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

Van Personen van Belang naar Bevolkingen: De Industrialisering van Profiling

De opkomst van profiling — van gerichte, handmatige scrutiny van specifieke “personen van belang” naar de geautomatiseerde, continue monitoring van gehele bevolkingen — vertegenwoordigt een van de meest ingrijpende transformaties in de uitoefening van macht, de rol van technologie en de grenzen van individuele autonomie. Wat ooit aanzienlijke menselijke inspanning, institutionele prioritering en bewuste selectie vereiste, is geëvolueerd tot een naadloze infrastructuur die gedragsdata van miljarden mensen in real-time genereert, aggregeert en analyseert, vaak als een incidenteel neveneffect van het alledaagse leven.

Deze transformatie was niet louter voorbestemd door technologie alleen. Ze ontstond uit de interactie van bureaucratische expansie, herhaalde veiligheids-crises, economische prikkels verbonden aan datamonetisering, en de meedogenloze daling van de marginale kosten van dataverzameling, -opslag en -afleiding. Het resultaat is niet simpelweg “meer surveillance”, maar een kwalitatief ander regime: een dat natuurlijke wrijving vervangt door wrijvingsloze schaal, menselijk oordeel door algoritmische automatisering, en uitzonderlijke verdenking van de weinigen door baseline-observatie van de velen.

In de kern ligt een fundamentele metamorfose: profiling is verschoven van een **ambachtelijke kunst** — selectief, arbeidsintensief en verklarend — naar een **industrieel proces** — universeel, geautomatiseerd en voorspellend. Wat volgt traceert deze transformatie, met identificatie van de momenten waarop beperkingen erodeerden en nieuwe mogelijkheden kristalliseerden tot een systeem van continue, bevolkingsbrede inferentie.

I. Fundamenten: Profiling als Selectieve, Handmatige Praktijk

Profiling, in zijn meest basale vorm, omvat de systematische verzameling en interpretatie van informatie om kenmerken te infereren, gedrag te voorspellen of risicocategorieën toe te wijzen. De oorsprong reikt diep terug tot de oudheid.

Oude rijken voerden volkstellingen uit niet alleen voor belasting of conscriptie, maar ook voor classificatie. Romeinse autoriteiten en Chinese keizerlijke bestuurders sorteerden bevolkingen op beroep, loyaliteit en status, en produceerden vroege relationele kaarten die potentiële dreigingen konden identificeren. Religieuze instellingen hielden registers bij van geboorten, huwelijken, biechten en moreel gedrag, en bouwden proto-sociale grafieken die netwerken van invloed en afwijking onthulden.

Deze systemen deelden echter een bepalende beperking: **informatie was duur**. Het verzamelen, verifiëren, opslaan en interpreteren van data vereiste aanzienlijke menselijke ar-

beid. Als gevolg bleef profiling **selectief, episodisch en begrensd**. Het richtte zich op elites, dissidenten of strategisch relevante groepen — niet op gehele bevolkingen.

In vroegmodern Europa bleef deze selectiviteit bestaan, zelfs terwijl staten hun surveillance-apparaat uitbreidden. Inlichtingenefforts richtten zich op ketters, politieke rivalen, smokkelaars en buitenlandse agenten via informanten, onderschepte correspondentie en fysieke surveillance. De *cabinets noirs* — of Zwarte Kamers — van Frankrijk en andere staten belichaamden deze aanpak: teams van klerken openden handmatig brieven, kopieerden ze en verzegelden ze opnieuw voor verzending. Deze operaties waren inherent beperkt. Ze richtten zich op hoogwaardige doelen omdat alles breder logistiek onmogelijk was.

Zelfs in dit stadium werd de kracht van **metadata** duidelijk begrepen. Informatie over communicatie — afzender, ontvanger, timing en route — kon netwerken en intenties blootleggen zonder toegang tot de inhoud. Het Britse Post Office-spionageschandaal van 1844 bracht dit scherp in de publieke aandacht. De Italiaanse revolutionair Giuseppe Mazzini, een balling in Londen, vermoedde dat zijn brieven door de autoriteiten werden geopend op verzoek van buitenlandse mogendheden. Hij en zijn aanhangers plaatsten papaverzaadjes en zandkorrels in enveloppen als markeringen; toen de brieven verstoord aankwamen, spoorde Mazzini de radicale MP Thomas Duncombe aan om het onderwerp in het Parlement aan te kaarten. Het resulterende schandaal onthulde systematisch openen van brieven onder warrants uitgevaardigd door Minister van Binnenlandse Zaken Sir James Graham, wat woede, parlementaire onderzoeken en uiteindelijk de afschaffing van de geheime afdeling van het Post Office veroorzaakte. Het markeerde een van de eerste moderne privacy-panieken en benadrukte hoe relationele data alleen netwerken van associatie kon ontmantelen.

