Palantir i politiet

Metoderapport – Skup 2022

MORGENBLADET

Journalist: Hanne Østli Jakobsen

Publisert: 22. oktober 2021 – 6. januar 2022

INNHOLDSFORTEGNELSE

1 Praktisk informasjon

Innsender:

Hanne Østli Jakobsen

977 96 876 / hj@morgenbladet.no

Redaksjon:

Morgenbladet AS

Grubbegata 4-6

0179 Oslo

Prosjektperiode:

Mars – desember 2021. Første publikasjon 22. oktober 2021, foreløpig siste 6. januar 2022.

Lenker til artikler:

https://www.morgenbladet.no/aktuelt/2021/10/22/ny-teknologi-setter-stadig-flere-av-oss-i-politiets-sokelys/

https://www.morgenbladet.no/aktuelt/2021/10/22/palantirs-norske-system-virker-enna-ikke/

https://www.morgenbladet.no/aktuelt/teknologi/2021/12/03/slik-ble-politiets-supervapen-en-100-millioners-fiasko/

https://www.morgenbladet.no/aktuelt/2021/12/09/palantir-ville-analysere-norske-helsedata-under-pandemien/

https://www.morgenbladet.no/aktuelt/2021/12/17/overvakning-endret-loven-for-a-passe-til-palantirs-programvare/

https://www.morgenbladet.no/aktuelt/2022/01/06/vil-apne-for-storstilt-nettovervaking-fra-pst/

Takk til:

Fritt Ord, Sindre Granly Meldalen, Christian Belgaux, Peder Bernhard, Knut Egil Wang, Bjarne Riiser Gundersen og Sun Heidi Sæbø.

2 Innledning

«Som et Silicon Valley-teknologiselskap, har Palantir en agil kultur for softwareutvikling, definert av overlegen innovasjon og design …»

Setningen lyste mot meg fra kontrakten mellom det norske politiet og Palantir Technologies. Et sjeldent klart brudd på formaningen om «show, don't tell», ja visst – men erklæringen er også talende. Slik snakker de store teknologiselskapene, ikke bare i pressemeldinger, men i offisielle dokumenter i Norge. Hva lå bak ordene?

Da jeg leste setningen var det klart at dette agile selskapet hadde kommet på hælene i Norge. Det er nå fem år siden politiet inngikk en avtale om kjøp av programvare fra Palantir, det amerikanske teknologiselskapet som spesialiserer seg på dataanalyse og overvåkning. Denne høsten har Morgenbladet dokumenter at programmet fortsatt ikke fungerer som det skal. Kostnaden har steget fra et anslag på snaut 30 millioner til over 100 millioner kroner, men knapt noen av gevinstene som ble lovet i den mange hundre sider lange kontrakten er i dag realisert hos det norske politiet.

At IT-prosjekter blir dyrere enn antatt, er nærmest en naturlov. Men dette var ingen hvilken som helst IT-leverandør. Palantir regnes gjerne – og regner seg selv – som en av de store nyvinningene fra Silicon Valley, som bruker banebrytende teknologi for å løse problemer. De insisterer selv på at de ikke driver med persondata, men det er likevel råvaren: De behandler dataene som kundene deres sitter på. Når kunden er det norske politiet, er det dermed data om norske borgere de får i hende. Palantir er mektige, og et av de selskapene som først satset på statlige kunder, heller enn reklamefinansiering, som forretningsmodell. Samtidig har norske politikere et sterkt ønske om at Norge skal være ledende på digitalisering – vi har en egen strategi for kunstig intelligens og det snakkes om data og den digitale økonomien på inn- og utpust.

Når to så mektige aktører – store teknologiselskaper på den ene siden, og staten på den andre – har sammenfallende interesser, må pressen følge med. Samarbeidet mellom Palantir og politiet er av en type som vi vil se mer av: Store teknologiselskaper kommer til å by seg frem som en attraktiv partner for dem som vet mest om oss. Det er ekstremt viktig at pressen følger med og kikker dem i kortene når de diskuterer hvordan norske borgeres opplysninger skal brukes. Avveiningene mellom bedre kontroll på den ene siden, og grunnleggende borgerrettigheter på den andre, kan ikke skje i det stille.

Morgenbladet har ikke mye erfaring med et omfattende og systematisk innsynsarbeid av typen som dette prosjektet har krevd. Vi jobber heller ikke vanligvis opp mot justissektoren og politiet. Å skulle gå løs på Politidirektoratet skulle vise seg å være mer utfordrende enn vi hadde sett for oss – men desto viktigere, både for saken, og for det den har vist om hvordan direktoratet forholder seg til offentlighetsloven.

3 Slik kom arbeidet i gang

3.1 Hvor det startet: En helt annen nysgjerrighet, midt i pandemien

Jeg har fulgt selskapet Palantir i en rekke år, av ren nysgjerrighet. Palantir er mindre og mindre kjent enn de virkelig store Silicon Valley-selskapene, men forretningsmodellen deres gjør dem spennende: De inngår avtaler med statlige kunder, med myndigheter, heller enn å «gi bort» produktene sine. Hvis man, som jeg, er bekymret for den økende makten disse selskapene har til å forme vår verden, er en slik taktikk spesielt bekymringsverdig. Dermed har jeg fulgt deres arbeid i USA med interesse, og da de etablerte seg og begynte å jobbe

med norske kunder rundt 2017 økte interessen. Ideen om å grave i dette IT-prosjektet kom først i 2019, da kostnadsproblemene i politiets Palantir-prosjekt ble meldt i Politiforum. Men den store krisen som rammet Morgenbladet den høsten gjorde at arbeidet aldri kom i gang.

Så, da pandemiens første bølge herjet Norge, og Morgenbladet – som de fleste andre redaksjoner – forsøkte å dekke viruset fra hjemmekontor, kom meldingen i Politiforum om at prosjektet var «forsert avsluttet». Det er en merkelig formulering, og artikkelen gjorde meg bare mer nysgjerrig:

Den beskrev store kostnadsoverskridelser og samarbeidsproblemer, men det var vanskelig å få ordentlig grep på hva som hadde gått så galt, og hvilken rolle Palantir spilte i sagaen. Det, kombinert med nysgjerrigheten fra tidligere om hvem Palantir faktisk er og hva de gjør, gjorde at vi bestemte at nå var det på tide å gjøre et ordentlig forsøk på å forstå denne fadesen.

3.2 Hva var kjent fra før

Politiets samarbeid med Palantir har vært omtalt i norsk presse før Morgenbladet begynte å grave i saken. Særlig har Politiforum gjort et viktig arbeid – de har dekket prosjektet kontinuerlig siden før Palantir ble valgt, og vært særlig grundige i dekningen av perioden fra da den interne kritikken mot prosjektet kom i 2019. Deres arbeid har vært viktig for Morgenbladets graveprosjekt, men naturlig nok har de fokusert på politiets rolle, altså på den ene siden av saken.

I tillegg har både NRK og Aftenposten skrevet om Palantir i det norske politiet. I Aftenpostens gjennomgang av prosjektets problemer fra 2019 kunne vi lese om en rekke samarbeidsproblemer, juridisk sommel og stor konsulentbruk, blant annet. Aftenpostens journalister nevnte også en besnærende setning som jeg ikke ble helt klok på:

De skrev at et av de store problemene var at prosjektet på et tidspunkt ble utvidet til «å også inkludere en analyse- og informasjonsbehandlingsdel». Det er jo selve hovedproduktet som Palantir leverer – hvordan var dette ikke med fra starten?

Med andre ord: Selv etter det gode arbeidet til disse mediene var det vanskelig å forstå veien fra «supervåpen», slik programvarekjøpet ble omtalt da kontrakten ble inngått, til «forsert avslutning». Slik jeg så det, var det to viktige brikker som manglet.

3.3 De sentrale problemstillingene: *Hva* gikk så galt?

For det første manglet offentligheten en ordentlig beskrivelse av *hva* som hadde skjedd. Her snakker vi om 100 millioner skattekroner som er brukt på en teknologi som politiet *selv* innrømmer at ikke fungerer som den skal. Palantir hyller seg inn i myter, men det må da likevel være mulig for oss vanlige borgere å forstå hva det var de skulle forsøke å få til med programvaren sin, og hvorfor det ikke gikk? Rapporter om samarbeidsproblemer og «uenighet om kvalitet» holdt ikke, mente jeg:

Politiet sitter på data om borgernes lovbrudd, domfellelser, telefonsamtaler og bevegelser – det er viktig å forstå nøyaktig *hva* Palantir skulle gjøre med disse opplysningene.

Dette er dessuten altså et av de første eksemplene på samarbeid mellom såkalt «Big Tech» og den norske stat. Det er ingen grunn til å tro at det blir det siste: Google kjøper seg opp innen helseteknologi, og kan godt tenkes å ønske et samarbeid med Helsedepartementet – om de ikke allerede har foreslått det. Vi *må* vite hvordan de falbyr sine tjenester og hvordan våre folkevalgte og embetsfolk svarer på fremstøtene. Her var et eksempel der jeg visste at

samarbeidet hadde gått galt. Det var grunn til å tro at det fantes misfornøyde folk som kunne fortelle om prosessen, og dokumenter som kunne vise hvordan samarbeidet hadde gått. Jeg ville finne begge deler.

3.4 Og hvor er Palantir?

Palantir, med sitt rykte for hemmelighold og sine bånd til både CIA, det amerikanske forsvaret og Silicon Valley, får naturlig nok oppmerksomhet når det etablerer seg i Norge. Dermed er det påfallende hvor *fraværende* Palantir har vært i dekningen av politiets samarbeid med dem: Tidligere artikler har gått grundig gjennom hvordan politiet har kivet om dette prosjektet, men hvor var Palantir? De syntes knapt i dekningen, og de andre avisene hadde ikke fått dem i tale. Var det virkelig ikke mulig å vite mer om dette selskapet – deres teknologi, deres taktikker og fremgangsmåter?

Her kan det være nyttig med en liten ordliste, for å følge gangen i dette graveprosjektet:

- **Palantir** er et selskap, grunnlagt av blant andre Peter Thiel, en beryktet amerikansk investor som blant annet var tidlig inne i Facebook og som støttet Donald Trump.
- Palantir lager programvaren **Gotham,** som brukes til å sammenstille og analysere informasjon og som vanligvis selges til kunder i forsvars- og etterretningsbransjen.
- Det var dette programmet politiet i Norge kjøpte da de startet prosjektet **Omnia**. Omnia ble drevet av Politidirektoratet, **POD**, og hadde som mål å hjelpe politiet håndtere internasjonalt politiarbeid.
- Dette var fordi POD antok at det kom til å bli mange flere internasjonale henvendelser når Norge koblet seg på det europeiske **Prüm-samarbeidet,** som skal la politistyrker i Europa samarbeide og utveksle informasjon med hverandre.

Under Omnia skulle altså politiet bruke Gotham til å koble sammen en rekke politiregistre, som inneholder fingeravtrykk, DNA-profiler og informasjon om kjøretøy og førerkort. I Gotham skulle de så kunne lete etter koblinger mellom spor, finne sammenhenger mellom kriminalsaker og løse dem raskere. Det var i hvert fall ambisjonen.

4 Et svært prosjekt, vilkårlige dokumentert

4.1 Det som fantes i postlistene, og det som ikke fantes

Første skritt for å forstå Palantirs arbeid hos politiet var å skaffe oversikt over de tilgjengelige dokumentene i prosjektet. Fantes det rapporter som beskrev problemene? E-postutvekslinger fra kritiske perioder? Møtereferater? Prosjektet var eid og drevet av Politidirektoratet, og jeg søkte derfor etter spor etter prosjektet med alle tenkelige søkeord, og stavemåter av disse, i deres postlister. Det holdt ikke å lete etter «prüm» og «omnia», også «prum», «prym» og «omina» måtte med. Dette arbeidet ble dokumentert i en oversikt i Excel, samtidig som jeg ba om innsyn i dokumentene.

Ganske raskt ble to ting tydelig: For det første fantes et knippe viktige saksnumre, som samlet mye av de journalførte dokumentene i prosjektet. Disse brukte jeg derfor tid på å gjøre meg kjent med – de lot meg få et første innblikk i gangen i prosjektet, fra før anbudet ble lyst ut i 2016 til i dag. Det var viktig å få kronologien på plass: I et langvarig og komplisert prosjekt – der hendelsene jeg var mest interessert lå flere år tilbake i tid – måtte jeg ha bedre kontroll på tidspunkter og endringer enn selv kildene. Da kunne jeg stille kontrollspørsmål, vurdere troverdighet og verifisere utsagn.

Denne kronologien ble samlet i et eget Word-dokument, der jeg noterte datoer, hendelser, navn, spørsmål jeg ennå ikke hadde svar på – og svar på spørsmålene etter hvert som jeg fant dem. Det ble spesielt viktig i skriveprosessen mot slutten: Med Excel-oversikten over dokumentene og kronologien kunne jeg kjapt gå tilbake og finne tidspunkter og de aktuelle opplysningene jeg skulle skrive om.

Det viktigste jeg oppdaget, var at det måtte være store hull i journalføringen. I postlistene fant jeg for eksempel referater fra møter i prosjektets styringsgruppe fra før Palantir vant anbudet, men bare ett møte fra etter at Palantir ble valgt og prosjektet startet for alvor. Det var vel ingen grunn til at man da skulle slutte å ha møter?

Det var i det hele tatt påfallende få dokumenter å finne fra året 2017, prosjektets første år og da det ifølge Aftenposten ble utvidet til å inkludere «en avansert analyse- og informasjonsbehandlingsdel».

Det var mystisk: Hvis prosjektet ble vesentlig endret etter oppstart, hvordan hadde ingen diskutert det eller dokumentert det?

4.2 Et persongalleri begynner å tre frem

Det kom flere nyttige innsikter ut av disse første ukene med arbeid i postlistene. For det første ble det klart at Palantir knapt var å finne: Søker du etter «Palantir» i de offentlige postlistene, finner du stort sett bare innsynsforespørsler fra medier som Morgenbladet og Politiforum. Det begynte etter hvert å komme svar på innsynsbegjæringen (om enn på langt nær alle; mer om det snart), men dokumentene inneholdt lite: standardiserte møtereferater og presentasjoner uten annet innhold enn illustrasjoner av «Kripos» som står igjen på plattformen når «Prüm-toget» forlater stasjonen. Palantirs gjøren og laden, møtene mellom deres representanter og politiet, var ikke der.

Videre var det nå mulig å lage en skisse av et persongalleri i sakskomplekset. Her og der var det navn: en prosjekteier og en løsningsarkitekt var nevnt i en e-post, et møtereferat inneholdt en deltagerliste som jeg kunne dechiffrere via Google og Linkedin for å finne ut hvem deltagerne var, og hvilken rolle de hadde. Alle navn og arbeidssteder ble notert i Excel, og tentative kart over koblinger og roller ble tegnet opp, kastet og tegnet på nytt etter hvert som nye folk dukket opp.

Linkedin lot meg anonymt sjekke alle navn som dukket opp (er denne personen fortsatt i POD? Var hen der i perioden jeg lurer på? osv.), og også finne navn på andre som har oppgitt å jobbe i enten Palantir eller IT-avdelingen til POD i den aktuelle perioden.

I denne startfasen tok jeg noen tentative ringerunder. Jeg valgte å *ikke* ringe lederne i politiet eller i Palantir på dette tidspunktet. Vi vurderte det som at jeg trengte å vite mer før jeg tok kontakt med dem, i tilfelle de faktisk ville svare. Men jeg hadde funnet flere «menige» deltagere i prosjektet, IT-folk som testet programvaren etter hvert som programmet ble satt opp, som nå hadde gått videre til nye jobber. Én leder kontaktet jeg likevel tidlig: Prosjektlederen, en innleid konsulent som jobbet for POD. Hans navn var det som oftest gikk igjen i dokumentene, og han var innleid. Nå hadde han fått seg ny jobb, viste Linkedin, og om han ville prate, ville det kunne løse saken nesten på egenhånd. Han svarte imidlertid blankt nei – og henviste til taushetsplikt om tidligere prosjekter.

Dette visste vi at ville bli en utfordring i dette prosjektet: Linkedin hadde vist oss at flere involverte var innleide konsulenter, som neppe ville ha mye å vinne på å svare på spørsmål om en tidligere oppdragsgiver.

De fleste vi ringte i denne runden sa nei til å snakke, det være seg på bakgrunn eller som åpne kilder. Noen virket i utgangspunktet åpne for å snakke, for så å aldri ta telefonen igjen. Men ringerunden ga også grunn til håp: Noen beklaget at de ikke kunne bidra selv, men sa de syntes det var bra at noen gravde i dette prosjektet, eller nevnte at «ja, det ble jo ikke akkurat slik vi hadde sett for oss». Det ga motivasjon til å fortsette arbeidet.

