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

Fra personer af interesse til befolkninger: Industrialiseringen af profilering

Fremkomsten af profilering – fra målrettet, manuel granskning af specifikke „personer af interesse“ til automatiseret, kontinuerlig overvågning af hele befolkninger – repræsenterer en af de mest dybtgående transformationer i udøvelsen af magt, teknologiens rolle og grænserne for individuel autonomi. Hvad der engang krævede betydelig menneskelig indsats, institutionel prioritering og bevidst udvælgelse, har udviklet sig til en sømløs infrastruktur, der genererer, aggregerer og analyserer adfærdsdata på milliarder af mennesker i realtid, ofte som en tilfældig biprodukt af hverdagslivet.

Denne transformation var ikke forudbestemt af teknologien alene. Den opstod gennem samspillet mellem bureaukratisk ekspansion, gentagne sikkerhedskriser, økonomiske incitamenter knyttet til datamonetisering og den vedvarende reduktion i den marginale omkostning ved dataindsamling, lagring og slutning. Resultatet er ikke blot „mere overvågning“, men et kvalitativt anderledes regime: et der erstatter naturlig friktion med friktionsfri skala, menneskelig skøn med algoritmisk automatisering og undtagelsesvis mistanke om de få med baseline-observation af de mange.

I sin kerne ligger en fundamental metamorfose: profilering er skiftet fra en **håndværksmæssig praksis** – selektiv, arbejdskrævende og forklarende – til en **industriel proces** – universel, automatiseret og prædiktiv. Det følgende sporer denne transformation og identificerer de øjeblikke, hvor begrænsningerne blev eroderet, og nye kapaciteter krystalliserede sig til et system af kontinuerlig, befolkningsdækkende slutning.

I. Grundlaget: Profilering som selektiv, manuel praksis

Profilering indebærer i sin mest basale form den systematiske indsamling og fortolkning af information for at slutte karakteristika, forudsige adfærd eller tildele risikokategorier. Dens oprindelse strækker sig dybt tilbage i antikken.

Oldtidens imperier gennemførte folketællinger ikke blot til beskatning eller udskrivning, men også til klassifikation. Romerske myndigheder og kinesiske kejserlige administratorer sorterede befolkninger efter erhverv, loyalitet og status, hvilket producerede tidlige relationelle kort, der kunne identificere potentielle trusler. Religiøse institutioner førte registre over fødsler, ægteskaber, skriftemål og moralsk adfærd og konstruerede proto-sociale grafer, der afslørede netværk af indflydelse og afvigelse.

Disse systemer delte dog en afgørende begrænsning: **information var dyr**. Indsamling, verificering, lagring og fortolkning af data krævede betydelig menneskelig arbejdskraft. Som følge heraf forblev profilering **selektiv, episodisk og afgrænset**. Den fokuserede på eliter, dissidenter eller strategisk relevante grupper – ikke hele befolkninger.

I det tidlige moderne Europa fortsatte denne selektivitet, selv da staterne udvidede deres overvågningsapparat. Efterretningsindsatsen rettede sig mod kættere, politiske rivaler, smuglere og udenlandske agenter gennem informanter, opsnappede breve og fysisk overvågning. De franske og andre staters *cabinets noirs* – eller sorte kamre – eksemplificerede denne tilgang: hold af skrivere åbnede breve manuelt, kopierede dem og forseglede dem igen til levering. Disse operationer var i sagens natur begrænsede. De fokuserede på højværdimål, fordi noget bredere var logistisk umuligt.

