungssysteme – insbesondere in staatlichen oder nachrichtendienstlichen Kontexten – Identitäten über Datensätze hinweg wieder verbinden. Das gemeinsame Auftreten in Fotos oder bei geteilten Ereignissen stärkt abgeleitete Beziehungen weiter.

Die Implikation ist tiefgreifend:

> Identität ist nicht mehr etwas, das man erklärt, sondern etwas, das kontinuierlich abgeleitet wird.

Dies beseitigt einen Großteil der Reibung, die früher die Überwachung einschränkte. Die Identifizierung hängt nicht von einem einzelnen Signal ab; sie entsteht aus Redundanz über viele hinweg.

V. Fusion: Von Datenpunkten zu Ontologien

Der Höhepunkt dieser Entwicklung ist die **Datenfusion**: die Integration disparater Datensätze in einheitliche Analysesysteme.

Plattformen wie Palantir Technologies aggregieren Regierungsakten, Finanztransaktionen, Social-Media-Aktivitäten, Standortdaten und Kommunikationsmetadaten zu kohärenten Modellen von Personen und Netzwerken. Diese Systeme erstellen dynamische Ontologien, die Analysten ermöglichen, Beziehungen abzufragen, Muster zu erkennen und Vorhersagen zu generieren.

Ein konkretes Beispiel veranschaulicht den Wandel. In der Einwanderungsvollstreckung füllt Palantirs Tool „Enhanced Leads Identification and Targeting for Enforcement“ (ELITE) Karten mit potenziellen Zielen, die aus Visadaten, Beschäftigungsdaten, Telefonmetadaten, sozialen Verbindungen und sogar Medicaid- oder HHS-Adressinformationen gespeist werden, um „Adressvertrauenswerte“ zuzuweisen und Dossiers zu generieren. Beamte können „zielreiche“ Viertel für Operationen identifizieren und Personen markieren, nicht allein aufgrund direkter Beweise, sondern weil ihre **verhaltens- und relationsbezogene Signatur** zuvor identifizierten Fällen ähnelt. Ähnliche Fusion findet sich in Tools wie ImmigrationOS, die Reisehistorien, Biometriedaten und soziale Daten zur Priorisierung integrieren.

Verdacht wird nicht mehr entdeckt – er wird **erzeugt**.

Profiling dokumentiert die Realität nicht nur; es konstruiert sie aktiv, indem es probabilistische Assoziationen hervorhebt, die operationell handhabbar werden.

VI. Von der Erklärung zur Prävention

Traditionelles Profiling war weitgehend retrospektiv. Es suchte vergangene Handlungen zu erklären – wer ein Verbrechen begangen hat, wer eine Verschwörung organisiert hat, wer eine Bedrohung darstellte.

Industrielles Profiling ist prädiktiv und präventiv. Es identifiziert:

- Wer möglicherweise ein Verbrechen begehen wird
- Wo Verbrechen möglicherweise stattfinden werden
- Wer möglicherweise in Verzug gerät, radikalisiert wird oder abweicht

Diese Logik wird oft mit der Vision in *Minority Report* verglichen, in der Personen verhaftet werden, bevor sie Verbrechen begehen. Während zeitgenössische Systeme keine deterministische Voraussicht besitzen, ist die strukturelle Ähnlichkeit klar: Predictive-Policing-Tools analysieren historische Daten, 911-Anrufe, Kennzeichenleser und soziale Signale, um „Heat Lists“ oder Risikoscores zu generieren.

Moderne Systeme operieren mit Wahrscheinlichkeit. Personen werden nicht markiert, weil sie handeln werden, sondern weil sie **statistisch anderen ähneln, die es getan haben**.

Der Wandel ist subtil, aber tiefgreifend:

> Individuen werden nicht mehr primär nach ihren Handlungen beurteilt, sondern nach ihrer Position in einer probabilistischen Landschaft.

Verdacht wird strukturell – kontinuierlich erzeugt statt durch diskrete Ereignisse ausgelöst.