4.3 Direkte forespørsler til Politidirektoratet

Fra en tidligere kildesamtale, fra da jeg bare var nysgjerrig på Palantir i Norge på egenhånd, hadde jeg fått høre om en tur til California som kunne være viktig for Omnia-prosjektet. Kilden fortalte at sentrale ledere i politiet hadde vært på «studietur» i USA, og besøkt blant annet Palantir. Dette skulle ha skjedd *før* kontrakten ble inngått. Vi visste at andre medier tidligere hadde fått innsyn i deler av kontrakten mellom politiet og Palantir. Men etter samtaler i redaksjonen ble vi enige om at selve anbudsprosessen likevel var verdt å se nærmere på: Hintene om turen til California var indikasjon på at prosessen burde ettergås.

Jeg sendte derfor tre direkte innsynsforespørsler til POD:

- For det første ville jeg ha reiseregningene IKT-sjefen i POD. Han skulle ha vært med på denne turen – reiseregningene kunne verifisere det, og var dermed første skritt for å finne ut hvilken betydning reisen hadde.
- Dernest ba jeg om innsyn i kontrakten mellom politiet og Palantir.
- Til sist formulerte jeg, med hjelp fra Sindre Granly Meldalen i Presseforbundet, et §9-innsynskrav om kommunikasjonen mellom en rekke sentrale personene i Politidirektoratet, og Palantirs ansatte, om implementeringen av prosjektet Omnia i perioden januar-november 2017. Dette dekket perioden fra prosjektet startet til det ble utvidet til å inkludere analysedelen. Her *måtte* nøkkelen til hvorfor prosjektet hadde gått sånn på tverke ligge.

Innsynskravet var helt i tråd med tidligere forståelse av §9 – vi definerte konkrete personer, et konkret prosjekt og en avgrenset tidsperiode. Det burde kunne avsløre om det fantes kommunikasjon mellom Palantir og politiet som ikke var ført i postlistene.

Men herfra gikk alt veldig mye saktere.

5 Innsynsmuren hos Politidirektoratet

5.1 Sendrektighet og surr med hjemler

Hovedproblemet i arbeidet med å dokumentere Palantir-prosjektet i politiet har vært Politidirektoratets håndtering av innsynsforespørsler. Bare en sjelden gang har den generelle regelen om svar innen tre virkedager blitt overholdt. Begrunnelsene vi har fått for avslagene har vært mildt sagt forvirrende: En innsynsforespørsel om et dokument om «Utfordringer i overlevering til linje» tok først fire uker å få svar på. Begjæringen ble så avslått med henvisning til taushetsplikt (§ 13.1). Men da jeg ba om utvidet begrunnelse, endret de hjemmelen – nå inneholdt notatet «interne saksforberedelser», og måtte unntas. Et notat om «Krav til opplysningenes kvalitet» ble på sin side avslått med henvisning til politiregisterloven (om taushetsplikt om personlige forhold). Da vi ba om begrunnelse, kom svaret fra POD om at de hadde konferert med Kripos, avsender av notatet, og begge var enige om at dokumentet måtte unntas offentligheten – med henvisning til en helt annen hjemmel i loven, denne gangen om hensyn til «spanings- og etterretningsvirksomheten».

På et tidspunkt ble et dokument om Kripos' DNA-register avslått fordi det inneholdt informasjon om «forhandlingar om rammeavtalar med landbruks-, fiskeri- og reindriftsorganisasjonane».

Denne praksisen oppfattet vi som lite tillitsvekkende, og et tegn på en bekymringsverdig «avslå først, begrunn senere»-holdning.

Disse problemene hadde vært enklere å håndtere om innsynsbegjæringene ble ekspedert innen rimelig tid. Etter hvert lærte jeg at dersom et svar kom kjapt, var innsynskravet som gjerne innvilget. Men når dagene og etter hvert ukene begynte å gå, var det en indikasjon på at kravet ville bli avslått. Da gikk det nye uker med å vente på utvidede begrunnelser, og enda nye dager og uker før klager ble behandlet. For notatet nevnt over, «Krav til opplysningenes kvalitet», ble en langvarig klageprosess heldigvis ikke nødvendig – fordi jeg etter hvert fikk tak i dokumentet via andre kilder. Mer om det senere.

Ingen av mine klager førte frem fullt og helt. Det er ikke lett å argumentere mot politregisterloven: Når politiet henviser til sine «tekniske innretninger» eller «hensyn til etterforskningsvirksomhet», er det vanskelig å vinne frem. Av prinsipp valgte jeg å klage så langt jeg kunne på et avslag på innsyn i en statusrapport (tertialrapport) og en årsrapport fra Kripos – som skulle være brukere av Omnia når programmet var på plass – til POD fra 2016. Jeg ville vite hvordan Kripos hadde omtalt prosjektet dette viktige året, da kontrakten ble inngått, men begge innsynsbegjæringer ble avvist. Begrunnelsen var både interne saksforberedelser, og dessuten bestemmelsene i politiregisterloven som beskytter omtale av politiets metoder. Vi mente det var voldsomt at den offisielle og regelmessige kommunikasjonen mellom Kripos og POD kunne holdes vekk fra borgerne for alltid. At rapporten var flere år gammel, talte sterkt for merinnsyn. Pressen har en viktig kontrollfunksjon, og opplysninger som i utgangspunktet må unntas i 2016 bør i større grad utleveres fem år senere. POD skrev også at dokumentene inneholdt opplysninger som, hvis det ble gitt innsyn, ville «lette gjennomføringen av straffbare handlinger». Denne unntakshjemmelen gjelder imidlertid bare opplysninger, og ikke hele årsrapporter. Vi klaget, og saksgangen her var oppsiktsvekkende treg og verdt å fremheve:

Den opprinnelige innsynsbegjæringen ble sendt den 12. mai 2021, avslått tre uker senere, før det tok nye tre uker å få en utvidet begrunnelse. Jeg klaget en uke senere, men det var først etter en purring i september – hvor jeg tok med Justisdepartementet på kopi for sikkerhets skyld – at noe skjedde. Departementet påla POD å få opp farten, men det tok ennå en full måned før avslaget ble delvis omgjort i slutten av oktober.

Det tok med andre ord *fem måneder og to uker* å føre en i utgangspunktet helt ordinær innsynsprosess til slutten. Det sier seg selv at det blir vanskelig å kontrollere det myndighetene gjør når selv lovens håndhever forholder seg til offentlighetsloven på denne måten.

5.2 Kontrakten

Også de direkte innsynsforespørslene var trælete prosesser, skulle det vise seg. Den «enkleste» var kontrakten mellom Palantir og politiet – den tok kun et kvartal, fra opprinnelig begjæring i mai til innvilget innsyn i september. Da kontrakten endelig kom, oppdaget vi imidlertid at et av de sentrale dokumentene vi var blitt innvilget innsyn i kun inneholdt *oddetallssidene*. Et mer enn 200 sider langt dokument var halvert. Vi tok kontakt umiddelbart, både på telefon og e-post, for å få fikset det vi antok måtte være en ærlig glipp så fort som mulig. Men det tok fortsatt mer enn en uke før riktig versjon av dokumentet ble oversendt.

Da kontraktdokumentene endelig kom i riktig format, ble de svært viktige for saken. I dem fantes det som knapt finnes i postlistene, nemlig den konkrete kommunikasjonen mellom politiet og Palantir – med deres egne ord. Dette var ikke møtereferater eller dokumentasjon av direkte samtaler, men det var et viktig vindu til å forstå hvordan de to partene forsto seg selv og presenterte seg selv for hverandre. Da vi leste gjennom dokumentene, så vi tydelig den dynamikken som vi hadde vært nysgjerrig på fra starten – hvordan et mektig tech-selskap møter en ivrig etat fra et lite land.

Politiet gjentok flere ganger at dette hadde de *ingen* erfaring med. De understreket at «kontraktøren burde ta med sin fulle erfaring fra lignende etater og andre utrullinger, og ikke nøle med å foreslå bedre måter å løse behovene». Palantir på sin side svarte med innfløkte beskrivelser av det som i bunn og grunn er søkefunksjonalitet, og understreket selskapets «komplette dedikasjon til vårt mål om å bemektige kundene til å bruke data for å oppnå transformative resultater».

Dette ble et svært viktig moment i saken.

5.3 Reiseregningene – var «teknologituren» en nøkkel eller et blindspor?

Begjæringen om reiseregningene til IKT-sjefen ble først avslått fordi de var så gamle at de nå var arkivert i et annet system. Dermed mente POD at de ikke lenger kunne regnes som dokumenter. Det avslaget var åpenbart feil – at et dokument er arkivert og dermed vanskelig tilgjengelig er beklagelig, men ingen god grunn til hemmelighold. Vi klagde, og fikk medhold i klagen, men igjen tok det uker og måneder å få tak i de riktige reiseregningene.

Et større problem var at ingen av reiseregningene vi til slutt fikk ut fra tiden før Palantir-kontrakten ble inngått, viste noen tur av typen jeg hadde hørt om. Hadde kilden tatt feil?

På dette tidspunktet hadde jeg snakket med kilder som ikke var direkte tilknyttet Omnia-prosjektet, men som hadde kjennskap til det. Jeg tok kontakt, og spurte om de hadde hørt om en slik tur. Det hadde de – men den hadde skjedd på vårparten 2017, mente de. Og altså *etter* at kontrakten var inngått. Det ga en ny runde innsynsforespørsler, denne gangen tok det «kun» to og en halv uke å få svar, og i svaret fant jeg en tur til California i mars 2017 registrert. Nærmere forespørsler til POD viste at de kalte det en «teknologitur», og at en rekke personer i PODs ledelse var med på besøkene i Palo Alto, San Fransisco og Seattle.

Dermed hadde vi fått verifisert to ting: For det første hadde denne turen skjedd, men for det andre – den hadde skjedd *etter* kontraktsinngåelse. Hvilken betydning hadde turen da for hvordan Palantir-prosjektet vokste ut over sine egne rammer og ble en fiasko? Vi visste at det var lite sannsynlig at disse lederne som var med på turen ville stille til intervju. De hadde ikke gjort det tidligere. Håpet lå i § 9-innsynsbegjæringen: Hvis jeg kunne se hvordan IKT-sjefen og de andre øverst i systemet snakket med Palantir, kunne det gi noen svar.

5.4 § 9-innsyn i kommunikasjon i prosjektet

Den første § 9-begjæringen om kommunikasjonen mellom PODs folk og Palantir ble sendt tidlig på sommeren 2021. Etter en runde med tilbakemelding om at kravet vårt var for vidt, konkretiserte vi det ned til en noe kortere tidsperiode i 2017, til færre personer og til kommunikasjonen om utvidelsen av Omnia-prosjektet til å også inkludere en analyse- og informasjonsbehandlingsdel. Vi valgte oss ut IKT-ledelsen i POD, sjefen og hans nestledere – og tenkte at andres kommunikasjon eventuelt kunne følge senere. Så feil kan man ta.

Hele august og september gikk, uten at det kom noe svar på den oppdaterte begjæringen. Vi klaget til Justisdepartementet og ba dem behandle kravet i stedet – det førte kun til at departementet ba POD få opp farten. Så, i oktober, fikk jeg plutselig en e-post fra en saksbehandler i POD. De hadde ved en inkurie oversett forespørselen min, sa han, men nå ville han gjerne hjelpe. Jeg gjentok innsynsbegjæringen, og håpet på det beste.

Et par dager senere begynte så den mest besynderlige delen av prosessen:

En mandag morgen dumpet en e-post inn i innboksen, med 12 vedlegg. Da jeg begynte å gå gjennom dem, viste det seg imidlertid at det var hele kontrakten med Palantir, *på nytt*. Så, utover dagen, fortsatte e-postene å komme: Jeg fikk tilsendt e-poster fra journalister i NRK og Politiforum, innsynsbegjæringer *de* hadde sendt og dokumentene de hadde fått ut til svar. Til slutt satt jeg med flere titalls dokumenter, og ingen av dem hadde noe med § 9-begjæringen min om kommunikasjonen mellom politiet og Palantir å gjøre.

Vi konfererte i redaksjonen, og med Sindre i Presseforbundet: Skulle vi bare la dette surre og gå, og håpe at de kom til poenget til slutt – og at det kanskje dukket opp noe annet verdifullt underveis? Vi bestemte oss likevel for å ta kontakt og forklare at noe var feil: Det var viktig at arkivet ikke brukte mer tid enn nødvendig på *feil* saksbehandling, når det allerede var så vanskelig å få til den riktige.

Det viste seg at saksbehandleren i POD hadde misforstått begjæringen vår, og trodde vi ba om *alle journalførte dokumenter* i saken for perioden. Vi presiserte på nytt, for tredje gang, hva kravet faktisk gjaldt.

Den 21. oktober, tre måneder etter at begjæringen først ble sendt, kom endelig en faktisk behandling av innsynskravet. Det ble avvist på alle punkter – det Morgenbladet har bedt om er ikke en sak etter § 28, skrev POD, men et *tidsrom* eller eventuelt en dokumenttype (e-poster og SMS-er). Det springer mange saker ut av Omnia-prosjektet, skrev de, og det var ikke tilstrekkelig presisert hvilken sak vi ba om.

Så fulgte det mest påfallende: POD skrev at uansett om det vi ba om *var* en sak, ville de ikke kunne utlevere noen e-poster, for personene det gjaldt hadde sluttet i POD og e-postene dermed var slettet.

- Dette er oppsiktsvekkende: Arkivplikten går lenger enn journalføringsplikten, og vi hadde fra tidligere sett hvor få dokumenter som var å finne i postlistene om dette prosjektet.

På dette punktet hadde jeg også, etter nye runder i postlistene til Politidirektoratet, oppdaget noe interessant:

- En rekke dokumenter i dette prosjektet var arkivert mange måneder og noen ganger år etter at dokumentene ble opprettet. Påfallende mye av dokumentasjonen som var å finne var journalført omtrent samtidig, våren 2018. Da gransket politiets internrevisjon Omnia-prosjektet, visste vi, og da dukket altså mange måneder gamle dokumenter opp i postlistene.

Det var en viktig innsikt, hentet fra noe så banalt som å sammenligne dokumentdato og publiseringsdato i Einnsyn-portalen, som beviste at journalføringen i dette prosjektet åpenbart var mangelfull. Men her mente altså POD at alle e-poster som var verdt å arkivere, var å finne i postlistene. Eventuelt annen kommunikasjon som kunne belyse prosessen da Palantir kom inn i det norske politiet, nå var slettet.

Dette fremstod for oss som både mangelfull arkivering og journalføring, og som uhjemlet sletting av arkivverdig materiale – rett og slett et mulig lovbrudd.

Når e-postene var slettet var det lite sannsynlig at en klage kunne vinne frem og faktisk gi uttelling i form av dokumenter. Men det var en viktig prinsippsak her: Vi *hadde* bedt om en sak, mente vi, og det var viktig – for oss, og for senere undersøkelser av denne eller andre saker – at POD anerkjente det.

Vi klagde derfor på PODs avvisning av at vi hadde presisert saken godt nok, og viste på nytt til den helt konkrete avgrensingen vi hadde gjort (konkrete personer, et konkret aspekt ved Omnia-prosjektet, og en konkret tidsperiode). Gjennom pandemien har flere andre redaksjoner brukt samme paragraf til å få ut kommunikasjon om f.eks. skolestenginger i en gitt tidsperiode mellom navngitte personer – dette var ikke noe annerledes.

PODs saksbehandler var lite lysten på å sende klagen over til Justisdepartementet, viste det seg. Han ringte og spurte om vi ikke kunne droppe det – «e-postene er jo uansett slettet, det kan ikke ha noe for seg å belemre Justis med dette?», sa han. Jeg insisterte på at jeg ville klage på deres forståelse av hva som er en sak etter § 28, og en uke senere fikk jeg endelig kopi av klageoversendelsen.

Der hadde Politidirektoratet snudd fullstendig: Helt innledningsvis i klagevurderingen skrev POD at de nå la til grunn at «innsynskravet i tilstrekkelig grad identifiserer en bestemt sak». Deretter fulgte en nærmere beskrivelse av hvordan e-postene til personene innsynskravet gjaldt nå var slettet, og at POD ikke hadde grunn til å tro at de hadde inneholdt arkivverdig materiale.

Her fikk vi altså medhold – fem måneder etter at begjæringen ble sendt – om at det vi hadde bedt om var en sak. Det var en viktig seier, og det burde aldri tatt så lang tid.