Selv på dette stadium var magten i **metadata** imidlertid klart forstået. Information om kommunikation – afsender, modtager, tidspunkt og rute – kunne afsløre netværk og hensigter uden adgang til indholdet. Den britiske postkontors spionageskandale i 1844 bragte dette i skarpt offentligt fokus. Den italienske revolutionær Giuseppe Mazzini, i eksil i London, mistænkte, at hans breve blev åbnet af myndighederne på anmodning fra fremmede magter. Han og hans tilhængere placerede valmuefrø og sandkorn i kuverterne som markører; da brevene ankom forstyrrede, fik Mazzini den radikale parlamentsmedlem Thomas Duncombe til at rejse sagen i Parlamentet. Den efterfølgende skandale afslørede systematisk brevåbning under kendelser udstedt af indenrigsminister Sir James Graham, hvilket udløste vrede, parlamentariske undersøgelser og i sidste ende afskaffelsen af postkontorets hemmelige afdeling. Det var en af de første moderne privatlivspanikker og understregede, hvordan relationelle data alene kunne nedbryde associationsnetværk.

Som reaktion opstod juridiske normer som „brevhemmelighed“ (*Briefgeheimnis*, *secret de la correspondance*). Disse principper begrænsede brugen af kommunikationsdata strengt til operationelle formål som levering og forbød sekundær udnyttelse til overvågning eller profilering. Den underliggende idé var enkel, men dyb:

> Data genereret til et specifikt formål bør ikke genbruges til at konstruere bredere profiler af individer eller netværk.

Dette princip skulle genlyde gennem århundreder – men til sidst erodere under teknologisk og institutionelt pres.

II. Det bureaukratiske århundrede: Skalering uden automatisering

Det 20. århundrede udvidede profilering dramatisk, samtidig med at mange af de tidligere begrænsninger blev bevaret. Kravene fra total krig krævede hidtil uset informationsindsamling. Brevcensur, signalefterretning og kodebrydning udvidede overvågningen ud over eliter til bredere befolkninger. Institutioner som National Security Agency institutionaliserede storskalet aflytning, mens indenlandske myndigheder samlede omfattende filer om politiske grupper, mistænkte radikale og kriminelle netværk.

Alligevel forblev profilering **fundamentalt målrettet**. Aflytninger var knyttet til specifikke personer eller linjer. Efterretningsfiler blev kurateret af menneskelige analytikere. Selv da mængden steg, forblev **menneskelig opmærksomhed flaskehalsen**.

Tidlige computersystemer (1950'erne–1970'erne) begyndte at ændre omfanget af registerføring. Regeringer og virksomheder digitaliserede velfærdsregistre, kreditoplysninger og kriminelle databaser, hvilket muliggjorde hurtigere hentning og krydsreferencing. Men disse systemer opererede stadig på **diskrete poster**, ikke kontinuerlige strømme af adfærd.

I 1970'erne førte bekymringer om centraliserede „databanker" til juridiske reaktioner. Den amerikanske Privacy Act af 1974 og tidlige europæiske databeskyttelseslove introducerede principper om formålsbegrænsning, dataminimering og gennemsigtighed. Disse rammer udvidede logikken fra brevhemmelighed til den digitale tidsalder.

De var dog bygget på en afgørende antagelse: at dataindsamling var **afgrænset og episodisk**. De regulerede poster – ikke strømme. Denne antagelse skulle snart bryde sammen.

III. Vendepunktet: Fra poster til dataudstødning

Det afgørende brud sker i slutningen af 1990'erne og begyndelsen af 2000'erne med internettets fremkomst – ikke blot som et kommunikationsmedie, men som en infrastruktur, der kontinuerligt producerer data.

Digitale systemer genererer **dataudstødning**: metadata skabt automatisk som biprodukt af almindelig aktivitet. Hver forbindelse, forespørgsel, klik og bevægelse producerer spor, der kan logges, lagres og analyseres til ubetydelig omkostning.

Dette markerer det afgørende skift:

> Profilering ophører med at være en aktivitet udført på data og bliver en infrastruktur, der kontinuerligt producerer det.

Internetudbydere fanger forbindelseslogs, DNS-forespørgsler og routinginformation, hvilket afslører adfærdsmønstre selv uden adgang til indhold. I modsætning til post-metadata – flygtig og decentraliseret – er digital metadata vedvarende, centraliseret og trivielt søgbar.