Als reactie ontstonden juridische normen zoals de “geheimhouding van correspondentie” (*Briefgeheimnis*, *secret de la correspondance*). Deze principes beperkten het gebruik van communicatiegegevens strikt tot operationele doeleinden zoals bezorging, en verboden secundair gebruik voor surveillance of profiling. Het onderliggende idee was eenvoudig maar diepgaand:

> Data gegenereerd voor een specifiek doel mogen niet worden hergebruikt om bredere profielen van individuen of netwerken te construeren.

Dit principe zou eeuwenlang echoën — maar uiteindelijk eroderen onder technologische en institutionele druk.

II. De Bureaucratische Eeuw: Schaalvergroting Zonder Automatisering

De twintigste eeuw breidde profiling dramatisch uit terwijl veel van de eerdere beperkingen behouden bleven. De eisen van totale oorlog vereisten ongekende informatieverzameling. Censuur van post, signal intelligence en codebreking breidden surveillance uit voorbij elites naar bredere bevolkingen. Instellingen zoals de National Security Agency in-

stitutionaliseerden grootschalige interceptie, terwijl binnenlandse agentschappen uitgebreide dossiers aanlegden over politieke groepen, vermeende radicalen en criminele netwerken.

Toch bleef profiling **fundamenteel gericht**. Afluisteroperaties waren gekoppeld aan specifieke individuen of lijnen. Inlichtingendossiers werden samengesteld door menselijke analisten. Zelfs bij toenemend volume bleef **menselijke aandacht de bottleneck**.

Vroege computersystemen (jaren 1950–1970) begonnen de schaal van archivering te veranderen. Overheden en bedrijven digitaliseerden welzijnsregisters, kredietgeschiedenissen en criminele databases, waardoor snellere opvraging en kruisverwijzing mogelijk werd. Maar deze systemen opereerden nog steeds op **discrete records**, niet op continue stromen gedrag.

Tegen de jaren 1970 leidden zorgen over gecentraliseerde “databanken” tot juridische reacties. De Amerikaanse Privacy Act van 1974 en vroege Europese wetten op gegevensbescherming introduceerden principes van doelbinding, dataminimalisatie en transparantie. Deze kaders breidden de logica van correspondentiegeheim uit naar het digitale tijdperk.

Ze waren echter gebouwd op een cruciale aanname: dat dataverzameling **begrensd en episodisch** was. Ze reguleerden records — niet stromen. Deze aanname zou spoedig instorten.

III. Het Inflectiepunt: Van Records naar Data-exhaust

De beslissende breuk vindt plaats in de late jaren 1990 en vroege jaren 2000 met de opkomst van het internet — niet louter als communicatiemedium, maar als infrastructuur die continu data produceert.

Digitale systemen genereren **data-exhaust**: metadata die automatisch ontstaat als neveneffect van gewone activiteit. Elke verbinding, query, klik en beweging produceert sporen die tegen verwaarloosbare kosten kunnen worden gelogd, opgeslagen en geanalyseerd.

Dit markeert de beslissende verschuiving:

> Profiling stopt met een activiteit die op data wordt uitgevoerd en wordt een infrastructuur die het continu produceert.

Internet Service Providers vangen verbindingslogs, DNS-queries en routeringsinformatie op, waardoor gedragspatronen zichtbaar worden zelfs zonder toegang tot inhoud. In tegenstelling tot postale metadata — vluchtig en gedecentraliseerd — is digitale metadata persistent, gecentraliseerd en triviaal doorzoekbaar.