6 Palantir: hermetisk stengt

Omnia-prosjektet hadde etter alle solemerker blitt en verkebyll, også for Palantir. Heller ikke de ønsker forsinkelser og krangling når de skal levere programvare, og vi var nysgjerrige på hvordan Palantir selv anså dette prosjektet. Det skulle imidlertid vise seg å bli en vegg vi ikke maktet å forsere. POD har vært oppsiktsvekkende vanskelige i dette prosjektet, men det er ingenting sammenlignet med forsøket på å få Palantir til å svare.

Innsynsarbeidet vårt avslørte kun noen få navn på Palantir-ansatte som hadde vært involvert i prosjektet hos det norske politiet. En sjekk på Linkedin viste at ingen av disse jobbet i Palantir lenger – og våre henvendelser til dem forble ubesvarte, eller kom tilbake med beskjed om å kontakte «media@palantir.com». Det samme gjaldt andre norske ansatte i Palantir som jeg fant via Linkedin: ingen ville prate.

6.1 Metoder som kan bli nyttige senere

Metodisk kan det være verdt å merke seg at det kan være nyttig å mase, selv når man egentlig tror det er nytteløst. På et tidspunkt forsøkte jeg å få kontakt igjen med Palantir-kilder som allerede hadde latt være å svare på gjentatte forespørsler. Men denne gangen traff jeg en av dem på et heldig tidspunkt: han var på ferie, og hadde satt opp autosvar på e-posten, som også kom til meg – og i det var mobilnummeret hans. Det hadde jeg ikke funnet andre steder. Det var en god påminnelse om at man ikke vet hva man får før man spør.

Jeg har også hatt god nytte av to andre nettsider i arbeidet med denne saken. For det første har jeg brukt mye tid på Glassdoor.com, en side der ansatte kan skrive anonyme vurderinger av arbeidsgiveren sin. Denne siden brukte DN med stort hell i sitt arbeid med Equinor i USA-saken, leste jeg i metoderapporten deres fra 2020, og jeg tenkte at den kunne inneholde

nyttig info om Palantir også. Det stemte: Palantir er vesentlig mindre i Europa enn i USA, og ved å sortere vurderingene etter geografi fikk jeg en rekke beskrivelser av hvordan det var å jobbe i Palantir i Sverige og England og Tyskland. Så vidt jeg har kunnet se, har ingen norske Palantir-ansatte brukt verktøyet ennå. Siden hjalp meg likevel forstå jobben og hverdagen til Palantirs såkalte «*forward deployed engineers*» godt nok til at jeg kunne skrive presise henvendelser til dem jeg ønsket å få i tale, vise at jeg forstod hva jobben deres var og hva jeg ønsket fra dem. At ingen av dem var villige til å snakke, hindrer ikke at siden var nyttig: Kunnskapen om Palantirs organisering og arbeidsmetoder ble brukt da jeg forsøke å få Palantir til å tre frem fra skyggene i skrivingen av saken.

Den andre siden jeg vil nevne er RocketReach.co – som blant annet oppgir formatet på e-postene til et gitt selskap. Bruker de initialene til de ansatte, fornavn, fornavn.etternavn? Det kan du finne på RocketReach, og i denne saken måtte jeg kontakte mange mennesker som jeg ikke hadde e-posten til. Jeg ville helst ikke gå via presseavdelingen om jeg kunne unngå det, og med RocketReach kunne jeg gjette meg til riktig e-postadresse og ta kontakt direkte.

6.2 Kunnskap er (journalistisk) makt

Underveis i arbeidet med dette prosjektet, innså jeg at det ville være viktig å forstå selve *teknologien* til Palantir. Politi- og justisfeltet er et område der Morgenbladet knapt har kilder – vi følger svært sjelden blålysene. Dermed vurderte vi at vårt sterkeste argument for å få kildene til å prate var kunnskap om teknologien. Jeg ville vise meg som en vettug og kompetent samtalepartner for folk som jobber i politiet, men som jobber med IT-systemer i det daglige og som i bunn og grunn er IT-folk.

Ved hjelp av tidligere dekning i internasjonal presse og forskningslitteratur skaffet jeg meg en oversikt over de sentrale teknologiske begrepene: Palantir lager *semantiske nettverk*, der *objekter* organiseres *relasjonelt* etter en felles *taksonomi* – og så videre. Selv velger Palantir å vise frem teknologien som glatte visualiseringer, men forskere og teknologer har arbeidet med grunnprinsippene i tiår. Via Google kunne jeg søke etter forskning på denne teknologien, og sortere den etter forsker tilknyttet norske institusjoner som jeg visste var sterke på digital teknologi (NTNU, Forsvarets forskningsinstitutt, osv.). Slik fant jeg frem til flere fagartikler, og dessuten norske forskere som jobber på feltet. Samtaler med dem ble nyttig bakgrunnskunnskap da jeg etter hvert kom i kontakt med kilder i selve Omnia-prosjektet: Jeg kunne for eksempel spørre om de tekniske problemene bestod i å identifisere objektene i databasene, eller om det heller handlet om å i det hele tatt koble opp? Slike spørsmål gjorde at samtalen skiftet gir: Jeg opplevde at kildene gikk dypere i sine forklaringer og begynte å snakke friere.

Det samme gjaldt politifaglig terminologi. Politiets IT-systemer er et villnis av ulike databaser, som er koblet på ulike måter, som overlapper og inneholder opplysninger om alt fra DNA og dommer til telefonovervåkning. Dette brukte jeg mye tid på å finne hode og hale på. Særlig bachelor- og mastergradsoppgaver fra Politihøyskolen og de juridiske fakultetene viste seg å være nyttige for helt grunnleggende beskrivelser av hva politiet lagrer og hvordan. Med den kunnskapen kunne jeg komme med et velplassert «ja, du snakker om PO?» når en kilde begynner å beskrive et politiregister – og dermed forandret samtalen seg fra en halvt nølende beskrivelse til dyptgående og engasjerte utgreiinger om alt som er galt med Palantirs måte å drive IT-utvikling. Fagterminologi bør åpenbart brukes så lite som mulig i teksten som kommer ut av et graveprosjekt, men den er uvurderlig i kildesamtalene.

7 Behov for en lokkesak

7.1 Andre veier til målet

Samtidig som jeg jobbet meg gjennom listen over dem vi hadde identifisert som involvert i prosjektet, og forsøkte å få dem i tale, så jeg meg om etter kilder mer perifert forbundet med Omnia-prosjektet som muligens ville ta en prat. Én av dem viste seg å bli en nøkkel til saken. Denne personen hadde inngående kunnskap om prosjektet, selv om han selv ikke har noe med det å gjøre direkte. Vi gikk et par runder i redaksjonen på om vi burde kontakte ham – vi visste nemlig at det var en risiko for at det, via ham, kunne bli kjent for andre aviser at Morgenbladet jobbet med en sak om Palantir. Da vi likevel valgte å forsøke, var det i hovedsak av to grunner:

For det første var det åpenbart for enhver som var nysgjerrig på Palantir og søkte i postlistene at Morgenbladet jobbet med denne saken. Alle våre innsynsforespørsler ble journalført svært detaljert, med konkret beskrivelse av alt vi ba om innsyn i. Dette står i klar kontrast til hvordan departementets egne dokumenter er journalført, der saks- og dokumenttittel som regel er helt overfladiske. Videre visste vi at denne kilden hadde et godt kildenettverk i store deler av politiet. Gjentatte forsøk på å ta kontakt med folk direkte hadde i all hovedsak vært fruktesløse – vi trengte noen som kunne gå god for oss.

Det viste seg at gamblingen fungerte. Kilden ville gjerne prate da vi tok kontakt – dette var noen som er frustrert over pengene og ressursene politiet har brukt på å få Palantirs program til å fungere – og vi avtalte et møte. Over flere timer med samtaler, og en rekke e-poster i etterkant, sammenlignet vi notater, fant kunnskapshull som én eller begge satt med, og kilden var også villig til å dele dokumenter som POD hadde nektet meg innsyn i.

7.2 Forskningsprosjektet som lokket

Jeg valgte bevisst å ikke spørre denne kilden om han kunne introdusere meg til noen av hans kontakter i politiet disse første samtalene. Jeg ville bygge tillit og *vise* at vi var troverdige og seriøse om denne saken, ikke bare si det.

På dette tidspunktet, i oktober 2020, hadde vi nok dokumenter til å kunne skrive en sak om at problemene i Palantir-prosjektet fortsatt vedvarte, halvannet år etter at det formelt sett var avsluttet. Men det ville komme litt «ut av det blå» for Morgenbladets lesere å melde dette – de færreste hadde nok hørt om Palantir eller Omnia. Vi trengte derfor en anledning til å skrive en skikkelig introduksjon til problemkomplekset.

Noen uker tidligere hadde jeg kommet over et forskningsprosjekt som kunne fungere som påskuddet vi trengte. Et knippe internasjonale forskere hadde nettopp startet et arbeid for å studere såkalt «predictive policing» – forutseende politiarbeid. Forskningsprosjektet handlet om de samme overordnede problemstillingene som vårt gravearbeid: Hva vet vi om algoritmestyrt politiarbeid? Hvilke fallgruver er det når teknologien gjør inntog i politietaten? Hvor mye påvirkes alle de involverte av hypen om Silicon Valley?

En artikkel om forskningsprosjektet ble en perfekt anledning til å fortelle om Palantir, og gi et første innblikk i det som da var kjent om deres arbeid i Norge. Vi trengte ikke ha hele den norske historien på plass: Tvert imot håpet vi at denne saken ville gjøre det klart for kildene vi søkte at vi jobbet med saken, og at vi var troverdige, kunnskapsrike og verdt å prate med.

7.3 «Underdrivelse» som metode

Ett strategisk valg i denne lokkesaken, som stod på trykk i slutten av oktober, var å ikke tråkke så hardt på gasspedalen i beskrivelsen av nå-tilstanden i prosjektet som vi kunne. Jeg satt på informasjon om at det var betydelige svakheter og forsinkelser i prosjektet, men endte med å sammenfatte disse rimelig kort og underdrevet:

Vi skrev at det var problemer med å sende e-poster via Omnia-systemet, men gikk ikke inn i detaljene på hvor omfattende problemene var. Vi visste for eksempel at det gjaldt for alle politiregistrene som skulle kobles til Omnia, men nevnte bare ett.

Dette var fordi jeg visste at det fortsatt fantes kilder rundt om i Norge som var frustrert over at Omnia ennå ikke fungerte. Vi håpet det ville være forlokkende å snakke med noen som åpenbart kjente prosjektet godt, men som likevel «ikke hadde fattet omfanget» skikkelig.

8 Samtalene og dokumentene kommer sammen

Lokkesaken fungerte. Samme fredag som den stod på trykk, sendte jeg den til et knippe kilder jeg hadde snakket med og stolte på, og spurte om de kunne tenke seg å sende den videre til deres kontakter – med beskjed om at jeg gjerne ville prate.

Allerede mandagen etter kom telefonen vi hadde håpet på:

En i politiet som hadde vært deltager i prosjektet hadde lest saken, og ville prate. Han tok kontakt, vi avtalte et møte i Morgenbladets lokaler, slik at vi kunne snakke uforstyrret – og den samtalen ble en hovednøkkel til saken som etter hvert kom på trykk.

Vi valgte å la denne kilden være anonym på trykk: Han ble omtalt i saken som «Johansen». Jeg snakket lenge med ham selv om det, og selv om han nå gjerne ville prate om Omnia, var han bekymret for å bli navngitt. Han fortalte om til tider svært amper stemning i prosjektet, med hissig krangling og ett tilfelle der det ble truet om personalsak da Johansen og hans kolleger stilte spørsmål ved Palantir-prosjektets gjennomførbarhet. Dette hadde vi også bekreftet fra dokumenter vi hadde fått tilgang til. Selv om Johansen ikke lenger er direkte involvert i Omnia, var det grunn til å tro at det kunne få konsekvenser for ham, og for hans nære i politiet, om han ble navngitt.

Vi visste at Johansen tidligere hadde vært i kontakt med journalister om denne saken. Samtalene viste seg likevel å bli mer fruktbare enn jeg kunne drømme om på forhånd. I månedene etter at Palantir-problemene først ble omtalt i mediene hadde nemlig Johansens arbeidshverdag forandret seg: Nå var han i en posisjon der han kunne fortelle om sine erfaringer på en friere måte enn tidligere.

Dette viser hvor nyttig det kan være å forsøke å grave på nytt i prosjekter der andre medier tidligere har snust. Tid kan være en viktig faktor i hva en kilde kan fortelle, og med litt større avstand til hendelsene kan det bli mulig å kaste lys over beslutninger og prosesser som har store konsekvenser for borgerne, men som de involverte i første omgang ikke kan snakke om.

8.1 Dokumentene åpner seg opp

Samtalene med Johansen var svært viktige, og ikke bare for det han selv kunne fortelle direkte. For det første var det en aha-opplevelse å gå tilbake og lese dokumentene jeg hadde fått innsyn i, etter å ha snakket med han. Nå ga opplysninger og formuleringer som jeg tidligere ikke hadde bitt meg merke i, ny mening.

Ett dokument, en e-postutveksling jeg hadde fått mer enn seks måneder tidligere, inneholdt en beskrivelse av hvordan Palantir hadde tilbudt «en opsjon» i forbindelse med kontraktsforhandlingene. Dette forstod jeg ikke, og ting man ikke forstår er vanskelige å huske. Men Johansen beskrev inngående hva denne opsjonen bestod i: *Dette* var den beryktede «analyse- og informasjonsbehandlingsdelen» – bare beskrevet med andre ord. Ved hjelp av Johansens forklaringer og beskrivelsene i dokumentene ble det tydelig at «analysedelen» var del av Omnia hele veien, men det hadde variert hvor omfattende den skulle *brukes*. Tidligere artikler om Palantir hadde omtalt dette som en kritisk forandring i prosjektet, men i realiteten hadde frøet til fiaskoen – formålsutglidningen, ressursene som manglet når prosjektet vokste, uenighetene om hvilke av politiets databaser som skulle kobles til Palantir – vært der fra starten, helt siden Palantir første gang begynte å selge seg inn som en attraktiv partner for politiet. Nå hadde jeg to sterke kilder som underbygget dette, uavhengig av hverandre.

Ved hjelp av Johansens forklaringer kunne jeg også forstå det som ble sagt i det ene direkte møtet med Palantir som finnes i postlistene: Én e-postutveksling mellom et par Palantir-folk og prosjektlederen er journalført, og jeg hadde fått innsyn i den, men innholdet ga knapt mening. Etter å ha gått gjennom kronologien i prosjektet med Johansen, forstod jeg imidlertid både hva de pratet om i utvekslingen, og også hva det betydde at Palantir var villige til å gå på et økonomisk tap for et problem som ikke var deres feil. Problemet *måtte* løses om politiet noensinne skulle benytte opsjonen om utvidet bruk av Palantirs programvare – klart det var i Palantirs interesse å være rause mens POD jobbet med saken.

8.2 Andre kilder får riktig argument for å snakke

Samtalen med Johansen ble også nøkkelen som fikk andre kilder med tilknytning til Omnia-prosjektet til å åpne seg. Gjennom Johansen fikk jeg et klarere bilde av hva som hadde vært den sentrale konfliktlinjen i prosjektet: Jeg hadde trodd det var snakk om én side som ikke ville ha Palantirs teknologi og spilte opp feilene, og en annen som var godt fornøyd og som ville forsvare det. Men etter å ha pratet med Johansen, forstod jeg at *alle* her var misfornøyde – også de som i utgangspunktet ville at Omnia skulle fungere.

Det gjorde at jeg endret fremgangsmåte i de neste fremstøtene mot kildene: Når kildene først tok telefonen, snakket jeg om hvor frustrerte de måtte være for hvordan dette hadde gått på tverke – og dessuten hvordan bare én fortelling om prosjektet hadde kommet frem til nå. Jeg ville gjerne høre deres side av historien, om de ville ta en prat? Det ville flere, dette var åpenbart et mer fornuftig tilbud enn å forsøke å få dem til å forsvare Omnia i nåværende form. Slik fikk jeg nye opplysninger om prosjektet, som både bekreftet og motsa Johansens fortelling. Fra da handlet mye av jobben om å kontrollere opplysninger via dokumenter og oppfølgingssamtaler. Blant annet viste disse samtalene at den beryktede «teknologituren» til California – som jeg hadde brukt så mye tid på å få reiseregningene fra – antageligvis ikke var sentral. De kildene som mente turen var viktig, tidfestet den på vidt sprikende måter og hadde kun mistanker og antagelser å komme med om turens innhold og betydning. Mens de som presist og på egenhånd kunne fortelle om turen, beskrev den som lite viktig – prosjektet hadde begynt å gå galt før sjefene dro til USA. Dermed droppet vi turen fra saken.