Oven på denne infrastruktur forvandlede platforme som Google og Meta profilering til en kerneøkonomisk model. Søgemaskiner fanger hensigt; sociale netværk kortlægger relationer; mobile økosystemer sporer bevægelse. Indlejrede trackere udvider synligheden på tværs af store dele af nettet. Metas tracking-pixels, der findes på omkring en tredjedel af verdens populære websites, overvåger aktivitet langt ud over deres egne platforme og fanger ofte følsomme signaler fra sundheds-, finans- eller politiske kontekster.

En kritisk erkendelse opstår i dette miljø:

> Indhold bliver i vid udstrækning overflødigt. I mange tilfælde er relationelle mønstre ikke blot proxyer for mening – de er analytisk mere nyttige end indholdet selv.

Metadata angiver ikke blot, at kommunikation fandt sted; det muliggør **sandsynlighedsbaseret rekonstruktion af indhold**. Hvem kommunikerer med hvem, hvornår, hvor ofte og i hvilken bredere kontekst kan stærkt begrænse, hvad der kommunikeres. Offentligt tilgængelig information – delte tilhørsforhold, professionelle roller, politiske positioner, sociale bånd – indsnævrer yderligere rummet af plausible fortolkninger.

Over tid bliver disse begrænsninger prædiktive. Metadata er ikke blot deskriptivt; det er generativt. Det ledsager ikke blot indhold – det kan ofte **tilnærme eller slutte det**, især når det aggregeres i stor skala.

Søgeforespørgsler afslører hensigt. Kommunikationshyppighed afslører relationsstyrke. Samlokalisering afslører association. Ved tilstrækkelig skala konvergerer disse signaler til højpræcise adfærdsmodeler, der ofte gør direkte adgang til indhold unødvendig.

Virksomhedssystemer optimerer adfærd til monetisering; statssystemer begrænser den til kontrol – men begge er afhængige af den samme underliggende maskineri: **prædiktion gennem storskalet adfærdsslutning**.

IV. Identitet uden flugt: Vedvarende ankre

Et definerende træk ved industriel profilering er fremkomsten af **vedvarende identitet**.

Tidligere systemer stolede på mutable identifikatorer – navne, dokumenter, adresser – der kunne ændres eller skjules. Moderne systemer rekonstruerer identitet gennem overlappende signaler:

- Enhedsfingeraftryk
- Adfærdsmønstre
- Sociale grafer
- Biometriske markører (ansigter, gang, stemme)

Offentligt delte billeder fungerer som holdbare ankre. Selv når individer skifter konti eller adopterer pseudonymer, kan ansigtsgenkendelsessystemer – især i statslige eller efterretningsmæssige kontekster – genforbinde identiteter på tværs af datasæt. Samforekomst i billeder eller delte begivenheder styrker yderligere de sluttede relationer.

Implikationen er dyb:

> Identitet er ikke længere noget, man erklærer, men noget, der kontinuerligt sluttes.

Dette eliminerer meget af den friktion, der tidligere begrænsede overvågning. Identifikation afhænger ikke af et enkelt signal; den opstår gennem redundans på tværs af mange.

V. Fusion: Fra datapunkter til ontologier

Kulminationen på denne udvikling er **datafusion**: integrationen af forskellige datasæt i unifiede analytiske systemer.

Platforme som Palantir Technologies aggregerer offentlige registre, finansielle transaktioner, sociale medieaktiviteter, lokationsdata og kommunikationsmetadata til sammenhængende modeller af individer og netværk. Disse systemer konstruerer dynamiske ontologier, der tillader analytikere at forespørge relationer, opdage mønstre og generere forudsigelser.

Et konkret eksempel illustrerer skiftet. Inden for immigrationshåndhævelse fylder Palantirs værktøj Enhanced Leads Identification and Targeting for Enforcement (ELITE) kort med potentielle mål ved at trække på visumregistre, beskæftigelsesdata, telefonmetadata, sociale forbindelser og endda Medicaid- eller HHS-adresseoplysninger for at tildele „adressekonfidensscores“ og generere dossierer. Betjente kan identificere „mål-rige“ kvarterer til operationer og flagge individer ikke kun på baggrund af direkte beviser, men fordi deres **adfærdsmæssige og relationelle signatur** ligner tidligere identificerede tilfælde. Lignende fusion ses i værktøjer som ImmigrationOS, der integrerer rejsehistorik, biometri og sociale data til prioritering.

