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

Från personer av intresse till befolkningar: Industrialiseringen av profilering

Framväxten av profilering – från riktad, manuell granskning av specifika ”personer av intresse” till automatiserad, kontinuerlig övervakning av hela befolkningar – utgör en av de mest djupgående förändringarna i utövandet av makt, teknikens roll och gränserna för individuell autonomi. Det som en gång krävde betydande mänsklig ansträngning, institutionell prioritering och medvetet urval har utvecklats till en sömlös infrastruktur som genererar, samlar och analyserar beteendedata på miljarder människor i realtid, ofta som en oavsiktlig biprodukt av vardagslivet.

Denna förändring var inte förutbestämd av tekniken ensam. Den uppstod ur samspelet mellan byråkratisk expansion, upprepade säkerhetskriser, ekonomiska incitament kopplade till datamonetisering och den obevekliga minskningen av marginalkostnaden för datainsamling, lagring och slutledning. Resultatet är inte bara ”mer övervakning”, utan ett kvalitativt annorlunda regim: ett som ersätter naturlig friktion med friktionsfri skala, mänskligt omdöme med algoritmisk automatisering och exceptionell misstanke mot de få med grundläggande observation av de många.

I dess kärna ligger en fundamental metamorfos: profilering har förskjutits från en **hantverksmässig yrkesutövning** – selektiv, arbetsintensiv och förklarande – till en **industriell process** – universell, automatiserad och prediktiv. Det följande spårar denna förändring, identifierar de ögonblick där begränsningarna eroderade och nya förmågor kristalliserades till ett system för kontinuerlig, befolkningsomfattande slutledning.

I. Grunderna: Profilering som selektiv, manuell praxis

Profilering, i sin mest grundläggande form, innebär systematisk insamling och tolkning av information för att dra slutsatser om egenskaper, förutsäga beteende eller tilldela kategorier av risk. Dess ursprung sträcker sig djupt in i antiken.

Forntida imperier genomförde folkräkningar inte bara för beskattning eller utskrivning, utan även för klassificering. Romerska myndigheter och kinesiska kejserliga administratörer sorterade befolkningar efter yrke, lojalitet och status, vilket skapade tidiga relationella kartor som kunde identifiera potentiella hot. Religiösa institutioner förde register över födslar, äktenskap, bekännelser och moraliskt beteende, vilket konstruerade proto-sociala grafer som avslöjade nätverk av inflytande och avvikelse.

Ändå delade dessa system ett avgörande villkor: **information var dyr**. Insamling, verifiering, lagring och tolkning av data krävde betydande mänskligt arbete. Som ett resultat förblev profilering **selektiv, episodisk och avgränsad**. Den fokuserade på eliter, dissidenter eller strategiskt relevanta grupper – inte hela befolkningar.

I det tidigmoderna Europa fortsatte denna selektivitet även när staterna utvidgade sin övervakningsapparat. Underrättelseinsatser riktade sig mot kättare, politiska rivaler, smugglare och utländska agenter genom informatörer, avlyssnad korrespondens och fysisk övervakning. De franska och andra staters *cabinets noirs* – eller svarta kammare – exemplifierade detta tillvägagångssätt: team av skrivare öppnade brev manuellt, kopierade dem och förseglade dem igen för leverans. Dessa operationer var till sin natur begränsade. De fokuserade på högvärdiga mål eftersom allt bredare var logistiskt omöjligt.