Sjefene i Omnia-prosjektet, og den daværende IKT-ledelsen i politiet, ville fortsatt ikke la seg intervjue til saken, selv med denne nye tilnærmingen. Det var som forventet – og for vårt prosjekt var det ikke essensielt. Det vi hadde satt oss fore å finne ut, var hvordan dette møtet mellom et «Big Tech»-selskap og det norske politiet hadde foregått. Vi ville dokumentere offentlig det som hadde foregått bak scenen da disse to mektige institusjonene begynte å samarbeide. Det kunne vi nå beskrive på en veldokumentert måte.

9 Organisering av arbeidet

Dette er et prosjekt jeg har jobbet med på egenhånd som journalist. Vi var så heldige å få støtte fra Fritt Ord, slik at jeg kunne frikjøpes fra den daglige avisproduksjonen og konsentrere meg om arbeidet med denne saken i et par måneder. Det viste seg å være viktig: Som nevnt har Morgenbladet lite erfaring med denne typen store gravesaker og innsynsarbeid, og det har vært krevende å skaffe oversikt over saken, over dokumentene og å bli kjent med lovene. Det gjelder både offentlighetsloven, som man aldri blir utlært i, og dessuten spesiallovene som regulerer politiets registre og som ble mye brukt for å avslå innsynsbegjæringer. Det kunne vært nyttig å være flere journalister på dette prosjektet – det kan bli vel mye indre monolog når man jobber alene – men samtidig vil soloarbeid ofte være nødvendig i en liten redaksjon. Det var tilfredsstillende å se at det var mulig å fullføre prosjektet uten et stort team.

Selv om jeg har vært eneste journalist på denne saken, betyr det ingenlunde at jeg har vært alene. Kolleger i Morgenbladet har lyttet og sparret, og vi har hatt jevnlige møter med reportasjeleder og redaktør for å snakke om fremdrift, mulige endringer og strategier for å komme videre. Jeg har dessuten vært så heldig å få ha kontinuerlig dialog med jurist Sindre Granly Meldalen gjennom nesten hele prosjektet. Han har sparret om formuleringer for innsynsbegjæringer, hjulpet meg tolke avslag og legge strategi for klagene, og sukket sammen med meg over hjemmelsurr og treghet i POD. Uten ham hadde vi aldri fått dokumentene, eller innrømmelsene om offentlighetsloven, som vi til slutt fikk.

10 Dette er nytt

I dette prosjektet har Morgenbladet for første gang dokumentert *hvordan* dette første møtet mellom det norske politiet og Palantir har gått. Vi har – via dokumenter og samtaler – kunnet vise frem iveren etter å få et nytt og kult dataverktøy som preget alle de involverte. Dette er en iver som både politiet og Palantir delte, men som ikke nødvendigvis vil deles av borgerne som overvåkes med Palantirs teknologi.

Vi har dokumentert hvordan opplysninger som aldri skulle vært fôret inn i Palantirs systemer, likevel ble inkludert – sannsynligvis i strid med både politiregisterloven og Norges personvernlovgivning.

At slike problemer siden ble rettet opp, hindrer ikke at de er viktig å dokumentere offentlig: Det er først når vi vet om feilene at vi kan ha en opplyst diskusjon om fordelene og ulempene ved at politiet tar i bruk ny og kraftig teknologi.

Sakene i Morgenbladet har dokumentert hvordan Palantir snakker når de henvender seg til myndighetene i Norge. Selskapene forteller store historier om alt de kan få til, og tegner teknologien som unikt kraftig og viktig. Dette er viktig å dokumentere, for det gjør det mulig å ettergå påstandene i etterkant: Leverer de det de lover, løser de problemene som de får skattebetalernes penger for å fikse?

En sentral problemstilling for journalister som vil holde oppsyn med det offentlige er bruken av konsulenter. Én sak er kostnadene – Aftenposten har tidligere dokumenter hvor mye Omnia har kostet i form av konsulentbruk. Like viktig er det faktum at med innleide konsulenter øker risikoen for ansvarspulverisering. I arbeidet med denne saken har vi gjentatte ganger blitt møtt med beklagelser fra konsulenter som ikke kan snakke på grunn av taushetsplikt om tidligere oppdrag. Mange kilder kan ha slike forpliktelser – og iblant velger de å ignorere dem – men for konsulenter virker det ekstra vanskelig: De har dobbel

taushetsplikt, både overfor prosjektene de har vært utleid til, og overfor egen primærarbeidsgiver. Da skal det enda mer til for å velge å snakke om kritikkverdige forhold, selv mange år senere.

Morgenbladets saker om Palantir-prosjektet viser hvordan dette kan spille ut i praksis: Med hyppig utskifting av både innleide konsulenter, og egne ansatte, var det til slutt knapt noen i POD som faktisk kjenner prosjektets gang. De har ansvaret, men ikke innsikten. De offisielle svarene fra POD om Omnia bærer preg av dette – den nåværende ansvarlige for prosjektet hadde rett og slett ikke informasjonen vi etterspurte. Dette vanskeliggjør pressens kontrollfunksjon.

Morgenbladet har også avslørt at Palantir forsøkte å selge seg inn til norske *helsemyndigheter* da pandemien traff Norge – med samme type innsalg som de i sin tid brukte hos politiet. Direktoratet for e-helse er neppe siste etat som mottar et «godt tilbud» fra Palantir, eller fra de andre mektige teknologiselskapene som former livene våre. Facebook er allerede intranett-leverandør for en rekke norske etater og kommuner, Google jobber for å bli større innen helseteknologi.

Hvis entusiasmen som Morgenbladet har dokumentert fra møtet mellom politiet og Palantir er en indikasjon, bør pressen følge nøye med i fortsettelsen.

11 Funn og konsekvenser

Sakene om Palantir i Morgenbladet er ikke av typen der noen måtte gå: Avsløringen var allerede ute. Vi mener likevel det har vært viktig å gå i dybden i denne saken, fordi fortellingen om det som gikk galt da Silicon Valley møtte norsk politi bør dokumenteres og diskuteres offentlig. Dette er to svært mektige aktører som begge har interesse av å samarbeide, og av å holde detaljene om samarbeidet så hemmelige som mulig. Deres visjon om å bruke teknologi for å vite mest mulig om borgerne er ikke nødvendigvis noe borgerne ønsker. Slike møter vil også fortsette å skje – nye forsøk på samarbeid mellom teknologiselskaper og norske myndigheter vil komme. Innsikten om hvordan det gikk galt da Palantir og politiet kom sammen vil være viktige når pressen skal holde oppsyn med denne arenaen for maktutøvelse i fremtiden.

- Morgenbladet har dokumentert hvordan Politidirektoratet har hatt svært mangelfull og til dels lovstridig journalføring over mange år. Dokumenter i viktige saker er journalført sent eller aldri, og e-poster vi ikke vet innholdet i, er slettet. Dette forvansker pressens jobb med å ettergå etaten betraktelig. Dette er særlig kritisk i politietaten, som har myndighet til å utøve vold mot borgerne.

- POD har en svært problematisk praktisering av offentlighetsloven. Sendrektighet og surr med lovhjemler er et problem i enhver etat, men det er særlig kritisk at de som er satt til å håndheve loven er så dårlig til å følge den. Igjen gjør dette det vanskeligere for pressen å utøve sin kontrollfunksjon med en etat som mottar 19 millioner kroner i året over statsbudsjettet, og som holder oppsyn med politiets årlige budsjett på mer enn 20 milliarder kroner.

- Sivilombudet har rettet skarp kritikk mot POD for hvordan de håndterer innsynsbegjæringer. Ombudets undersøkelser har avslørt at PODs praksis har vært å ignorere begjæringer av en viss alder som ikke blir purret. Dette er det ikke hjemmel for i offentlighetsloven, påpeker ombudet.

- Prosjektet har dokumentert ansvarspulveriseringen som oppstår når innleide konsulenter tar over oppgaver i staten, og hvilket hinder konsulentene kan være mot offentlig innsyn i viktige prosesser. Saken har også understreket risikoen i at viktige dokumenter kan forsvinne når ansatte og konsulenter beveger seg videre til nye stillinger, og e-postene deres blir slettet – slik de er blitt i denne saken.

- Saken har dokumentert et tydelig eksempel på hvordan den norske stat forholder seg til «Big Tech». Myndighetene har fremvist en oppsiktsvekkende vilje til å la et mektig, privat selskap legge føringene for et prosjekt som har store konsekvenser for borgerne.

- Siden den første saken ble publisert er det kommet en rekke tips til redaksjonen om lignende problemer i andre offentlige IT-prosjekter. Det er krevende for en liten redaksjon å følge opp alle tips, men disse sakene ligger åpenbart der ute – for Morgenbladet eller for andre redaksjoner.

- Det er fornyet interesse for et aktuelt lovforslag fra Justisdepartementet, som vil at PST – som ifølge flere uavhengige kilder bruker Palantirs programvare – skal ha mulighet til å samle inn og lagre store deler av det åpne nettet. Både EOS-komiteen på Stortinget og en rekke andre høringsinstanser er svært kritiske til hvor bredt og vagt lovforslaget er formulert, slik Morgenbladet har skrevet om.

- Danmark har tidligere gjort en lignende lovendring som den som nå diskuteres i Norge, og konsekvensene av denne ble nylig omtalt og diskutert i Morgenbladet. Perspektivene fra Danmark er dermed blitt løftet inn i den norske pågående debatten.

11.1 En anklage og en kaffeinvitasjon fra Palantir

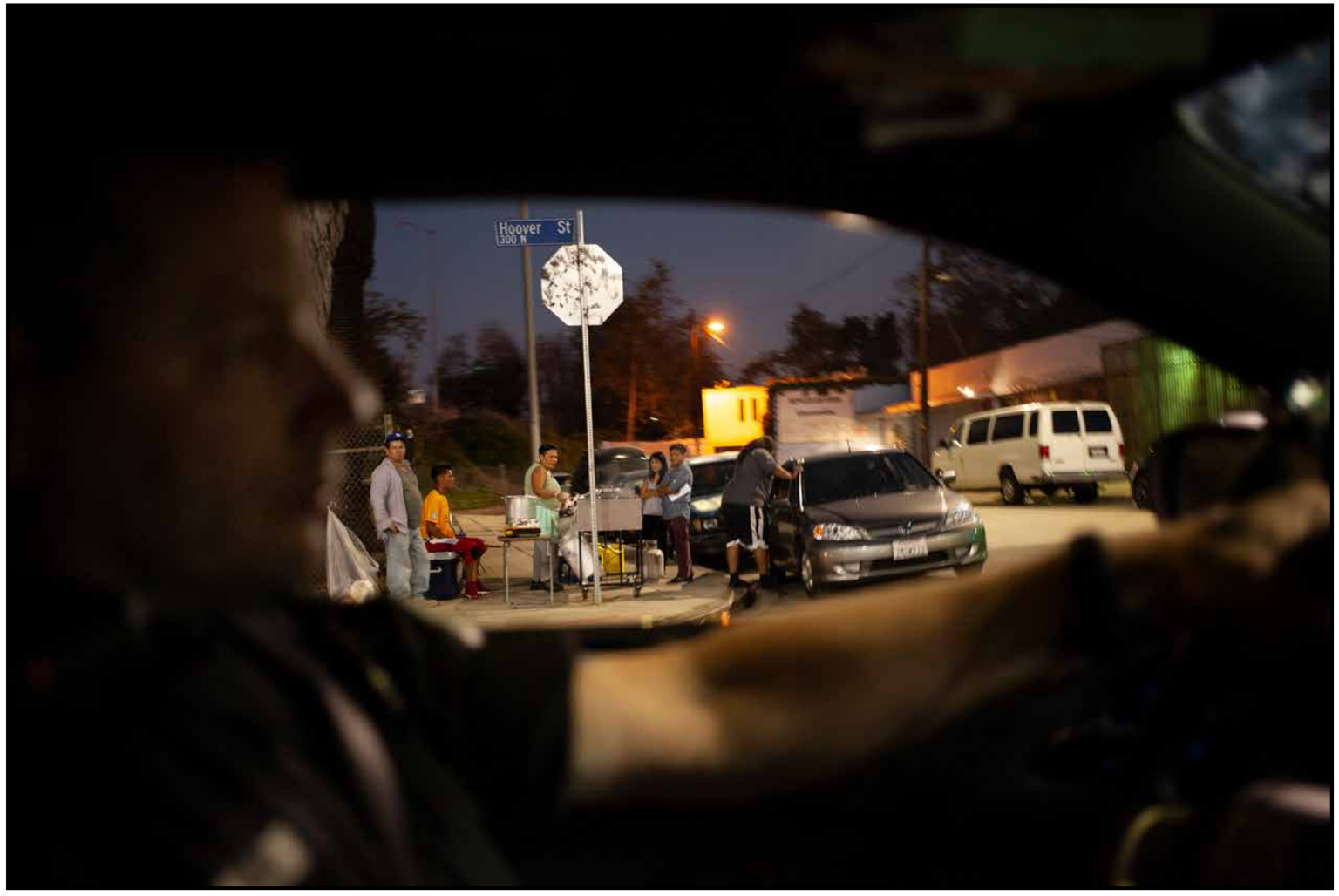
På et offentlig seminar i Danmark i desember 2021 ble en representant for Palantir spurt om Morgenbladets dekning av deres jobb i det norske politiet. Representanten svarte med å påstå at sakene våre inneholdt «en rekke feil og unøyaktigheter», og selskapet ville kontakte Morgenbladet om dette. I skrivende stund har Palantir ennå ikke tatt kontakt, og noen nærmere spesifisering av hva som skulle være feil i vår dekning er ikke kommet.

Vi kan likevel ikke være sikre på at påstanden ikke har hatt betydning. Det var folk til stede på dette arrangementet som vi kan ønske å snakke med i fremtiden, i Morgenbladets pågående dekning av teknologi og teknologidebatt. Disse kildene kan nå sitte med et inntrykk av at Morgenbladet er upålitelige.

Omtrent samtidig med dette seminaret, tikket det imidlertid også inn en e-post fra en annen representant for selskapet, med det første fyldige svaret Palantir har kommet med i Morgenbladets arbeid. Dette var i anledning saken om Palantirs tilbud til Direktoratet for e-helse om hjelp til pandemihåndtering – og representanten sendte oss en rekke formuleringer som de tydeligvis ofte bruker: De samme setningene har stått på trykk i for eksempel The Guardian. Men samtidig lurte representanten på om vi ikke kunne tenke oss å møtes for en kopp kaffe og en prat om Palantir? Det kunne gi *oss* en mulighet til å lære mer om Palantir, skrev han – og representanten kunne kanskje få en følelse av hva *de* kunne gjøre for å være mer åpne og transparente i Norge. Vi takket ja til invitasjonen.

Ny teknologi setter stadig flere av oss i politiets søkelys

OVERVÅKNING *Omstridte Palantir lager datasystemer for norsk politi. I både Norge og resten av verden er bruken av avanserte programmer i ferd med å forandre politiet selv.*



I søkelyset: I oktober 2016 var Joel Miller, en sersjant i Los Angeles Police Department (LAPD), på patrulje, og observerte et ulovlig gatekjøkken i det sentrale Los Angeles. Om Miller stopper og snakker med noen når han er ute, blir informasjonen om både samtalen og alle tilstedeværende fylt ut på et feltintervjukort, som siden fôres inn i datasystemene. Der kan Palantirs programmer sammenstille informasjonen med data fra sosiale medier, fra justissystemet og en rekke andre registre. Slik vet politiet stadig mer om dem de skal beskytte og tjene.
FOTO: KNUT EGIL WANG

HANNE ØSTLI JAKOBSEN

Teknologi virker objektivt, ukontroversielt, kvantitativt. Når du glatter over det menneskelige elementet, skjønnsavgjørelsene som er bakt inn, kan du si at «det er bare matte», og miste de problematiske sidene av syne.

Det sier sosiologen Sarah Brayne på telefon fra morgenpendlingen i storbyen Austin i USA. Brayne, som jobber ved University of Texas i Austin, har gjort det som nå anses som en liten sosiologisk bragd: I 2013 fikk hun adgang til politiet i Los Angeles, et av de største politidistriktene i USA, og fikk bli med dem for å observere hvordan de bruker avanserte dataprogrammer i arbeidet.

Braynes mål har vært å finne ut hvordan politiet bruker *predictive policing:* dataverktøy og metoder som benytter analyser av stordata for å forsøke å forutse hvor, eller av hvem, et lovbrudd vil begås. Los Angeles er blant de største kundene til analyseselskapet Palantir Technologies – som også leverer programvare til norsk politi.