Mistanke opdages ikke længere – den **genereres**.

Profilering dokumenterer ikke blot virkeligheden; den konstruerer den aktivt ved at fremhæve sandsynlighedsbaserede associationer, der bliver operationelt handlingsrettede.

VI. Fra forklaring til præemption

Traditionel profilering var i vid udstrækning retrospektiv. Den søgte at forklare tidligere handlinger – hvem begik en forbrydelse, hvem organiserede et plot, hvem udgjorde en trussel.

Industriel profilering er prædiktiv og præemptiv. Den identificerer:

- Hvem der måske vil begå en forbrydelse
- Hvor forbrydelse måske vil finde sted
- Hvem der måske vil misligholde, radikalisere eller afvige

Denne logik sammenlignes ofte med visionen i *Minority Report*, hvor individer anholdes, før de begår forbrydelser. Selvom samtidige systemer mangler deterministisk forudseenhed, er den strukturelle lighed klar: prædiktive politiværktøjer analyserer historiske data, 911-opkald, nummerpladelæsere og sociale signaler for at generere „heat lists“ eller risikoscores.

Moderne systemer opererer på sandsynlighed. Individer flagges ikke, fordi de vil handle, men fordi de **statistisk ligner andre, der har gjort det**.

Skiftet er subtilt, men dybtgående:

> Individer dømmes ikke længere primært på deres handlinger, men på deres position i et sandsynlighedslandskab.

Mistanke bliver strukturel – genereret kontinuerligt snarere end udløst af diskrete begivenheder.

VII. Retten i inferensens tidsalder

Juridiske rammer som General Data Protection Regulation forsøger at pålægge begrænsninger gennem samtykke, gennemsigtighed og minimering. Alligevel står de over for strukturelle begrænsninger.

De fleste retssystemer regulerer **data som et objekt**. Moderne profilering henter sin magt fra **relationer og slutninger**, som er langt sværere at definere, observere eller begrænse.

Yderligere udfordringer omfatter:

- Kontinuerlige dataflow på tværs af jurisdiktioner
- Brede undtagelser for national sikkerhed og „legitime interesser“
- Uigennemsigtige algoritmiske systemer, der er resistente over for tilsyn

Resultatet er et vedvarende mismatch:

> Juridiske rammer designet til en tidsalder med poster kæmper for at styre en tidsalder med kontinuerlig, prædiktiv inferens.

VIII. Magtens asymmetri

Industriel profilering producerer en strukturel ubalance.

Individer genererer data kontinuerligt gennem deltagelse i moderne liv. Undgåelse er mulig, men dyr og ufuldstændig. Imens:

- Virksomheder opretholder uigennemsigtige systemer beskyttet af hemmelighed
- Stater får adgang til og integrerer data gennem juridisk myndighed eller partnerskaber
- Teknisk kompleksitet skjuler ansvarlighed

Resultatet er en klar asymmetri:

> De mange gøres læselige; de magtfulde forbliver relativt uigennemsigtige.

IX. Internalisering: Profilering og selvregulering af adfærd

Ud over dens institutionelle og teknologiske dimensioner producerer industrialiseringen af profilering en dyb psykologisk transformation. Overvågning fungerer ikke længere udelukkende som en ydre kraft; den bliver internaliseret.

Denne dynamik blev forudset af Michel Foucault i hans analyse af panoptikonet: et teoretisk fængselsdesign af Jeremy Bentham, hvor indsatte, der er synlige for en central obser-

vatør, de ikke kan se, internaliserer disciplin og regulerer deres egen adfærd under usikkerheden om konstant overvågning. Panoptikonets magt ligger ikke i evig observation, men i **forventningen** om den.

Industriel profilering udvider denne logik dramatisk. Individer opererer i miljøer, hvor handlinger kan registreres, analyseres og fortolkes på uigennemsigtige måder – af platforme, der optimerer for engagement, eller stater, der vurderer risiko. Resultatet er et skift mod **selvregulering**.