Bovenop deze infrastructuur transformeerden platforms zoals Google en Meta profiling tot een kern economisch model. Zoekmachines vangen intentie; sociale netwerken brengen relaties in kaart; mobiele ecosystemen volgen beweging. Ingebedde trackers breiden zichtbaarheid uit over grote delen van het web. Meta’s tracking pixels, aanwezig op ongeveer een derde van de populaire websites ter wereld, monitoren activiteit ver buiten hun

eigen platforms, vaak gevoelige signalen uit gezondheid, financiën of politieke contexten opvangend.

Een cruciaal inzicht ontstaat in deze omgeving:

> Inhoud wordt grotendeels overbodig. In veel gevallen zijn relationele patronen niet slechts proxies voor betekenis — ze zijn analytisch nuttiger dan de inhoud zelf.

Metadata geeft niet simpelweg aan dat communicatie plaatsvond; het maakt **probabilistische reconstructie van inhoud** mogelijk. Wie met wie communiceert, wanneer, hoe vaak en in welke bredere context kan sterk beperken wat er wordt gecommuniceerd. Openbaar beschikbare informatie — gedeelde affiliaties, professionele rollen, politieke posities, sociale banden — vernauwt verder de ruimte van plausibele interpretaties.

Na verloop van tijd worden deze beperkingen voorspellend. Metadata is niet louter beschrijvend; het is generatief. Het begeleidt inhoud niet slechts — het kan het vaak **benaderen of infereren**, vooral wanneer het op schaal wordt geaggregeerd.

Zoekopdrachten onthullen intentie. Communicatiefrequentie onthult relatiekracht. Co-locatie onthult associatie. Bij voldoende schaal convergeren deze signalen naar zeer accurate gedragsmodellen die directe toegang tot inhoud vaak overbodig maken.

Bedrijfssystemen optimaliseren gedrag voor monetisering; staatssystemen beperken het voor controle — maar beide vertrouwen op dezelfde onderliggende machinerie: **voorspelling door grootschalige gedragsinferentie**.

IV. Identiteit Zonder Ontsnapping: Persistente Ankers

Een bepalend kenmerk van industriële profiling is de opkomst van **persistente identiteit**.

Eerdere systemen vertrouwden op veranderbare identificatoren — namen, documenten, adressen — die konden worden gewijzigd of verhuld. Moderne systemen reconstrueren identiteit door overlappende signalen:

- Apparaatvingerafdrukken
- Gedragspatronen
- Sociale grafieken
- Biometrische markers (gezichten, gang, stem)

Openbaar gedeelde afbeeldingen dienen als duurzame ankers. Zelfs wanneer individuen accounts wijzigen of pseudoniemen aannemen, kunnen gezichtsherkenningssystemen — vooral in staats- of inlichtingcontexten — identiteiten herverbinden over datasets heen. Co-occurrence in foto’s of gedeelde evenementen versterkt verder de geïnfereerde relaties.

De implicatie is diepgaand:

> Identiteit is niet langer iets dat men verklaart, maar iets dat continu wordt geïnfereerd.

Dit elimineert veel van de wrijving die surveillance ooit beperkte. Identificatie hangt niet af van één enkel signaal; het ontstaat uit redundantie over vele.

V. Fusie: Van Datapunten naar Ontologieën

De bekroning van deze evolutie is **datafusie**: de integratie van disparate datasets in verenigde analytische systemen.

Platforms zoals Palantir Technologies aggregeren overheidsrecords, financiële transacties, sociale media-activiteit, locatiegegevens en communicatiemetadata tot coherente modellen van individuen en netwerken. Deze systemen bouwen dynamische ontologieën die analisten in staat stellen relaties te bevragen, patronen te detecteren en voorspellingen te genereren.

Een concreet voorbeeld illustreert de verschuiving. Bij immigratiehandhaving vult Palantir's Enhanced Leads Identification and Targeting for Enforcement (ELITE)-tool kaarten met potentiële doelen, puttend uit visumrecords, werkgelegenheidsdata, telefoonmetadata, sociale connecties en zelfs Medicaid- of HHS-adresinformatie om "adresvertrouwensscores" toe te wijzen en dossiers te genereren. Ambtenaren kunnen "doelrijke" buurten identificeren voor operaties, waarbij individuen niet alleen op basis van direct bewijs worden gemarkeerd, maar omdat hun **gedrags- en relationele handtekening** lijkt op eerder geïdentificeerde gevallen. Soortgelijke fusie verschijnt in tools zoals ImmigrationOS, die reisgeschiedenissen, biometrie en sociale data integreren voor prioritering.