Ved hjelp av kraftige dataprogrammer kan politiet gjøre mer finmaskede analyser av kriminalitetsstatistikk, finne sammenhenger og løse saker der de før sto fast. Men systemene lar også politiet kaste et stadig større overvåkningsnett over oss alle: Flere fanges opp og registreres i politiets databaser, uavhengig av om de har gjort noe galt. Og er du først blitt registrert inn, kan det være vanskelig å slippe ut igjen.

Resultatet av Braynes arbeid er boken *Predict and Surveil*, som kom ut på tampen av året i fjor. Tittelen er en bokstavrimende henvisning til det amerikanske politiets motto «Protect and Serve». Ikke *beskytt og tjen*, men *forutse og overvåk*.

– Teknologi har en makt og en mystikk som kan tåkelegge de menneskelige prosessene som inngår i teknologien. Det gjør det vanskelig å forstå hva som faktisk er problemet når noe går galt i politiarbeidet, sier Brayne.

– Hvem skal holdes ansvarlig: politimannen, avdelingen, programmet eller teknologiselskapet?

Synesteinene i Politidirektoratet

Også i Norge blir politiarbeid sakte forandret av dataprogrammer. Men kanskje ikke alltid helt som tenkt. Mest beryktet er politiets valg av Palantir Technologies som IT-leverandør.

Folk i sjefsstillinger elsker disse systemene. Menige offiserer hadde en tendens til å protestere mer.
SARAH BRAYNE

Analyseselskapet fra Silicon Valley ble grunnlagt av Peter Thiel og Alex Karp i 2003, og har kalt seg selv opp etter palantírene – synesteinene fra bokserien *Ringenes Herre*. I J.R.R. Tolkiens verden er dette magiske steiner som kan vise bilder av hendelser i det fjerne, det være seg langt bort, eller for lenge siden, eller det som kan skje i fremtiden. Virkelighetens Palantir lager datasystemer med navn som Gotham – etter byen der Batman bor – som kan sammenstille, sammenligne og analysere store mengder data.

Norsk politi inngikk en kontrakt med Palantir i 2016; selskapets system skulle gjøre politiet i stand til å utveksle fingeravtrykk og annen slik biometrisk informasjon med andre land i Europa og USA. Det skulle gjøre det lettere å svare når for eksempel Tyskland tar kontakt med en internasjonal etterlysning, eller vi spør tyskerne om en mistenkt her.

Søk gjennom systemene – har noen informasjon, fingeravtrykk, foto, av den mistenkte? Still det sammen med annen relevant informasjon og send det over. Kjapt, enkelt.

Palantir er en mytemaskin. Knapt en artikkel skrives om selskapet uten at teksten nevner både fantasy-opphavet til navnet (se over), og dessuten ryktet om at deres analyser var essensielle da amerikanerne fant og drepte Osama bin Laden i Pakistan i 2011. Hvor ryktet kom fra, er ikke godt å si. Selskapet har selv delt en nyhetsartikkel om det på sine nettsider, men vært vage og kledelig beskjedne når journalister har spurt. I en større profilartikkel om selskapet i New York Magazine skriver journalist Sharon Weinberger likevel: «Ingen jeg snakket med i nasjonal sikkerhet eller etterretning, tror Palantir spilte en viktig rolle i å finne bin Laden.»

Like fullt: Palantir har kunder over hele verden, både politi, etterretningsorganer, banker og private bedrifter bruker innsiktene deres. I mai 2017, et snaut halvår etter at kontrakten med det norske politiet var inngått, meldte nettavisen Digi.no at norsk politi var i gang med å bruke det «kraftige analyseverktøyet», som i norsk fatning har det fått navnet «Omnia» – «alt» på latin. Denne kunngjøringen skulle vise seg å være høyvannsmerket for prosjektet.

Blant andre Politiforum har skrevet om hvordan implementeringen av Palantirs programvare ble en verkebyll. Prosjektet este i både tid og kostnader – anskaffelsen som skulle koste 40 millioner kroner og være klar i 2018, har til nå kostet over 100 millioner. Det har vært tekniske problemer i koblingen mellom systemet og politiets databaser, og fagfolk har advart om Omnias evne til å ivareta personvernet.

→

PALANTIR OG PRÜM

- Politidirektoratet inngikk kontrakt med Palantir Technologies i desember 2016.
- Målet med anskaffelsen var å sette politiet i stand til å bli fullverdig del av det såkalte Prüm-samarbeidet, en avtale om grenseomskridende politisamarbeid i Europa. En tilsvarende avtale med USA heter PCSC, og forpliktelsene under den skulle også løses ved hjelp av Palantirs programmer.
- Da kontrakten ble inngått, skrev flere aviser om hvordan politiets nye «supervåpen» skulle hjelpe politiet bekjempe kriminalitet.
- Etter at prosjektet ble avsluttet i fjor, spurte stortingsrepresentant Lene Vågslid (Ap) daværende justisminister Monica Mæland om pengebruken.
- «Det kan se ut til at summen på 100 millioner er brukt på et prosjekt som foreløpig ikke har gitt noen resultater», svarte Mæland.

I starten av 2020, mens resten av Norge ble stadig mer opptatt av koronaviruset som spredte seg i verden, trakk Politidirektoratet i nødbremsen. Prosjektet ble avsluttet, uten at det var ferdig:

«Politidirektoratet (POD) har besluttet å avslutte Omnia-prosjektet selv om ikke alle kriteriene for prosjektavslutning er tilfredsstilt», skrev daværende avdelingsdirektør Kristin Kvigne i et brev til Kripos februar 2020.

Hvordan forebygge drapsforsøk: I august i år ble en tenåring knivstukket i Sandvika i Bærum; den unge gutten overlevde, men saken etterforskes som drapsforsøk. Gjerningspersonen er ennå ikke funnet. Forsker Helene Gundhus vil undersøke hvordan politiet bruker dataverktøy for å forsøke å forebygge ungdomskriminalitet.
FOTO: BERIT ROALD / NTB

«De vil bare ha det»

– Folk i sjefsstillinger elsker disse systemene, forteller Sarah Brayne om programmenes inntreden i LAPD.

– Menige offiserer hadde en tendens til å protestere mer. Av forskjellige grunner.

Politisystemet i Los Angeles er enormt, det jobber 13 000 politifolk og sivile i etaten. En av dem er Manuel (et pseudonym), han jobber i LAPDs tekniske avdeling og er hoderystende til datainnkjøp i avdelingen:

«Sjefene våre blir lett distrahert av det nyeste og flotteste skinnende leketøyet. Men de forstår ikke hva som kreves for at det skal integreres, og ingen tenker på hvordan det skal implementeres. De vil bare ha det», sier Manuel i Braynes bok.

I årene mellom 2013 og 2018 satt Brayne en rekke ganger bak i bilen mens politifolk var på patrulje. Hun hang med på helikopterutrykninger, intervjuet sjefer og fikk demonstrasjoner av programmene til Palantir og Pred Pol – et annet stort selskap innen forutseende politiarbeid. Blant dem Brayne møtte, var «Doug», en av Palantirs ingeniører som var utplassert hos LAPD. Han lot henne se på mens Palantirs programvare søkte etter en diffus beskrivelse av bilen til en mistenkt. Et par tastetrykk og noen omtrentlige antagelser om bilens alder og merke snevret søket inn fra 140 millioner registrerte kjøretøy til 13. Disse burde undersøkes nærmere, ifølge Doug. «Hva skjer om dere blinker ut feil person?», spurte Brayne. «Jeg vet ikke», svarte Doug.

Betjentene Brayne møtte på, var ofte mer skeptiske. Særlig dersom overvåkningen rammet dem selv, var det lite entusiasme å spore.

– Politifolk ønsker at deres egen ekspertise og intuisjon og erfaring skal bli verdsatt. De sier: «Jeg trenger ikke en algoritme», forteller Brayne.

Til tider fremstår politiarbeidet Brayne observerer i kjølvannet av dataanalysene, som smått absurd: Analyser av bruken av helikoptrene i Los Angeles viste etter hvert at et politihelikopter måtte fly over et utpekt «hotspot»-område 51 ganger per uke for å gi en merkbar nedgang i kriminalitetsstatistikken. Politiet valgte å legge på litt, og hang over det utvalgte området opp mot 90 ganger per uke. Ressursbruken får Brayne til å le over telefonlinjen fra Texas.

Hva med litt mer data?

Utenfor akuttmottakene i deler av Los Angeles har politiet satt opp automatiske registreringsskilt-avlesere. Iblant blir nemlig skadde etter gjengopprør bare sluppet kjapt av ved døren. Men hvis politiet kan registrere skiltene på bilene, kan de bygge seg opp kunnskap om hvem som kjenner den skadde – kanskje de er del av det samme kriminelle nettverket? Eller kanskje de er offerets mor eller bror, helt uten kriminell bakgrunn. Nå vel, nå er de i politiets databaser uansett.

Dette er en av Braynes viktigste konklusjoner fra arbeidet: Politiet registrerer stadig flere i sine systemer, men overvåkningen rammer ikke likt. I USA er det en klar økt risiko for at minoriteter og folk i fattigere områder havner i politiets systemer. Det kan rettferdiggjøre mer politinærvær, som igjen fører til nye møter med politiet, nye registreringer – og slik fortsetter sirkelen.

– I den norske debatten om Palantir er det blitt sagt at disse verktøyene hjelper politiet å vite det de allerede vet. Det flytter informasjonen politiet allerede har, ut av siloer, og gjør det mulig å se den i sammenheng. Er det et gyldig perspektiv?

– Det kan være delvis sant – ja, informasjon kan være lagret i siloer, og det kan være vanskelig å bruke den på tvers. Men det er to ting her: For det første oppstår det en vesensforskjell når du kobler sammen data, sier Brayne.

Sosiologen beskriver hvordan hun nå vet undertegnedes telefonnummer. Greit nok, én bit informasjon. Men hva så om hun kan finne ut hvor jeg bor, og hvor bilen min var parkert i går kveld, og hvem jeg bor med?

– Dette kan være informasjon som politiet har, men det å kombinere de ulike bitene kan være transformerende – det blir noe kvalitativt nytt. Og det kan ha implikasjoner for personvern og borgerrettigheter, sier Brayne.

– Det andre er at følgende ofte skjer: Et politidistrikt bestemmer at ok, vi skal ta i bruk det nye programmet med disse utvalgte datakildene. Så sier teknologiselskapet: «Vi har andre kunder som også har integrert *disse* datakildene. Ville det være nyttig for dere også?»

Det er ingen tvang med i bildet, understreker Brayne, bare et betimelig stilt spørsmål fra en god selger.

– Selskapene har en mellommann-rolle, som til slutt ender med at mer data mates inn i systemene.

De som står i fare for å skli ut

– Det er mange antagelser om hva forutseende politi er, og det har vært lite forsket på, empirisk, forteller Helene Oppen Ingebrigtsen Gundhus i lyset fra de øverste etasjene på Domus Juridica, jussbygget i Oslo sentrum.

Gundhus er en av 16 deltagere i det ferske forskningsprosjektet CUPP – *Critical perspectives on predictive policing* – som skal studere hvordan politiets bruk av avanserte dataverktøy fungerer i seks land i Europa. For Gundhus' del vil prosjektet konsentrere seg om ungdomskriminalitet:

Hun skal studere hvilke digitale verktøy politiet bruker i arbeidet med å forebygge ungdomskriminalitet, og særlig hvordan de jobber for å blinke ut risiko- og beskyttelsesfaktorer blant ungdommene politiet kommer i kontakt med. Hvem blant dem som begår ungdomskriminalitet, står i fare for å skli utfor, hvem trenger hva slags oppfølging?

– Det finnes ikke datadrevne systemer i bruk i norsk politi som automatisk henter inn data. Du har egne programmer som visualiserer og brukes til analyse, men dataene registreres inn av folk, forteller Gundhus.

– Så forsøker man å si noe *ut fra de dataene* – hvem man skal velge ut for videre oppfølging med tiltak, hvem skal man hente inn til bekymringssamtale? Der er det mange manuelle vurderingsprosesser som pågår.

Kriminologen definerer «predictive policing» som bruken av dataverktøy som kvantifiserer og analyserer, og dermed sier noe om hvor politiressursene skal settes inn.

– Er det prinsipielle betenkeligheter med at politiet kan bruke avanserte dataverktøy til analyser av egne registre?

– Ja, det krever en tolkningskompetanse. Det er viktig å ikke se på diagrammene og nettverkskartene som kommer opp, som statiske – de er dynamiske og krever tolkning. Det er problematiske sider ved å la dem bli en sannhet om miljøene de kartlegger, svarer forskeren.

«Det vil øke hvem som registreres i politiets registre»

I disse dager er Gundhus og hennes kolleger på feltarbeid i Oslo-politiet. Ett viktig forskningsspørsmål er om tilgjengelige dataverktøy endrer terskelen for hvem politiet registrerer i sine databaser.

– Slike systemers fortrinn er at en opplysning som er registrert og søkbar, er mer nyttig enn noe som står i en notisblokk ingen leser. Så det er vel ikke radikalt å tro at innføringen av disse systemene vil føre til mer registrering?

– Ja, det vil øke hvem som registreres inn i politiets dataregistre. Og det er mistenkeliggjørende om du finnes i politiregistre. Det er klart, sier Gundhus.

– Jo større del av ungdomsgruppen som ikke er registrert for kriminalitet fra før, som innlemmes i kartene, desto mer overvåkning blir det. Og hva gjøres med de som velges ut for videre oppfølging: Brukes risikovurderingene til å sette inn velferdstiltak, eller mer politikontroll?

Som Brayne har vist i sin studie fra Los Angeles: Bare det å finnes i en politidatabase kan forandre hvordan politiet ser på deg. Kanskje ble du registrert fordi du var sammen med en kompis på et uheldig tidspunkt – det var aldri deg politiet var interessert i. Men det faktumet er ikke like tydelig i et system som simpelthen peker på at «Per Hansen» er en bekjent av «Knut Pettersen», kjent kriminell.

Målet med prosjektet, sier Gundhus, er å lære mer om *hvordan* verktøyene brukes i dagens politi, men også å drive bevisstgjøring.

– Det er en intervensjonistisk del av prosjektet. Vi ønsker å skape en økt refleksjon og bevissthet om utfordringer ved å stole altfor blindt på det som er innhentet av data.

hj@morgenbladet.no

Det er mistenkeliggjørende om du finnes i politiregistre.
HELENE OPPEN INGEBRIGTSEN GUNDHUS

Palantirs norske system virker ennå ikke

ETTER *fem år og 100 millioner investerte kroner i Palantirs programvare sender politiet fortsatt fingeravtrykk med e-post.*

Palantir-programmet Omnia er fortsatt i bruk i politiet. Men fem år etter at kontrakten med det amerikanske teknologiselskapet ble inngått – og mer enn et år etter at prosjektet for å implementere systemet offisielt ble avsluttet – har Omnia fortsatt problemer.

Prosjektet ble «forsert avsluttet» i februar 2020. Det eneste arbeidet som skulle skje videre, var småplukk som skulle få systemet så klart at det kunne godkjennes under Prüm-avtalen – en overenskomst om at politi i samarbeidsland skal kunne sende hverandre informasjon om kjøretøy, fingeravtrykk og DNA-profiler. Palantirs programvare ble kjøpt inn for å håndtere denne utvekslingen.

«Det gjenstår noe arbeid og leveranser, men dette er definert som forbedringer og mindre viktige leveranser», skrev Kristin Kvigne, daværende avdelingsdirektør i Politidirektoratet (POD), i februar i fjor.

I april i år purret så Justis- og beredskapsdepartementet (JD) på POD, etter at det i et brev kom frem at tidsfristen som tidligere var oppgitt til departementet, ville bli brutt. Morgenbladet har fått tilgang til dokumenter fra mai i år, der assisterende politidirektør Håkon Skulstad skriver at «Prüm-funksjonalitet er implementert i fagsystemene», men at Kripos og Politiets IT-tjenester (PIT) har møtt på «uforutsette utfordringer» i arbeidet med å få det til å fungere. «Implementeringsprosessen er forholdsvis omfattende», skrev Skulstad, og meldte at de antageligvis vil avslutte prosjektet tidlig i 2022.

I dag er det Ingrid Dagestad, seksjonssjef for Internasjonal seksjon i Politidirektoratet, som har ansvar for prosjektet. Og nå er tidsplanen ennå litt forskjøvet.

– Den gjenstående utviklingen i henhold til revidert plan går som planlagt. Vi er operative første halvår 2022, senest sommeren 2022, skriver Dagestad i en e-post til Morgenbladet.