Redan på detta stadium förstods dock **metadata**s kraft tydligt. Information om kommunikation – avsändare, mottagare, tidpunkt och väg – kunde avslöja nätverk och avsikter utan att kräva tillgång till innehållet. Den brittiska postkontorets spionageskandal 1844 förde detta i skarpt offentligt fokus. Den italienske revolutionären Giuseppe Mazzini, i exil i London, misstänkte att hans brev öppnades av myndigheterna på begäran av utländska makter. Han och hans anhängare placerade vallmofrön och sandkorn i kuverten som markörer; när breven anlände störda, uppmanade Mazzini den radikale parlamentsledamoten Thomas Duncombe att ta upp frågan i parlamentet. Den efterföljande skandalen avslöjade systematisk brevöppning under order utfärdade av inrikesministern Sir James Graham, vilket väckte indignation, parlamentariska utredningar och så småningom avskaffandet av postkontorets hemliga avdelning. Det markerade en av de första moderna integritetspanikerna och underströk hur relationsdata ensamt kunde riva upp nätverk av associationer.

Som svar uppstod rättsliga normer som ”korrespondensens sekretess” (*Briefgeheimnis*, *secret de la correspondance*). Dessa principer begränsade användningen av kommunikationsdata strikt till operativa syften som leverans, och förbjöd sekundär exploatering för övervakning eller profilering. Den underliggande idén var enkel men djup:

> Data som genereras för ett specifikt syfte bör inte återanvändas för att konstruera bredare profiler av individer eller nätverk.

Denna princip skulle eka genom århundradena – men till slut erodera under teknologiskt och institutionellt tryck.

II. Det byråkratiska seklet: Skalning utan automatisering

Det tjugonde århundradet expanderade profileringen dramatiskt samtidigt som många av dess tidigare begränsningar bibehölls. Kraven från totalt krig krävde en aldrig tidigare skådad informationsinsamling. Brevcensur, signalunderrättelse och kodknäckning utvidgade övervakningen bortom eliter till bredare befolkningar. Institutioner som National Security Agency institutionaliserade storskalig avlyssning, medan inhemska myndigheter sammanställde omfattande filer om politiska grupper, misstänkta radikaler och kriminella nätverk.

Ändå förblev profileringen **i grunden riktad**. Avlyssning knöts till specifika individer eller linjer. Underrättelsefiler kuraterades av mänskliga analytiker. Även när volymen ökade förblev **mänsklig uppmärksamhet flaskhalsen**.

Tidiga datasystem (1950-talet–1970-talet) började förändra skalan för registerhantering. Regeringar och företag digitaliserade välfärdsregister, kreditregister och brottsdatabaser, vilket möjliggjorde snabbare hämtning och korsreferering. Men dessa system arbetade fortfarande med **diskreta register**, inte kontinuerliga beteendeströmmar.

På 1970-talet ledde oro över centraliserade ”databanker” till rättsliga svar. Den amerikanska Privacy Act från 1974 och tidiga europeiska dataskyddslagar införde principer om syftesbegränsning, dataminimering och transparens. Dessa ramverk utvidgade logiken från korrespondenssekretess till den digitala eran.

De byggdes dock på en avgörande antagande: att datainsamling var **avgränsad och episodisk**. De reglerade register – inte flöden. Detta antagande skulle snart kollapsa.

III. Inflektionspunkten: Från register till dataexhaust

Det avgörande brottet inträffar i slutet av 1990-talet och början av 2000-talet med internets framväxt – inte bara som ett kommunikationsmedium, utan som en infrastruktur som kontinuerligt producerar data.

Digitala system genererar **dataexhaust**: metadata som skapas automatiskt som en biprodukt av vanlig aktivitet. Varje anslutning, sökning, klick och rörelse producerar spår som kan loggas, lagras och analyseras till försumbar kostnad.

Detta markerar det avgörande skiftet:

> Profilering upphör att vara en aktivitet som utförs på data och blir en infrastruktur som kontinuerligt producerar den.

Internetleverantörer fångar anslutningsloggar, DNS-frågor och routningsinformation, vilket avslöjar beteendemönster även utan tillgång till innehåll. Till skillnad från postmetadata – flyktig och decentraliserad – är digital metadata beständig, centraliserad och trivialt sökbar.