Verdenking wordt niet langer ontdekt — ze wordt **gegenereerd**.

Profiling documenteert de realiteit niet slechts; het bouwt haar actief op door probabilistische associaties naar voren te brengen die operationeel actionable worden.

VI. Van Uitleg naar Preventie

Traditioneel profiling was grotendeels retrospectief. Het zocht uitleg van voorbije acties — wie een misdrijf pleegde, wie een complot organiseerde, wie een bedreiging vormde.

Industriële profiling is voorspellend en preventief. Het identificeert:

- Wie mogelijk een misdrijf zal plegen
- Waar misdaad mogelijk zal plaatsvinden
- Wie mogelijk in gebreke zal blijven, radicaliseren of afwijken

Deze logica wordt vaak vergeleken met de visie in *Minority Report*, waarin individuen worden gearresteerd voordat ze misdrijven plegen. Hoewel hedendaagse systemen deterministische vooruitziendheid missen, is de structurele gelijkenis duidelijk: predictieve politietools analyseren historische data, 911-oproepen, kentekenlezers en sociale signalen om "hitlijsten" of risicoscores te genereren.

Moderne systemen werken op waarschijnlijkheid. Individuen worden gemarkeerd niet omdat ze zullen handelen, maar omdat ze **statistisch lijken op anderen die dat hebben gedaan**.

De verschuiving is subtiel maar diepgaand:

> Individuen worden niet langer primair beoordeeld op hun acties, maar op hun positie binnen een probabilistisch landschap.

Verdenking wordt structureel — continu gegenereerd in plaats van getriggerd door discrete gebeurtenissen.

VII. Recht in het Tijdperk van Inferentie

Juridische kaders zoals de General Data Protection Regulation proberen limieten op te leggen via toestemming, transparantie en minimalisatie. Toch staan ze voor structurele beperkingen.

De meeste juridische systemen reguleren **data als object**. Moderne profiling ontleent macht aan **relaties en inferenties**, die veel moeilijker te definiëren, te observeren of te beperken zijn.

Extra uitdagingen omvatten:

- Continue datastromen over jurisdicties heen
- Brede uitzonderingen voor nationale veiligheid en “legitieme belangen”
- Opaque algoritmische systemen die weerstand bieden aan toezicht

Het resultaat is een aanhoudende mismatch:

> Juridische kaders ontworpen voor een tijdperk van records worstelen om een tijdperk van continue, predictieve inferentie te besturen.

VIII. De Asymmetrie van Macht

Industriële profiling produceert een structureel onevenwicht.

Individuen genereren continu data door deelname aan het moderne leven. Vermijding is mogelijk maar kostbaar en incompleet. Ondertussen:

- Handhaven bedrijven opaque systemen beschermd door geheimhouding
- Krijgen staten toegang tot en integreren data via juridische autoriteit of partnerschappen
- Verbergt technische complexiteit aansprakelijkheid

Het resultaat is een duidelijke asymmetrie:

> De velen worden leesbaar gemaakt; de machtigen blijven relatief ondoorzichtig.

IX. Internalisering: Profiling en de Zelfregulering van Gedrag

Buiten zijn institutionele en technologische dimensies produceert de industrialisering van profiling een diepgaande psychologische transformatie. Surveillance opereert niet langer uitsluitend als een externe kracht; ze wordt geïnternaliseerd.

Deze dynamiek werd voorzien door Michel Foucault in zijn analyse van de panopticon: een theoretisch gevangenisontwerp van Jeremy Bentham waarin gevangenen, zichtbaar voor een centrale waarnemer die ze niet kunnen zien, discipline internaliseren en hun eigen gedrag reguleren onder de onzekerheid van constante observatie. De macht van de panopticon ligt niet in perpetuele observatie maar in de **anticipatie** ervan.

Industriële profiling breidt deze logica dramatisch uit. Individuen opereren binnen omgevingen waarin acties kunnen worden geregistreerd, geanalyseerd en geïnterpreteerd op ondoorzichtige manieren — door platforms die optimaliseren voor engagement of staten die risico beoordelen. Het resultaat is een verschuiving naar **zelfregulering**.