Dagestad opplyser at «det meste» av utviklingsarbeidet er ferdigstilt, og at Omnia i dag brukes som saksbehandlingsløsning for internasjonalt politisamarbeid ved Kripos.

– Men det gjenstår testing, og etter hvert testing i produksjon. Dette gjelder både for DNA, fingeravtrykk og kjøretøy, skriver Dagestad.

– Brukes Omnia i dag for å utveksle fingeravtrykk med andre land?

– Utveksling av fingeravtrykk oversendes i dag på e-post på den tradisjonelle måten, men når Prüm er fullt ut operativ, vil en større del av biometrien bli søkt ut automatisk, sier Dagestad.

hj@morgenbladet.no

«Etter denne høsten er håpet om flertallsregjering svakere enn noen gang.»

ASLAK BONDE → 4

«Det er på tide å slå hull på myten om lett påvirkelige borgere.»

TORE WIG → 20

MORGENBLADET

KR 69,–
3.–9. DESEMBER 2021
ÅRGANG 202
NR. 47

EN UAVHENGIG UKEAVIS OM POLITIKK, KULTUR OG FORSKNING

MORGENDAGENS TANKER I DAG

SAPFO GJENDIKTET

Hvem har definisjonsmakten når antikkens store kvinnelige poet skal utgis på norsk, svensk og dansk?

INTERVJUER → 42

KRITISERER NOBELPRISEN

Er årets fredspris et tegn på Vestens tonedøvhet og intellektuelle latskap, spør journalisten Leonid Ragozin.

ESSAY → 16-17

REYER JACOBSZ VAN BLOMMENDAEL, DETALJ FRA *SOCRATE, SES DELVIS PRØVES ET ALCIBIADE* (1675)

GRETNE, GAMLE GRUBLERE

Nesten alle de store europeiske filosofene var ugifte, påpekte Mary Midgley.

ESSAY → 22–24

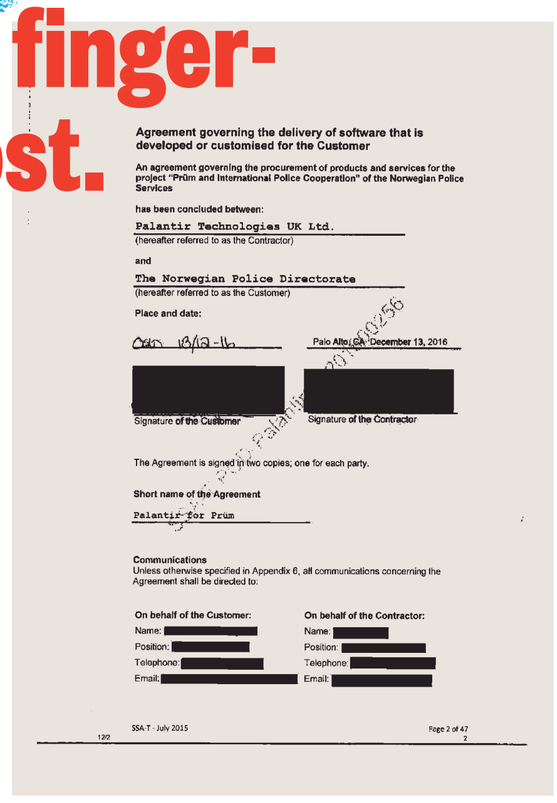
SLIK BLE POLITIETS DIGITALE «SUPERVÅPEN» EN 100-MILLIONERS FIASKO

Hva gikk galt da Silicon Valley møtte norsk politihverdag?

DOKUMENTAR SIDE 6-13

7070717000016

Dataverktøyet fra Silicon Valley skulle koble registre og gjøre det mulig å se «alt». Fem år senere sender politiet fortsatt fingeravtrykk på e-post.



Agreement governing the delivery of software that is developed or customised for the Customer

An agreement governing the procurement of products and services for the project "Prüm and International Police Cooperation" of the Norwegian Police Services

has been concluded between:

Palantir Technologies UK Ltd.
(hereafter referred to as the Contractor)

and

The Norwegian Police Directorate
(hereafter referred to as the Customer)

Place and date:

Oslo 13/12-16 Palo Alto, CA December 13, 2016

[redacted] [redacted]

Signature of the Customer Signature of the Contractor

The Agreement is signed in two copies, one for each party.

Short name of the Agreement

Palantir for Prüm

Communications
Unless otherwise specified in Appendix 6, all communications concerning the Agreement shall be directed to:

On behalf of the Customer:	On behalf of the Contractor:
Name: [redacted]	Name: [redacted]
Position: [redacted]	Position: [redacted]
Telephone: [redacted]	Telephone: [redacted]
Email: [redacted]	Email: [redacted]

SSA-T - July 2015 Page 2 of 47

Kjøp: Kontrakten mellom Politidirektoratet og Palantir Technologies, signert 13. desember 2016.

Palantirs overvåkningsteknologi er banebrytende og potent for den som tar den i bruk. I fem år har politiet i Norge mislyktes med akkurat det.

HANNE ØSTLI JAKOBSEN OG
CHRISTIAN BELGAUX (FOTO)

I april 2020, mens pandemiens første bølge herjet landet, sprakk nyheten i fagbladet Politiforum: IT-prosjektet Omnia – politiets storinnkjøp av programvare fra overvåkningsselskapet Palantir – var bråstanset. Dataprogrammet fungerte ikke, tre og et halvt år etter at det var kjøpt inn, og etter 100 millioner investerte kroner. Likevel hadde Politidirektoratet bestemt seg:

Selv om «ikke alle kriteriene for prosjektavslutning er tilfredsstilt», erklærte de Omnia-prosjektet for avsluttet.

Da Palantir kom til Norge, ble teknologien deres omtalt som et «supervåpen». Med programmet Gotham, det som i Norge ble hetende Omnia, skulle norsk politi se nye koblinger mellom gamle spor, finne skjulte sammenhenger mellom kriminalsaker og løse dem raskere. Palantir er for politiet det Google er for oss, ble det sagt. Men i fjor ble prosjektet altså avsluttet, samtidig som Politiforum meldte om bitre samarbeidsproblemer i prosjektet, et system som ikke fungerte og store spørsmål om hva som egentlig var levert.

De siste månedene har Morgenbladet undersøkt hva som faktisk skjedde da Silicon Valley møtte Norges politi. Gjennom mer enn femti innsynsbegjæringer, et titalls samtaler med kilder i og utenfor politiet, og over hundrevis av sider med kontrakter, e-poster, notater, rapporter og presentasjoner har det tegnet seg et bilde av et prestisjeprosjekt som gikk på tverke fra starten.

- Kravene fra politiet til programmet de skulle kjøpe, var som skreddersydd for Palantir – og Palantir vant anbudet.
- Politiet hadde selv «ingen erfaring» med slike systemer, skrev de, og ba teknologikjempen finne svarene.
- Prosjektet este gjennom hele 2017: Politiregistre ble koblet inn og ut av Palantirs program, uten at noen dokumenterer hvorfor.
- Gjennom dette året fantes det få dokumenter i de offentlige postlistene som kunne fortelle hva som foregikk. En rekke av dem ble journalført først et år senere, da politiets internrevisjon gransket prosjektet.
- Gjentatte ganger er det blitt stilt spørsmål ved om Palantirs programvare i det hele tatt var lovlig å bruke slik politiet ønsket.

Kilder Morgenbladet har snakket med, beskriver prosjektet som «galimatias» og «altfor ambisiøst».

– Omnia ble altfor stort, altfor fort, sier én.

Da Omnia-prosjektet ble avsluttet, kunne dataprogrammet fortsatt ikke håndtere utveksling av fingeravtrykk med andre land, slik det var ment. I dag sendes de ennå på e-post.

KAPITTEL 1
EN SYNESTEIN I NØDEN

Morgendagens software i dag

Et jetfly farer over himmelen. Et ristende hjelmkamera viser en soldat i en ørkenaktig krigssone, løpende sammenkrøpet mot et helikopter. Røyk siver over piggtrådhindre mens eksplosjoner går av langs bakken. Over tikker reklameteksten frem: «Morgendagens grunnleggende software. Levert i dag».

Overvåknings- og analyselskapet Palantir Technologies ble grunnlagt i 2003 av blant andre forretningsmannen Alex Karp og den etter hvert legendariske investoren Peter Thiel: kontrær libertarianer, Silicon Valleys første og tydeligste tilhenger av Donald Trump og en tidlig investor i Facebook. Selskapets navn hentet Thiel og Karp fra fantasyserien *Ringenes Herre* av J.R.R. Tolkien: Palantírene er synesteiner, som lar eieren se hva som skjer hvor som helst i verden. Slik er også ambisjonen for Palantir: Selskapet vil finne alle data for kundene, samle alt og koble alt.

Gotham, kalt opp etter Batmans hjemby, er programvaren som Palantir tilbyr til forsvars-, politi- og etterretningsorganisasjoner: «Gotham kobler og beriker massive mengder data i nærsanntid, og presenterer dem i ett enkelt bilde som lar brukeren ta raskere og mer selvsikre beslutninger», skriver Palantir på sine egne hjemmesider.

In-Q-Tel, CIAs investeringsfirma, var blant de første som spyttet penger inn i Palantir. Politiet i Los Angeles bruker programvaren deres, det gjør også FBI og det amerikanske forsvaret, og selskapet har etablert seg i stadig flere land i Europa. De har hintet om at de var involvert da amerikanerne fant og drepte Osama bin Laden i Pakistan i 2011, uten at dét er bekreftet.

Men Palantir er omstridt: Det er vanskelig å vite hvor mye selskapet vet, eller hvordan det opererer. Det inngår store kontrakter med offentlige etater uten at offentligheten vet om det, og aktivister og eksperter i USA har advart mot at Palantirs overvåkning kan gå på borgerrettighetene løs.

«Nye og bedre verktøy»

Den andre P-en i denne sagaen er Prüm, er en liten by vest i Tyskland. Den er som Schengen: Ikke kjent for stort annet enn avtalen den har lånt navnet sitt til.

Prüm-samarbeidet startet i 2005, og skal hjelpe Europas politifolk med å løse kriminalsaker som beveger seg over grensene. Et DNA-spor funnet i Norge kan være registrert i en litauisk eller fransk database: Prüm er avtaleverket som lar landenes politi fortelle hverandre om det. (En tilsvarende avtale med USA heter PCSC.) Norge signerte Prüm-avtalen i 2009, da Knut Storberget var justisminister. Svenskenes system for å koble seg på avtalen var klart to år senere. Norge er ennå ikke oppkoblet, tolv år etterpå.

For å oppfylle Prüm-avtalen trengte politiet, blant annet, et nytt dataprogram. Det gamle saksbehandlingssystemet for internasjonalt politiarbeid skulle fases ut, og når de koblet seg opp til andre land via Prüm, ville det bli mange flere henvendelser å håndtere. Hele etaten trengte å bli mer fremoverlent – dette var oppgaven Palantir skulle løse. Øverste IKT-sjef i politiet på den tiden var Cato Rindal, en sivilingeniør fra Bærum som tidligere hadde jobbet i både Accenture og som IKT-direktør i Sykehuspartner. Han ble ansatt i 2014, da meldte Teknisk Ukeblad at Rindal «hadde oppskriften på et mer moderne politi»:

«Etaten skal få nye og bedre verktøy for å jobbe smartere og dele kunnskap enklere», sa Rindal. «Vi skal velge færre og felles standardiserte løsninger.» Målet var sentral styring: Politidirektoratet (POD) og hans IKT-avdeling skulle ha kontroll. Rindal har ikke villet la seg intervjue til denne saken.

Anbudsprosessen startet sommeren 2016. Politiet trengte et program for å løse Prüm, og det skulle være velprøvd, så «hyllevare» som mulig. Om leverandøren måtte endre systemene sine, lage teknologisk skreddersøm, kunne det hele fort bli ustyrlig og dyrt.

KAPITTEL 2
SOM DU SPØR, FÅR DU SVAR

Hånd, møt hanske

I 2016 hadde Palantir ingen offisiell tilstedeværelse i Norge. Datterselskapet Palantir Technologies Norway AS ble stiftet først i januar 2017. Men Palantir var her allerede, ifølge flere kilder Morgenbladet har snakket med. De sier selskapet har jobbet opp mot flere norske kunder i lengre tid. De hemmelige tjenestene, som Politiets sikkerhetstjeneste (PST), må ikke ut med offentlige anbud for mange av sine anskaffelser.

Morgenbladet har spurt både PST og Forsvarets E-tjeneste om de har eller har hatt et kundeforhold med Palantir, men dette er gradert informasjon: De kan hverken bekrefte eller avkrefte.

Prüm-anbudet ble lyst ut 14. juni 2016, og i løpet av sommeren ble Palantir med i kampen om kontrakten. I kravspesifikasjonen fra politiet som Morgenbladet har fått innsyn i, finner man en etterlysning som viste seg å stå godt til det Palantir kunne tilby: →

Det norske politiet ville ha et system for «støtte til internasjonalt politisamarbeid» som kunne tilbys både i en fullversjon og i en «lettvektsvariant». Akkurat slik er Gotham organisert: Gotham finnes både som en «full klient» og i enklere varianter som for eksempel politifolk i LA har med seg på laptop i patruljebilen. Det var dessuten viktig for norsk politi at systemet kunne demonstreres ved hjelp av *video* – dette kravet fikk et eget avsnitt. Palantirs egne hjemmesider, og Youtube, viser en rekke videoer som presist kan beskrives slik politiet gjør det: «videoer som demonstrerer hvordan brukeroppgaver utføres via produktene, plattformene og komponentene som utgjør Løsningen».

Og politiet etterlyste et system som gjorde akkurat det Palantirs systemer gjør. Her kan vi sneie innom hva det faktisk er:

Palantir lager *semantiske nettverk* – en teknologi som organiserer verden. I et semantisk nettverk tar du en rotete virkelighet og tagger den: Dette er en person, dette er en hendelse, her er en annen person som er knyttet til hendelsen via en telefonsamtale. Når slikt rot – ustrukturert informasjon – blir organisert med et felles språk, blir det mulig å tegne koblingskart og se sammenhenger mellom tilsynelatende vidt forskjellige deler av virkeligheten.

Et bankkontonummer, notert av en politimann under en etterforskning for fem år siden, blir senere beslaglagt i opprullingen av et hvitvaskingsnettverk. I et godt semantisk nettverk kan du med et øyekast se hvem som eide kontoen den gangen, navnet på betjenten, om han merket seg flere opplysninger.

Norsk politi rokter 19 ulike registre, med opplysninger om DNA, kjøretøy, fingeravtrykk, tidligere dommer, etterforskningsopplysninger og en rekke annet. Noen kan søkes i på tvers, andre ikke, og systemene ble ikke laget for å samhandle. Dermed kan man legge Palantir *på toppen*: Føre opplysningene fra hvert register inn i Palantir, tagge alt i ett, felles språk og se sammenhenger. Ofte kalles det å la en organisasjon som politiet «vite hva den allerede vet».

I kravspesifikasjonen beskriver politiet hvordan systemet de søker, må kunne ta imot en melding, og så gå gjennom den «for å oppdage entiteter i den strukturerte og ustrukturerte delen av meldingen. […] For hver entitet er så dens tilstedeværelse i meldingen merket på en slik måte at når en bruker senere ser på entiteten i løsningen, blir både meldingen og andre entiteter koblet til den, vist.»

«Som et Silicon Valley-teknologiselskap …»

«Norsk politi har i dag ingen erfaring med den typen system som søkes i denne anskaffelsen». Det kan vi lese allerede på side 8 i den mer enn hundre sider lange kravspesifikasjonen.

Hvordan skal en norsk etat møte et amerikansk teknologiselskap? I årene siden Palantir og norsk politi fant sammen, har bevisstheten vokst om at Silicon Valleys giganter ikke bare vil «koble folk sammen», men også bruker store ressurser på å forsøke å vite mest mulig om oss. Palantir har aldri vært blant de største i dalen, men de er store innen etterretning, med politiske og profesjonelle koblinger til myndigheter og bedrifter i en rekke land. Ingeniørene omfavner Ringenes herre-mytologien – et av Palantirs motto er *Save the Shire*, «Redd Hobbsyssel», med henvisning til hobbitlandsbyen der Tolkiens historie starter – men selskapet tjener penger på å selge produktene sine, som alle andre.