Ovanpå denna infrastruktur förvandlade plattformar som Google och Meta profilering till en kärnekonomisk modell. Sökmotorer fångar avsikt; sociala nätverk kartlägger relationer; mobila ekosystem spårar rörelse. Inbäddade trackers utvidgar synligheten över stora delar av webben. Metas tracking pixels, närvarande på ungefär en tredjedel av världens populära webbplatser, övervakar aktivitet långt utanför dess egna plattformar, ofta genom att fånga känsliga signaler från hälsosammanhang, finans eller politik.

En kritisk insikt uppstår i denna miljö:

> Innehåll blir i stor utsträckning överflödigt. I många fall är relationsmönster inte bara proxies för mening – de är mer analytiskt användbara än innehållet självt.

Metadata indikerar inte bara att kommunikation ägde rum; den möjliggör **probabilistisk rekonstruktion av innehållet**. Vem som kommunicerar med vem, när, hur ofta och inom

vilket bredare sammanhang kan starkt begränsa vad som kommuniceras. Offentligt tillgänglig information – delade tillhörigheter, yrkesroller, politiska positioner, sociala band – minskar ytterligare utrymmet för plausibla tolkningar.

Med tiden blir dessa begränsningar prediktiva. Metadata är inte bara beskrivande; den är generativ. Den åtföljer inte bara innehåll – den kan ofta **approximera eller inferera det**, särskilt när den aggregeras i stor skala.

Sökfrågor avslöjar avsikt. Kommunikationsfrekvens avslöjar relationsstyrka. Samlokalisering avslöjar association. Vid tillräcklig skala konvergerar dessa signaler till högst exakta beteendemodeller som ofta gör direkt innehållsåtkomst onödig.

Företagsystem optimerar beteende för monetisering; statliga system begränsar det för kontroll – men båda förlitar sig på samma underliggande maskineri: **prediktion genom storskalig beteendeinferens**.

IV. Identitet utan flykt: Beständiga ankare

En definierande egenskap hos industriell profilering är framväxten av **beständig identitet**.

Tidigare system förlitade sig på föränderliga identifierare – namn, dokument, adresser – som kunde ändras eller döljas. Moderna system rekonstruerar identitet genom överlappande signaler:

- Enhetsfingeravtryck
- Beteendemönster
- Sociala grafer
- Biometriska markörer (ansikten, gång, röst)

Offentligt delade bilder fungerar som hållbara ankare. Även när individer byter konton eller antar pseudonymer kan ansiktsigenkänningssystem – särskilt i statliga eller underrättelsekontexter – återkoppla identiteter över datamängder. Samförekomst i foton eller delade händelser stärker ytterligare de infererade relationerna.

Implikationen är djupgående:

> Identitet är inte längre något man deklarerar, utan något som kontinuerligt infereras.

Detta eliminerar mycket av den friktion som en gång begränsade övervakning. Identifiering beror inte på någon enskild signal; den uppstår ur redundans över många.

V. Fusion: Från datapunkter till ontologier

Kulmen på denna utveckling är **datafusion**: integrationen av disparata datamängder till enhetliga analytiska system.

Plattformar som Palantir Technologies aggregerar statliga register, finansiella transaktioner, sociala medieaktiviteter, platsdata och kommunikationsmetadata till sammanhängande modeller av individer och nätverk. Dessa system konstruerar dynamiska ontologier som gör det möjligt för analytiker att fråga om relationer, upptäcka mönster och generera prediktioner.

Ett konkret exempel illustrerar skiftet. Inom immigrationsverkställighet fyller Palantirs verktyg Enhanced Leads Identification and Targeting for Enforcement (ELITE) kartor med potentiella mål, baserat på visumregister, anställningsdata, telefonmetadata, sociala kopplingar och till och med adresser från Medicaid eller HHS för att tilldela ”address confidence scores” och generera dossier. Tjänstemän kan identifiera ”målrika” områden för operationer, flagga individer inte enbart baserat på direkt bevis utan eftersom deras **beteendemässiga och relationella signatur** liknar tidigare identifierade fall. Liknande fusion förekommer i verktyg som ImmigrationOS, som integrerar resehistorik, biometri och sociala data för prioritering.