Dette manifesterer sig som:

- Selv-censur i opslag, søgninger eller associationer
- Undgåelse af visse grupper, emner eller steder
- Tilpasning til opfattede normer for at minimere risikoscores
- Modifikation af adfærd på tværs af digitale og fysiske kontekster

Afgørende er, at disse tilpasninger ikke kræver eksplicit tvang. De opstår fra forventning.

> Kontrol udøves ikke kun gennem, hvad systemerne gør, men gennem, hvad individer undlader at gøre.

Effekterne strækker sig ud over individer. Når mennesker selv-censurerer og selv-sorterer, forstærker de genererede data mønstrene og former fremtidige forudsigelser. Systemet observerer ikke blot virkeligheden – det former den subtilt og skaber feedback-loops, der normaliserer konformitet.

X. Afslutningen på selektiv overvågning

Profilering har gennemgået en fundamental transformation:

- Fra **målrettet** til **universel**
- Fra **manuel** til **automatiseret**
- Fra **retrospektiv** til **prædiktiv**
- Fra **fragmenteret** til **integreret**

Tidligere systemer var begrænset af friktion – omkostning, tid, menneskelig opmærksomhed. Industrielle systemer fjerner disse begrænsninger. Overvågning bliver ambient. Inklusion bliver standard.

Princippet om, at data kun skal tjene sit umiddelbare formål, har givet plads til et paradigme, hvor **alle data potentielt er udnyttelige**.

XI. Konklusion: Prisen for deltagelse

Den lange bue fra brevhemmelighed til digital datafusion afslører et konsistent mønster: hver teknologisk udvidelse øger omfanget af profilering, mens juridiske og sociale reaktioner halter bagefter. Hvad der adskiller nutiden, er det strukturelle. Profilering er ikke læn-

gere en aktivitet rettet mod specifikke individer – det er en infrastruktur, som individer eksisterer inden i.

Kategorien „person af interesse“ opløses. Alle bliver genstand for kontinuerlig evaluering.

Denne transformation opretholdes ikke kun af statsmagt, men også af økonomiske incitamenter. Platforme, der ser ud til at være gratis, fungerer gennem adfærdsdataudtræk. Sætningen *„hvis du ikke betaler for produktet, er du produktet“* fanger en intuition – men underdriver virkeligheden.

Hvad der produceres, er ikke individet, men en **prædiktiv model** af individet – portabel, handlingsrettet og ofte utilgængelig for den person, den repræsenterer.

En central udfordring ligger i et gab mellem perception og virkelighed.

For det første undervurderer mennesker **virkningen** af det, der vides. Profilering fungerer gennem association. Relationer – fortidige, svage eller indirekte – kan forme udfald. En forbindelse til nogen, der senere bliver uønsket, kan påvirke muligheder. Man dømmes ikke kun individuelt, men relationelt.

For det andet undervurderer mennesker **omfanget** af det, der kan vides. Systemer slutter følsomme attributter – politiske, religiøse, seksuelle, økonomiske – ikke fra eksplicit afsløring, men fra mønstre. Disse slutninger bliver operationelle uanset deres nøjagtighed.

> Individer vurderes ikke kun på, hvad de afslører, men på, hvad der kan sluttes – og på, hvem de er forbundet med.

Deltagelse i digitalt liv indebærer således et implicit bytte: bekvemmelighed for læselighed. Dette bytte er hverken transparent eller forhandlingsbart.

Udfordringen er ikke at standse datificering, men at begrænse den – at genindføre friktion, håndhæve grænser og sikre ansvarlighed.

Det centrale spørgsmål er klart:

> Vil intervention ske, før infrastrukturen for permanent profilering bliver for dybt indlejret til at kunne udfordres meningsfuldt?

I mangel af sådan en intervention er prisen for deltagelse ikke blot data – men den gradvise erosion af grænsen mellem at blive observeret, at blive sluttet og i sidste ende at blive defineret.