Den 13. desember 2016 skrev Palantirs sjefsadvokat Matt Long og Kristin Kvigne, daværende assisterende politidirektør, under på kontrakten Palantir hadde vunnet. Den lød på 81 millioner kroner – mer enn dobbelt så mye som de drøyt 33 millionene prosjektgruppen (nølende) hadde anslått at anskaffelsen ville koste året før. Og i de mange hundre sidene med tekniske spesifikasjoner som Morgenbladet har fått innsyn i, ser man da også et søkende politi: Dette har vi aldri gjort før, kan dere hjelpe oss? «Politiet foretrekker å forandre sine arbeidsmetoder til å passe løsningen, heller enn å tilpasse løsningen til eksisterende arbeidsmetoder», skriver politiet. De hadde gjort undersøkelser for å se hva som var tilgjengelig i markedet, men likevel:

«Kunden vil (…) understreke at kontraktøren burde ta med sin fulle erfaring fra lignende etater og andre utrullinger, og ikke nøle med å foreslå bedre måter å løse behovene».

Og Palantir svarer:

«Som et Silicon Valley-teknologiselskap, har Palantir en agil kultur for softwareutvikling, definert av overlegen innovasjon og design – og komplett dedikasjon til vårt mål om å bemektige kundene til å bruke data for å oppnå transformative resultater.»

En skikkelig god deal

– En av grunnene til at Palantir vant, var at de prissatte alle integrasjonene til kroner 0. De sa «ja, vi integrerer *alle* registrene, til ingen penger, til en pakkepris».

Slik beskriver en som deltok i prosjektet hvordan Palantir gikk seirende ut av konkurransen – på tross av den høye prisen. Palantirs kongstanke er velkjent for selgere: Det viktigste er å få en fot innenfor døren. Så Palantir lot norsk politi kjøpe Gotham til prisen av lisensen. Hovedjobben, å lage integrasjonen mellom Gotham – Omnia – og politiets egne registre, sørge for at

– Jeg tror Palantir ble lurt inn i en bløff.
ANONYM DELTAGER I OMNIA-PROSJEKTET

PALANTIR TECHNOLOGIES

Amerikansk selskap for dataanalyse og etterretning, grunnlagt i 2003, med drøyt 2700 ansatte i en rekke land i Nord-Amerika og Europa.

Lager i hovedsak tre programmer: Gotham, til forsvar og etterretning, Foundry, til private bedrifter, og Apollo, som kan forenkle og automatisere utrulling og oppdatering av de to andre.

Ble børsnotert i september 2020.

Da hadde selskapet en beregnet verdi på rundt 20 milliarder dollar, eller ca. 180 milliarder kroner.

Arnestedet: Palantir kaller seg et Silicon Valley-selskap, selv om forretningsmodellen er mer «IT-konsulent» enn «apper og sosiale medier». Hovedkontoret deres lå inntil nylig i Palo Alto. FOTO: JIM WILSON / THE NEW YORK TIMES / NTB

opplysninger ble inkludert og oppdatert på riktig måte, var gratis.

En e-post fra Politidirektoratet i fjor bekrefter at «opsjonen» var kostnadsfri. En rekke kilder Morgenbladet har snakket med, både kritikere av Omnia og folk som mener det kunne blitt bra, sier valget om å godta den var skjebnesvangert: Palantir skulle ikke ha betalt, men tilbudet kostet: Å integrere 10 eller 15 eller 19 registre ville kreve mye ressurser – tid, planlegging, testing – fra *politiets* side.

– De sa: Ja – dere har kjøpt nytt saksbehandlingsverktøy, men nå skal dere se: Dere kan få integrert *alle* deres sentrale registre gratis, vi laster dem ned i Gotham, så kan dere søke og se på analyser på tvers. Bare gi oss mastertilgang til alle dataene, så fikser vi det, forteller en ansatt i Kripos som etter hvert skulle bli en skarp kritiker av prosjektet.

Taktikken er kjent fra Palantirs satsing i Europa. Avisene The Guardian, Der Spiegel og gravegruppen Lighthouse Reporting har dokumentert at Hellas fikk et lignende tilbud sommeren 2020: Palantir skulle lage et dashbord for pandemiovervåkning, gratis. Avtalen ble først offentlig kjent ni måneder etter at den ble inngått. Britiske myndigheter har på sin side latt Palantir bli samarbeidspartner med National Health Services for ett pund – også den avtalen ble inngått uten normale kontrollprosesser. Da prøveperioden var over, kostet det 24 millioner pund å fortsette lisensavtalen.

– Man velger leverandør i henhold til de administrative bestemmelsene, en evaluering av tid, kvalitet og pris. Opsjonene var en bonus, altså ikke et utvalgskriterium, sier Ingrid Dagestad, nåværende prosesseier for Omnia i POD, i dag. (Se intervju med Dagestad i egen undersak).

KAPITTEL 3
ETT PROGRAM SKAL SAMLE DEM, ETT SKAL FINNE DEM

Den store datadumpen

Det er ikke mange som vil snakke om hva som skjedde i månedene og årene etter at kontrakten ble inngått, mens Omnia kjørte seg fast og ble trøblete. IKT-direktør Rindal jobber i dag i Statens vegvesen, og har ikke ønsket å la seg intervjue. Eier av prosjektet var daværende seksjonssjef John Ståle Stamnes, i dag er han på Politihøgskolen. I det daglige ble prosjektet ledet av Jan Helge Ekeren, innleid fra Sopra Steria – men også han er ute av politiet. I en SMS til Morgenbladet skriver han at han som konsulent er bundet av taushetsplikt.

Men én fra politiet vil fortelle, om enn ikke under fullt navn. Det har vært mye ondt blod de siste årene, med press mot folk som har hatt innvendinger eller ønsket strengere kvalitetskrav, sier han. Så vi kaller ham Johansen. Johansen har vært i Kripos i årevis, tett på politiets registre. Slik han ser det, ble deltagerne i Omnia-prosjektet sveiseblinde av de teknologiske mulighetene – og glemte personvernet:

– De var ikke tro mot kravet om at formålet med innhenting av informasjon må gjenspeiles i hvordan den informasjonen brukes. Det var et av kjernepunktene som sviktet, sier han.

Om du pågripes i Norge, har politiet lov til å ta bilde og fingeravtrykk av deg, og lagre det i registeret ABIS. Men skulle du etter hvert *frikjennes*, skal bildet og fingeravtrykket slettes. Varianter av slike regler finnes for alle politiets registre. Men her kommer noe datateknisk litt finurlig – og viktig for en etat som har monopol på å utøve vold mot norske borgere:

Når en opplysning slettes fra politiets registre, blir den sjelden slettet *helt*. Opplysningen fjernes fra det brukerne ser, men den ligger fortsatt nede i buken et sted. Slik kan man føre tilsyn med det politiet gjør. Datatilsynet skal for eksempel sjekke at Kripos røkter sine registre riktig, og da skal de ikke bare sjekke hva som finnes i systemene *nå*, men også hva som er blitt slettet, når og hvorfor.

Kripos-ansatte advarte de som skulle lage Omnia om slike finurligheter da kontrakten med Palantir ble inngått. Disse registrene er kompliserte saker, teknisk og juridisk. Politiets interne gransknings-rapport om prosjektet, som ble laget etter at prosjektet hadde kjørt seg fast i 2018, slår fast at prosjektet og Kripos har hatt «svært ulik oppfatning av hva som er tilstrekkelig datakvalitet».

Da kan slikt som dette skje: Palantirs ingeniører tok alle opplysninger fra noen registre, slettede som gyldige, og dumpet dem inn i Omnia. Dette beskrives både i kildesamtaler og i dokumenter Morgenbladet har fått tilgang til.

– Alt gikk inn, søkke og snøre. Det var fascinerende å se, det var så mye informasjon. Men så ser du at dette har vi ikke lov til, forteller Johansen i dag.

Den første pilotvarianten av Omnia ble tatt i bruk i juli 2017. Det tok ikke lang tid før saksbehandlere i Kripos kom til Johansen, forteller han, og lurte på hva som foregikk: Når de sjekket opplysninger i Omnia opp mot de originale registrene, fant de feil og opplysninger som ikke skulle vært der. Domfelte hadde fått dobbelt så lange fengselsstraffer som det straffesaksregisteret oppga.

– Folk kom til meg og sa: «Dette er galimatias». Når alt er på én arbeidsflate, må du kunne stole på dataene. Om ikke – om vi leverer feil data eller informasjon som ikke holder vann til samarbeidspartnere i utlandet – taper vi jo i rykte og renommé, sier Johansen.

– *Hva svarte prosjektet da dere meldte fra om feil?* ⟶

– «Ja, da skal vi rette opp det». Men jeg husker en periode, vi hadde fått beskjed om at en feil var rettet. Det tok meg tre minutter å dokumentere at det ikke var tilfelle, å finne nye feil av samme type. Egentlig må du backe helt tilbake og teste *alt*. Men Palantir mente at det var i orden.

Se for deg at politiets registre inneholder firefem «entiteter», personer, som heter sånn cirka Hanne Østli Jakobsen. Noen skriver Østlie, andre Jacobsen, andre har droppet Østli, eller Jakobsen.

– En av de tingene vi har mast om i politiet, er at om vi skal identifisere en person sikkert, må det basere seg på biometri, sier Johansen.

– Helst DNA, men i hvert fall bilde og fingeravtrykk. Identifisering basert på bare navn og fødselsdato, kanskje etnisitet? Nei. Men i Gotham var det bare å velge alle varianter av en person og trykke «*merge*».

Stor, større ...

Hva var det politiet trengte da de kjøpte Omnia? Selv det klarer ikke de involverte i prosjektet bli enige om.

Én variant er rimelig enkel: Omnia kan brukes for å samkjøre informasjonsflyten når biometriregistrene automatisk sender ut forespørsler til politi i andre land: Har dere dette fingeravtrykket registrert? *Hit / no hit*. Svaret spretter opp i Omnia når du slår på maskinen. Slik forsto Johansen prosjektet da han begynte å se nærmere på det sommeren 2017.

Litt mer avansert blir det om du også skal *håndtere* informasjonen som kommer fra de internasjonale forespørslene. En politietat i et annet land trenger for eksempel å vite hvilken informasjon norsk politi har om en DNA-profil. Da kan du gå inn i de ulike registrene der relevant informasjon kan tenkes å være, sjekke DNA, se hva vedkommende er domfelt for i et annet register, hvilken bil de kjører i et tredje.

Eller alt dette kan sjekkes på én gang, i ett program. I så fall trenger du (noe som) Palantir. *Det* var visjonen og planen for Omnia, sier folk som deltok i prosjektet.

Enda litt mer avansert blir det om informasjonen i Omnia skal brukes til å utarbeide hypoteser og drive etterforskning også i helnorske saker. Hvem var på et gitt sted når, og finnes det andre spor som kan koble dem til innbruddet? Jo mer informasjon du mater inn, desto bedre blir analysen. Hva med å ta med telefondata? Folkeregisteret? Oversikter over flyreiser?

I anbudskonkurransen anerkjente POD den muligheten – programmet de søkte, kunne tenkes å være nyttig også til innenriks politiarbeid. «Den typen bruk er likevel utenfor rammen til denne anskaffelsen», skriver de.

Slik ble det ikke.

... størst

– Omnia ble altfor stort, altfor fort. Man forsøkte å selge bjørnen før den var skutt.

Den beskrivelsen går igjen – fra kildene Morgenbladet har snakket med, i dokumentene som er journalført i prosjektet, i politiets interne granskningsrapport. Mye er imidlertid *ikke* journalført: Dokumentasjonen i de offentlige postlistene var sporadisk i 2017, prosjektets første år, viser Morgenbladets undersøkelser. I mars året etter, mens internrevisjonen gransker prosjektet, journalføres så sentrale og ofte mange måneder gamle dokumenter – en kvalitetssikringsrapport, e-poster om forsinkelser, et notat om informasjonssikkerhet.

– Alt gikk inn, søkke og snøre. Det var fascinerende å se, det var så mye informasjon. Men så ser du at dette har vi ikke lov til.
ANONYM MANGEÅRIG KRIPOS-ANSATT

Deltagerne som var med i prosjektet i 2017, og granskningsrapporten, oppsummerer året slik:

Omnia vokste. Registre ble tatt inn, og andre tatt ut, men antallet økte. Fra fem, til ni, til fjorten – uten at politiets internrevisjon har funnet dokumentasjon på hvilke opplysninger som skulle lastes inn i Omnia og hvorfor. En slik tilnærming er på kant med norsk lov: Både personvernlovgivningen og politiregisterloven slår fast at politiet bare skal behandle opplysninger når det har et klart formål, og da skal de behandle *så få opplysninger som mulig* for å løse oppgaven. Det er fjernt fra kongstanken til Palantir – samle alt, koble alt, og se hva du finner. I internrevisjonens rapport sier representanter for prosjektet at det har vært «et premiss at alle lov- og forskriftskrav skal ivaretas», men revisjonen konkluderer at det «i liten grad har vært tema» i dokumentene.

På spørsmål om hvorvidt disse integrasjonene var i tråd med norsk lov, svarer Ingrid Dagestad, nåværende ansvarlig for Omnia i POD, at det «hele tiden har vært gjort vurderinger opp mot legaliteten».

Blant IT-folk kalles det «function creep»: Noen kjøper seg en hammer, og plutselig ser de spikre overalt. Og Palantir skulle få samme betaling, uansett hvor mange registre som ble koblet til Omnia, så hvorfor ikke? «Prosjektet har hatt for stor tro på leverandørens [Palantirs] evne til å levere integrasjonene», skriver internrevisjonen.

– Du hadde masse nyansatte IT-folk i politiet på den tiden – de fleste av dem har jo gått videre til andre jobber nå. Men min forståelse var at de ville vise at de fikk til noe på IT-siden, sier en deltager i Omnia-prosjektet.

– Så da kom dette prosjektet, som selvsagt var altfor ambisiøst og skulle løse altfor mye med de ressursene som var satt av.

Fra åsted til maskin: I laboratoriet til Kripos på Brynseng i Oslo digitaliseres fingeravtrykk som politiet finner. Derfra blir de lagret – dersom det er lovlig – i registeret ABIS.

POLITIETS 19 SENTRALE REGISTRE

1 ABIS – foto
2 ABIS – fingeravtrykk
3 Arrestjournal
4 Arrest – lyd og bilde
5 Bekymringssamtale
6 DNA-registeret
7 ELYS II - etterlysningsregisteret
8 GTK – grense- og territorialkontroll
9 Informantregisteret
10 Indicia - kriminaletterretningsregisteret
11 Lydlogg
12 PO – politiets operasjonslogg
13 Saknetregisteret
14 SSP – reaksjonsregisteret
15 SSP – personidentitetsregisteret
16 SSP – politiopplysningsregisteret
17 Strasak - straffesaksregisteret
18 ASK – hvitvaskingsregisteret
19 UTSYS – utlendingsregisteret

Gotham: I 2017 skrev nettavisen Digi.no om politiets nye våpen, som kunne søke «lynrask» i 300 millioner fingeravtrykk. Det er fortsatt ikke tilfelle. På bildet er prosjektleder Jan Helge Ekeren (nr. 2 fra venstre) og prosjekteier John Ståle Stamnes (ytterst til høyre), og to andre daværende involverte i prosjektet, foran startskjermen til Palantirs program.

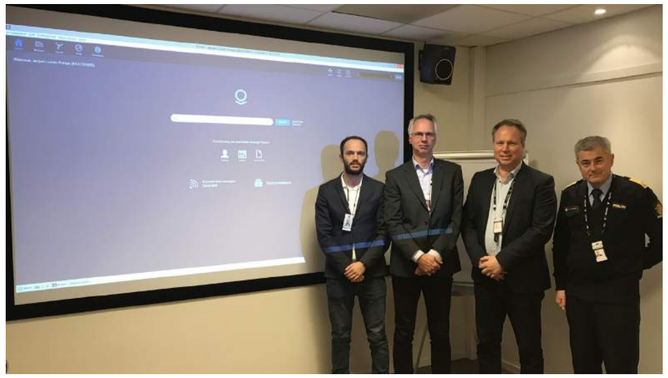
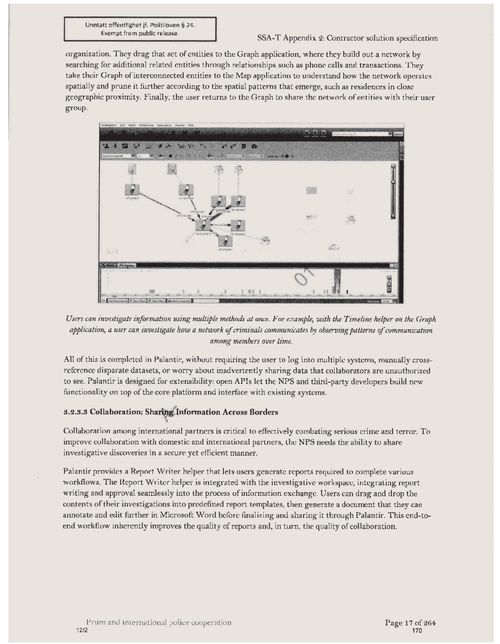


FOTO: MARIUS B. JØRGENRUD



Unrestrt offentlighet jf. Politiloven § 24.
Exempt from public release.