Misstanke upptäcks inte längre – den **genereras**.

Profilering dokumenterar inte bara verkligheten; den konstruerar den aktivt genom att lyfta fram probabilistiska associationer som blir operationellt handlingsbara.

VI. Från förklaring till preemptiv åtgärd

Traditionell profilering var i stor utsträckning retrospektiv. Den sökte förklara tidigare handlingar – vem begick ett brott, vem organiserade en konspiration, vem utgjorde ett hot.

Industriell profilering är prediktiv och preemptiv. Den identifierar:

- Vem som kan begå ett brott
- Var brott kan inträffa
- Vem som kan fallera, radikaliseras eller avvika

Denna logik jämförs ofta med visionen i *Minority Report*, där individer grips innan de begår brott. Även om samtida system saknar deterministisk framsyn är den strukturella likheten tydlig: prediktiva polisverktyg analyserar historisk data, 911-samtal, registreringsskyltsläsare och sociala signaler för att generera ”heat lists” eller riskpoäng.

Moderna system arbetar med sannolikhet. Individer flaggas inte för att de kommer att agera, utan för att de **statistiskt liknar andra som har gjort det**.

Skiftet är subtilt men djupgående:

> Individer bedöms inte längre främst utifrån sina handlingar, utan utifrån sin position i ett probabilistiskt landskap.

Misstanke blir strukturell – genereras kontinuerligt snarare än utlöst av diskreta händelser.

VII. Lagstiftning i inferensens tidsålder

Rättsliga ramverk som General Data Protection Regulation försöker införa begränsningar genom samtycke, transparens och minimering. Ändå möter de strukturella hinder.

De flesta rättssystem reglerar **data som ett objekt**. Modern profilering hämtar sin makt från **relationer och inferenser**, som är betydligt svårare att definiera, observera eller begränsa.

Ytterligare utmaningar inkluderar:

- Kontinuerliga dataflöden över jurisdiktioner
- Breda undantag för nationell säkerhet och ”berättigade intressen”
- Ogenomskinliga algoritmiska system som är resistenta mot tillsyn

Resultatet är en bestående brist på överensstämmelse:

> Rättsliga ramverk utformade för en tid av register kämpar för att styra en tid av kontinuerlig, prediktiv inferens.

VIII. Maktens asymmetri

Industriell profilering skapar en strukturell obalans.

Individer genererar data kontinuerligt genom deltagande i det moderna livet. Undvikande är möjligt men kostsamt och ofullständigt. Samtidigt:

- Upprätthåller företag ogenomskinliga system skyddade av sekretess
- Får stater tillgång till och integrerar data genom laglig myndighet eller partnerskap
- Döljer teknisk komplexitet ansvarsskyldighet

Resultatet är en tydlig asymmetri:

> De många görs läsbara; de mäktiga förblir relativt ogenomskinliga.

IX. Internalisering: Profilering och självkontroll av beteende

Utöver sina institutionella och teknologiska dimensioner producerar industrialiseringen av profilering en djup psykologisk förändring. Övervakning fungerar inte längre enbart som en extern kraft; den blir internaliserad.

Denna dynamik förutspåddes av Michel Foucault i hans analys av panoptikon: en teoretisk fängelsedesign av Jeremy Bentham där fångar, synliga för en central observatör de inte kan se, internaliserar disciplin och reglerar sitt eget beteende under osäkerheten om konstant bevakning. Panoptikonets makt ligger inte i ständig observation utan i **förväntan** om den.

Industriell profilering utvidgar denna logik dramatiskt. Individer verkar inom miljöer där handlingar kan registreras, analyseras och tolkas på ogenomskinliga sätt – av plattformar som optimerar för engagemang eller stater som bedömer risk. Resultatet är en förskjutning mot **självreglering**.