VII. Recht im Zeitalter der Inferenz

Rechtliche Rahmenwerke wie die Datenschutz-Grundverordnung versuchen, Grenzen durch Einwilligung, Transparenz und Minimierung zu setzen. Dennoch stoßen sie auf strukturelle Beschränkungen.

Die meisten Rechtssysteme regulieren **Daten als Objekt**. Modernes Profiling bezieht seine Macht aus **Beziehungen und Inferenzen**, die weitaus schwerer zu definieren, zu beobachten oder einzuschränken sind.

Zusätzliche Herausforderungen umfassen:

- Kontinuierliche Datenflüsse über Jurisdiktionen hinweg
- Breite Ausnahmen für die nationale Sicherheit und „berechtigte Interessen“
- Undurchsichtige algorithmische Systeme, die sich der Aufsicht widersetzen

Das Ergebnis ist eine anhaltende Diskrepanz:

> Rechtliche Rahmenwerke, die für das Zeitalter der Datensätze konzipiert wurden, kämpfen damit, das Zeitalter der kontinuierlichen, prädiktiven Inferenz zu regieren.

VIII. Die Asymmetrie der Macht

Industrielles Profiling erzeugt ein strukturelles Ungleichgewicht.

Individuen erzeugen kontinuierlich Daten durch die Teilnahme am modernen Leben. Vermeidung ist möglich, aber kostspielig und unvollständig. Gleichzeitig:

- Unterhalten Unternehmen undurchsichtige Systeme, die durch Geheimhaltung geschützt sind
- Greifen Staaten über rechtliche Befugnisse oder Partnerschaften auf Daten zu und integrieren sie
- Verschleiert technische Komplexität die Verantwortlichkeit

Das Ergebnis ist eine klare Asymmetrie:

> Die Vielen werden lesbar gemacht; die Mächtigen bleiben vergleichsweise undurchsichtig.

IX. Internalisierung: Profiling und die Selbstregulierung des Verhaltens

Jenseits seiner institutionellen und technologischen Dimensionen erzeugt die Industrialisierung des Profilings eine tiefgreifende psychologische Transformation. Überwachung wirkt nicht mehr ausschließlich als äußere Kraft; sie wird internalisiert.

Diese Dynamik wurde von Michel Foucault in seiner Analyse des Panopticons vorweggenommen: eines theoretischen Gefängnisdesigns von Jeremy Bentham, bei dem Insassen einen zentralen Beobachter sehen, den sie selbst nicht sehen können, und dadurch Disziplin internalisieren und ihr eigenes Verhalten unter der Unsicherheit ständiger Beobachtung regulieren. Die Macht des Panopticons liegt nicht in der permanenten Beobachtung, sondern in der **Antizipation** derselben.

Industrielles Profiling erweitert diese Logik dramatisch. Individuen agieren in Umgebungen, in denen Handlungen aufgezeichnet, analysiert und auf undurchsichtige Weise interpretiert werden können – von Plattformen, die Engagement optimieren, oder Staaten, die Risiken bewerten. Das Ergebnis ist ein Wandel hin zur **Selbstregulierung**.

Dies äußert sich in:

- Selbstzensur bei Posts, Suchanfragen oder Assoziationen
- Vermeidung bestimmter Gruppen, Themen oder Orte
- Anpassung an wahrgenommene Normen, um Risikoscores zu minimieren
- Verhaltensänderung über digitale und physische Kontexte hinweg

Entscheidend ist, dass diese Anpassungen keine explizite Zwangsausübung erfordern. Sie entstehen aus der Antizipation.

> Kontrolle wird nicht nur durch das ausgeübt, was Systeme tun, sondern durch das, was Individuen vermeiden zu tun.

Die Effekte gehen über Individuen hinaus. Während Menschen sich selbst zensieren und selbst sortieren, verstärken die erzeugten Daten Muster und formen zukünftige Vorhersagen. Das System beobachtet die Realität nicht nur – es formt sie subtil um und schafft Feedback-Schleifen, die Konformität normalisieren.