Dit manifesteert zich als:

- Zelfcensuur in posts, zoekopdrachten of associaties
- Vermijding van bepaalde groepen, onderwerpen of locaties
- Alignering met waargenomen normen om risicoscores te minimaliseren
- Aanpassing van gedrag over digitale en fysieke contexten

Cruciaal is dat deze aanpassingen geen expliciete dwang vereisen. Ze ontstaan uit anticipatie.

> Controle wordt uitgeoefend niet alleen door wat systemen doen, maar door wat individuen vermijden te doen.

De effecten reiken verder dan individuen. Terwijl mensen zichzelf censureren en zichzelf sorteren, versterken de gegenereerde data patronen, waardoor toekomstige voorspellingen worden gevormd. Het systeem observeert de realiteit niet alleen — het herschikt haar subtiel, en creëert feedbackloops die conformiteit normaliseren.

X. Het Einde van Selectieve Surveillance

Profiling heeft een fundamentele transformatie ondergaan:

- Van **gericht** naar **universeel**
- Van **handmatig** naar **geautomatiseerd**
- Van **retrospectief** naar **voorspellend**
- Van **gefparmenteerd** naar **geïntegreerd**

Eerdere systemen waren beperkt door wrijving — kosten, tijd, menselijke aandacht. Industriële systemen verwijderen deze beperkingen. Monitoring wordt ambient. Inclusie wordt

default.

Het principe dat data alleen haar onmiddellijke doel moet dienen heeft plaatsgemaakt voor een paradigma waarin **alle data potentieel exploiteerbaar is**.

XI. Conclusie: De Prijs van Participatie

De lange boog van postgeheim naar digitale datafusie onthult een consistent patroon: elke technologische expansie vergroot het bereik van profiling, terwijl juridische en sociale reacties achterblijven. Wat het heden onderscheidt is structureel. Profiling is niet langer een activiteit gericht op specifieke individuen — het is een infrastructuur waarbinnen individuen bestaan.

De categorie “persoon van belang” lost op. Iedereen wordt onderworpen aan continue evaluatie.

Deze transformatie wordt niet alleen in stand gehouden door staatsmacht, maar ook door economische prikkels. Platforms die vrij lijken opereren via gedragsdata-extractie. De uitspraak *“als je niet betaalt voor het product, ben jij het product”* vat een intuïtie — maar onderschat de realiteit.

Wat geproduceerd wordt is niet het individu, maar een **voorspellend model** van het individu — draagbaar, actionable en vaak ontoegankelijk voor de persoon die het vertegenwoordigt.

Een centraal uitdaging ligt in een kloof tussen perceptie en realiteit.

Ten eerste onderschatten mensen de **impact** van wat bekend is. Profiling opereert via associatie. Relaties — verleden, zwak of indirect — kunnen uitkomsten vormen. Een connectie met iemand die later ongewenst wordt kan kansen beïnvloeden. Men wordt niet alleen individueel beoordeeld, maar relationeel.

Ten tweede onderschatten mensen de **omvang** van wat bekend kan worden. Systemen infereren gevoelige attributen — politiek, religieus, seksueel, economisch — niet uit expliciete onthulling, maar uit patronen. Deze inferenties worden operationeel ongeacht hun nauwkeurigheid.

> Individuen worden geëvalueerd niet alleen op wat ze onthullen, maar op wat kan worden geïnfereerd — en op met wie ze verbonden zijn.

Participatie in het digitale leven impliceert dus een impliciete ruil: gemak voor leesbaarheid. Deze ruil is noch transparant noch onderhandelbaar.

De uitdaging is niet om dataficatie te stoppen, maar om haar te beteugelen — wrijving te herstellen, limieten af te dwingen en verantwoording te waarborgen.

De centrale vraag is duidelijk:

> Zal interventie plaatsvinden voordat de infrastructuur van permanente profiling te diep is ingebed om zinvol uitgedaagd te worden?

Bij afwezigheid van dergelijke interventie is de prijs van participatie niet louter data — maar de geleidelijke erosie van de grens tussen geobserveerd worden, geïnfereerd worden en uiteindelijk gedefinieerd worden.