Detta manifesterar sig som:

- Självcensur i inlägg, sökningar eller associationer
- Undvikande av vissa grupper, ämnen eller platser
- Anpassning till upplevda normer för att minimera riskpoäng
- Modifiering av beteende över digitala och fysiska sammanhang

Kritiskt nog kräver dessa anpassningar inte explicit tvång. De uppstår ur förväntan.

> Kontroll utövas inte bara genom vad systemen gör, utan genom vad individer undviker att göra.

Effekterna sträcker sig bortom individer. När människor självcensurerar och själv-sorterar förstärker den genererade datan mönster, vilket formar framtida prediktioner. Systemet observerar inte bara verkligheten – det omformar den subtilt, och skapar återkopplingsslingor som normaliserar konformitet.

X. Slutet för selektiv övervakning

Profilering har genomgått en fundamental förändring:

- Från **riktad** till **universell**
- Från **manuell** till **automatiserad**
- Från **retrospektiv** till **prediktiv**
- Från **fragmenterad** till **integrerad**

Tidigare system begränsades av friktion – kostnad, tid, mänsklig uppmärksamhet. Industriella system tar bort dessa begränsningar. Övervakning blir ambient. Inkludering blir standard.

Principen att data endast ska tjäna sitt omedelbara syfte har gett vika för ett paradigm där **all data potentiellt är exploaterbar**.

XI. Slutsats: Deltagandets pris

Den långa bågen från postsekretess till digital datafusion avslöjar ett konsekvent mönster: varje teknologisk expansion ökar omfattningen av profilering, medan rättsliga och sociala svar halkar efter. Det som utmärker nutiden är det strukturella. Profilering är inte längre en aktivitet riktad mot specifika individer – det är en infrastruktur inom vilken individer existerar.

Kategorin ”person av intresse” löses upp. Alla blir föremål för kontinuerlig utvärdering.

Denna förändring upprätthålls inte bara av statlig makt, utan av ekonomiska incitament. Plattformar som verkar gratis fungerar genom beteendedataextraktion. Frasen *”om du inte betalar för produkten är du produkten”* fångar en intuition – men underskattar verkligheten.

Det som produceras är inte individen, utan en **prediktiv modell** av individen – portabel, handlingsbar och ofta otillgänglig för den person den representerar.

En central utmaning ligger i ett gap mellan perception och verklighet.

För det första underskattar människor **påverkan** av det som är känt. Profilering fungerar genom association. Relationer – tidigare, svaga eller indirekta – kan forma utfall. En koppling till någon som senare blir oönskad kan påverka möjligheter. Man bedöms inte bara individuellt, utan relationellt.

För det andra underskattar människor **omfattningen** av vad som kan kännas till. System infererar känsliga attribut – politiska, religiösa, sexuella, ekonomiska – inte från explicit avslöjande, utan från mönster. Dessa inferenser blir operationella oavsett noggrannhet.

> Individer utvärderas inte bara utifrån vad de avslöjar, utan utifrån vad som kan infereras – och utifrån vem de är kopplade till.

Deltagande i det digitala livet innebär därför ett underförstått byte: bekvämlighet mot läsbarhet. Detta byte är varken transparent eller förhandlingsbart.

Utmaningen är inte att stoppa datafieringen, utan att begränsa den – att återställa friktion, upprätthålla gränser och säkerställa ansvarsskyldighet.

Den centrala frågan är klar:

> Kommer ingripanden att ske innan infrastrukturen för permanent profilering blir för djupt inbäddad för att kunna utmanas meningsfullt?

I avsaknad av ett sådant ingripande är priset för deltagande inte bara data – utan den gradvisa erosionen av gränsen mellan att bli observerad, att bli infererad och i slutändan att bli definierad.