X. Das Ende der selektiven Überwachung

Profiling hat eine fundamentale Transformation durchlaufen:

- Von **gezielt** zu **universal**
- Von **manuell** zu **automatisiert**
- Von **retrospektiv** zu **prädiktiv**
- Von **fragmentiert** zu **integriert**

Frühere Systeme waren durch Reibung beschränkt – Kosten, Zeit, menschliche Aufmerksamkeit. Industrielle Systeme entfernen diese Beschränkungen. Überwachung wird ambient. Inklusion wird zum Default.

Das Prinzip, dass Daten nur ihrem unmittelbaren Zweck dienen sollen, hat einem Paradigma Platz gemacht, in dem **alle Daten potenziell ausbeutbar** sind.

XI. Schluss: Der Preis der Teilhabe

Der lange Bogen von der Briefgeheimnis zur digitalen Datenfusion offenbart ein konsistentes Muster: Jede technologische Ausweitung vergrößert den Umfang des Profilings, während rechtliche und gesellschaftliche Reaktionen hinterherhinken. Was die Gegenwart auszeichnet, ist das Strukturelle. Profiling ist nicht mehr eine Tätigkeit, die sich gegen bestimmte Individuen richtet – es ist eine Infrastruktur, innerhalb derer Individuen existieren.

Die Kategorie der „Person von Interesse“ löst sich auf. Jeder wird zum Gegenstand kontinuierlicher Bewertung.

Diese Transformation wird nicht nur durch staatliche Macht aufrechterhalten, sondern auch durch wirtschaftliche Anreize. Plattformen, die frei erscheinen, funktionieren durch die Extraktion verhaltensbezogener Daten. Der Satz *„Wenn du nicht für das Produkt bezahlst, bist du das Produkt“* erfasst eine Intuition – unterschätzt jedoch die Realität.

Erzeugt wird nicht das Individuum, sondern ein **prädiktives Modell** des Individuums – portabel, handhabbar und demjenigen, den es repräsentiert, oft unzugänglich.

Eine zentrale Herausforderung liegt in der Kluft zwischen Wahrnehmung und Realität.

Erstens unterschätzen Menschen die **Auswirkung** dessen, was bekannt ist. Profiling operiert über Assoziation. Beziehungen – vergangene, schwache oder indirekte – können Ergebnisse prägen. Eine Verbindung zu jemandem, der später unerwünscht wird, kann Chancen beeinflussen. Man wird nicht nur individuell, sondern relational beurteilt.

Zweitens unterschätzen Menschen den **Umfang** dessen, was bekannt werden kann. Systeme leiten sensible Attribute – politische, religiöse, sexuelle, wirtschaftliche – nicht aus expliziter Offenlegung ab, sondern aus Mustern. Diese Inferenzen werden operational, unabhängig von ihrer Genauigkeit.

> Individuen werden nicht nur danach bewertet, was sie offenbaren, sondern danach, was abgeleitet werden kann – und danach, mit wem sie verbunden sind.

Die Teilhabe am digitalen Leben beinhaltet somit einen impliziten Tausch: Bequemlichkeit gegen Lesbarkeit. Dieser Tausch ist weder transparent noch verhandelbar.

Die Herausforderung besteht nicht darin, die Datafizierung aufzuhalten, sondern sie einzuschränken – Reibung wiederherzustellen, Grenzen durchzusetzen und Verantwortlichkeit sicherzustellen.

Die zentrale Frage ist klar:

> Wird ein Eingreifen erfolgen, bevor die Infrastruktur des permanenten Profilings zu tief verankert ist, um sie sinnvoll herauszufordern?

Ohne ein solches Eingreifen besteht der Preis der Teilhabe nicht nur aus Daten – sondern aus der allmählichen Erosion der Grenze zwischen Beobachtetwerden, Abgeleitetwerden und letztlich Definiertwerden.