SSA-T Appendix 2: Contractor solution specification

organization. They drag that set of entities to the Graph application, where they build out a network by searching for additional related entities through relationships such as phone calls and transactions. They take their Graph of interconnected entities to the Map application to understand how the network operates spatially and prune it further according to the spatial patterns that emerge, such as residences in close geographic proximity. Finally, the user returns to the Graph to share the network of entities with their user group.

Users can investigate information using multiple methods at once. For example, with the Timeline helper on the Graph application, a user can investigate how a network of criminals communicates by observing patterns of communication among members over time.

All of this is completed in Palantir, without requiring the user to log into multiple systems, manually cross-reference disparate datasets, or worry about inadvertently sharing data that collaborators are unauthorized to see. Palantir is designed for extensibility: open APIs let the NPS and third-party developers build new functionality on top of the core platform and interface with existing systems.

3.2.3.3 Collaboration: Sharing Information Across Borders

Collaboration among international partners is critical to effectively combating serious crime and terror. To improve collaboration with domestic and international partners, the NPS needs the ability to share investigative discoveries in a secure yet efficient manner.

Palantir provides a Report Writer helper that lets users generate reports required to complete various workflows. The Report Writer helper is integrated with the investigative workspace, integrating report writing and approval seamlessly into the process of information exchange. Users can drag and drop the contents of their investigations into predefined report templates, then generate a document that they can annotate and edit further in Microsoft Word before finalizing and sharing it through Palantir. This end-to-end workflow inherently improves the quality of reports and, in turn, the quality of collaboration.

Prüm and international police cooperation 12/2

Page 17 of 264 170

Salg: Fra Palantirs beskrivelse av eget system i kontrakten med politiet.

– Palantir skal brukes til *predictive policing*, for å finne et fenomen eller en trend. Og sånn statistikk tåler at det kommer en og annen slenger, en feilopplysning, sier Johansen.

Systemene for *personrettet* etterretning i Los Angeles leveres imidlertid av et annet firma. Og norsk politi skulle aldri bruke Palantir til å finne statistiske mønstre i hendelser – det skulle brukes til å systematisere arbeidet i konkrete saker, med konkrete ofre og mistenkte. Da må *alle* opplysninger være riktige, sier Johansen, og politiet må ha lov til å bruke dem.

– Når man så demofilmen fra Palantir som ble presentert, var den helt konge fin. Noe skjedde et sted, et bilnummer blir plukket opp, man følger bilen *live* i trafikken via GPS, identifiserer både person og telefoni og alt mulig, og gjør en pågripelse. Det er kjempeflott, det – jeg vil ikke bo i det samfunnet, men det er mulig, forteller han.

Johansen sier at det rent teknisk ikke er noe i veien for å sette opp kameraer som automatisk registrerer bilskilt i norske byer, eller å starte avlytting av en telefon med et tastetrykk.

– Men da har det skjedd noe på forhånd. Da har det vært en rettsprosess, en beslutning om at her er det skjellig grunn til mistanke.

KAPITTEL 4
TO FORTELLINGER OM OMNIA

Feil program til feil oppgave?

Høsten 2017 trakk en leder i Kripos, som har behandlingsansvaret for 17 av politiets registre, i nødbremsen for første gang. Pilotvarianten av Omnia, den med feilene som Johansen var så frustrert over, ble stanset: Omnia skulle ikke brukes samtidig som programmet ble snekret sammen. Etter dette gikk utviklingen i stampe.

Hverken Palantir eller prosjektet hadde nok folk til at de kunne gjennomteste de ulike delene av systemet før noen tok dem i bruk (det er gjerne når et dataprogram brukes, at feil dukker opp). Forsinkelsene tårnet seg opp, kalenderen viste etter hvert 2018, og prosjektdeltagerne og brukerne av Omnia kranglet videre om integrasjoner, datakvalitet og testing, viser dokumentene Morgenbladet har fått innsyn i.

Johansen mener feilene han fant i Omnia, var fundamentale – signaler om at prosjektet aldri ville kunne fungere.

Morgenbladet har tidligere skrevet om hvordan Palantir brukes i USA. Selskapets programmer er som aldrimette larver: Alle tenkelige opplysninger hentes inn og kobles. Slik kan man få et oppsiktsvekkende detaljert bilde av en by eller et område. Hvor skjer det mange innbrudd, til hvilke tider av døgnet? Gotham svarer på slike spørsmål for Los Angeles-politiet, noe som hjelper politiet å prioritere ressursene sine.

En teknologisk revolusjon, og de som skal bruke den

Andre i og rundt Omnia – som også vil være anonyme, de ser ikke ingen grunn til å starte en ny offentlig krangel – mener prosjektet kunne blitt bra. Noen peker på gjenstridighet hos Kripos, en motstand mot nye arbeidsmetoder, som årsak til at Omnia stagnerte. Andre mener hovedproblemet var at da prosjektet vokste og alt måtte gjennomtestes, var ressursene rett og slett for knappe:

– Prosjektet kom aldri opp i den hastigheten på utvikling, testing og feilretting som de ønsket, sier én med kjennskap til det.

Noen funksjoner i Omnia, som at «samme person» fra ulike registre enkelt kunne slås sammen til én med et tastetrykk, gjorde det heller *lettere* å oppdage feil, mener kilden.

– I et system der alt er samlet, er det enklere å se «er dette riktig?». Sannsynligheten for å dele feil informasjon til utenlandske myndigheter ble mindre, og videre ville man funnet mer relevant informasjon å dele, som kunne ledet til oppklaring av flere straffesaker.

Om det var feil i Omnia, var det fordi Kripos' registre ikke var godt nok vedlikeholdt, hevder en annen med kjennskap til prosjektet. Er det feil i registrene, følger feilene med inn i programmet som ligger på toppen. Og prosjektet *var* bevisst på at Palantir i Norge ikke kunne være som Palantir i USA. Omnia skulle for eksempel aldri inkludere data fra sosiale medier, selv om det teknisk sett var mulig. Andre personvernsproblemer underveis i prosjektet kan kilden ikke huske.

KAPITTEL 5
DET FUNGERENDE SYSTEMET SOM IKKE FUNGERER

Restart, ferdig

Resten av historien om Omnia ligner til forveksling problemene fra prosjektets første år, variasjoner av samme gjentagende melodi.

Gjennom 2018 og 2019 ble det gjort forsøk på å få prosjektet tilbake i gjenge. Palantir laget integrasjoner mellom Omnia og registrene, de ble testet – og feil og mangler dukket opp. Internrevisjonen leverte sin rapport i september 2018. Da anbefalte de en full gjennomgang av *hva* som skulle med i Omnia, *hvorfor* det skulle være der, og hva som var god nok kvalitet etter gjeldende lovverk.

Ifølge den opprinnelige kontrakten skulle Omnia være klart og i bruk i mars 2018. Halvannet år senere, i oktober 2019, begynte Politidirektoratet å utstede dagbøter til Palantir, 37 500 kroner dagen, fordi Omnia ennå ikke var ferdigstilt. Litt tidligere det året dokumenterte Aftenposten at prosjektet til da hadde brukt mer enn 38 000 konsulenttimer. Prosjektleder var byttet ut, og Omnia hadde fått en «restart» og blitt strippet ned til et minimum:

Kun de funksjonene som trengtes for å løse Prüm og PCSC – saksbehandling i forbindelse med biometriforespørsler – var nå med i prosjektet. ⟶

Etter fire uker stanset dagbøtene igjen, og da året var omme, var det slutt. I et brev fra Politidirektoratet til Kripos den 7. februar 2020 skriver POD at de anser Omnia som levert nok, og at prosjektet dermed ble «forsert avsluttet». Ifølge Politiforum mente *ingen*, hverken prosjektet, Kripos eller Palantir, at selv det minimale systemet var i gjenge.

«Det har vært viktig for POD å sette en tydelig sluttdato», sa Arild Hagen, fungerende prosjekteier på det tidspunktet, da Politiforum spurte om hvorfor. I dag, enda to år og mer enn ti millioner kroner etter at Omnia ble erklært klart, er integrasjonene i det minimerte prosjektet fortsatt under uttesting.

Glimt av Palantir

Palantir kan avverge planlagte terrorangrep. De kan finne mistenkte, sende soldater ut i krigssoner, eller være en hjelpende hånd for verdens myndigheter når en pandemi rammer. I hvert fall om du spør dem selv.

I en annen fortelling er Palantir et IT-konsulentselskap: De har laget et produkt, som salgsteamene selger aggressivt. Inntekten kommer ikke fra kunstig intelligens eller voldsomt innovativ programmering, men fra arbeidet til utsendte *forward deployed engineers* som kobler Palantirs programmer til kundens datasystemer. Selskapets folk i Norge er blitt beskrevet som «unge gutter i shorts», uten tyngden som trengtes for å argumentere for Omnia da feilene begynte å melde seg.

Palantir er lite synlig i Omnia-saken, slik den fremstår i de journalførte dokumentene og i kildesamtalene Morgenbladet har hatt. De har vært lite nevnt i kranglene mellom prosjektledelse og brukere. Sjefer i Palantir har kommunisert med PODs prosjektledelse i en egen leverandør-styringsgruppe, men ingen dokumenter fra disse møtene finnes i postlistene. Bare ett spor finnes etter selskapet der: To e-postutvekslinger mellom prosjektleder Ekeren og to daværende Palantir-sjefer fra høsten 2017, om forsinkelsene som da var begynt å bli merkbare.

«Vi sliter med eksterne avhengigheter på vår side av prosjektet», skrev Ekeren en ettermiddag i september det året. Kanskje ville ikke POD få løst det som trengtes for å koble fingeravtrykk- og DNA-databasen til Omnia før sent i november. «Hvilken påvirkning vil dette få for dere (hvilken finansiell påvirkning vil dette ha for politiet, om noen)?», spurte Ekeren.

Palantir var forståelsesfulle, på tilbudssiden: «Vi kan, som et tegn på velvilje, ta på oss den ekstra kostnaden som denne forsinkelsen vil forårsake», svarte Frida Nordström, Palantirs daværende sjef for Norge, Sverige og Finland, dagen etter. Nordström jobber ikke lenger i Palantir, og har takket nei til et intervju til denne saken.

PRÜM-AVTALEN

- En avtale om internasjonalt politisamarbeid i Europa.
- Ble opprinnelig undertegnet av syv EU-land. 27 land deltar nå i samarbeidet i en eller annen form.
- Avtalen tilrettelegger for automatisk utveksling av informasjon om biometri og kjøretøy.
- Den har også bestemmelser som for eksempel lar politi fra et land krysse landegrensene når det er umiddelbar fare, eller sende politi på fly mellom medlemsstatene.

Johansen fra Kripos sier han synes litt synd på Palantir i dag. De skulle lage Gotham for norsk politi, ikke en spesialløsning som håndterer automatiske fingeravtrykk- og DNA-forsendelser.

– Jeg tror Palantir ble lurt inn i en bløff. Jeg tror de ble fortalt at dette skulle ha helt andre bruksområder og annet inntjeningspotensial enn det som var planen. Utviklerne sa det, de også: Det var ikke dette de skulle gjøre – bruke tre år før de klarte å sende en e-post.

Ingrid Dagestad i Politidirektoratet sier i dag at politiet har et godt samarbeid med Palantir. Noam Perski, som har ansvar for Palantirs samarbeid med statlige myndigheter, skriver i en e-post at de ikke kan kommentere kundeprosjekter. «Vi er stolte av det samarbeidet har resultert i, og har en fruktbar, fremoverrettet relasjon med politiet», skriver han.

Drømmen som brast

Allerede før anbudet om et nytt dataprogram til politiet ble lyst ut, og flere måneder før politiet startet forhandlinger med Palantir, flagget prosjektleder Ekeren en sentral utfordring: «Erfaringsmessig er leverandørene ikke beskjedne», skrev han i en e-post tidlig i 2016, om hvordan prosjektet skulle sikre at leverandørene som meldte sin interesse, faktisk kunne gjøre det de sa de kunne.

Var Palantirs fortelling likevel vanskelig å motstå, selv med den erkjennelsen i mente?

Omnia ble til i kjølvannet av Merverdiprogrammet, et annet IT-prosjekt i politiet som kostet 240 millioner kroner over fire år, før det ble skrotet. Og her kom nå et amerikansk tech-selskap og fortalte, selvsikkert og over mer enn 250 sider med beskrivelser og diagrammer, hvordan de kunne ta alle politiets separate registre og koble dem i ett sømløst og intuitivt brukersnitt. Hvis politiet bare ville.

– Dette med informasjonsbehandling, det hadde vi ikke klart å løse selv. Det var kanskje der vi tenkte at dette skulle de, Palantir, klare å løse opp i, sier en av dem som har fulgt prosjektet.

Johansen i Kripos holder på at det var Prüm-avtalen Omnia ble kjøpt for – og det som trengtes da, var noe som kunne håndtere utveksling av fingeravtrykk og DNA, trygt og anonymisert, over landegrenser. Å kjøpe Gotham for noe slikt er som å kjøpe F16 for å sende pakker, mener han.

De involverte i prosjektet som ivret for at Omnia skulle ta politiet inn i fremtiden, synes sluttresultatet er like frustrerende som alle andre:

– Behovet for å finne ut av hva vi vet, det er der fortsatt, sier én.

– Det er fortsatt et problem: Hvordan skal vi kunne vite hva politiet allerede vet, med god nok tilgangsstyring, med god nok kvalitet. Det er fortsatt uløst.

hj@morgenbladet.no

– Hvis de mener de ikke ble hørt, er det en påstand.

Heller ikke Politidirektoratets nåværende prosjektleder kan svare på hvorfor Omnia vokste utover sine rammer. De håper å få programmet opp og i gjenge til neste år.

Ingrid Dagestad, seksjonssjef for Internasjonal seksjon i Politidirektoratet (POD), er i dag prosesseier for utvikling av Omnia hos POD. Det praktiske arbeidet med utvikling av dataprogrammet ligger hos Kripos og hos Politiets IKT-tjenester, kjent som PIT.

Dagestad kom inn i arbeidet med Prüm og Omnia etter at prosjektet var avsluttet. Hun kan derfor ikke svare for vurderingene som ble gjort de første årene etter at Palantir ble valgt, hverken om den kostnadsfrie opsjonen, eller om hvorfor prosjektet vokste seg større enn planlagt. Hun beskriver det opprinnelige Omnia som bestående av tre «moduler»: Den tekniske oppkoblingen av biometriregistrene, det internasjonale saksbehandlingsverktøyet som nå er godtatt og i bruk, og så den større «analysedelen» – det vi andre kjenner som Gotham.

– Det er søkefunksjonen og integrasjonen med alle registre. Jeg er ikke kjent med detaljene i analysedelen selv. Det sies å være et godt verktøy, men det er krevende med tanke på personvern og opp mot de nasjonale registrene, sier hun.

– Analysedelen er ikke i bruk i dag, den ble ikke gitt prioritet da prosjektet ble «restartet» i 2019. Ut fra mitt ståsted i dag tenker jeg at prioriteringen var fornuftig.

«Man må gjøre noen valg»

Saksbehandlingsverktøyet Palantir har levert, dagens Omnia, er skreddersøm, et system de har utviklet kun for det norske politiet – selv om politiet i 2016 understreket at de ønsket et system som «forble så standardisert som mulig».

– I store prosjekter må man gjøre noen valg. Det handler primært om kostnad, og om kapasitet – hva politiet totalt har mulighet til å gjennomføre av utviklingsløp. Når *scopet* til et prosjekt utvides og vokser ut av rammen som ligger til grunn, må noen gå inn og sette begrensninger, sier Dagestad.

– Et saksbehandlingsverktøy var det politiet søkte i 2016. Hvorfor da velge Palantir, et selskap som ikke *lager saksbehandlingsverktøy, men analyseprogrammet Gotham?*

– Hvordan de vurderte dette i kontrakten, kan jeg ikke mene noe om. Slik jeg ser det, er teknologene i Palantir, de som jobber sammen med PIT, også utviklere. Enhver stor teknologisk organisasjon kan levere hyllevare, og de kan også være med på et videre utviklingsløp.

– Ansatte i Kripos sier de meldte fra om at integreringen av registrene var komplisert, blant annet med tanke på personvern, og at Palantirs folk ville trenge hjelp, men at de ikke ble hørt?

– Det kan jeg ikke svare på. Hvis de mener de ikke ble hørt, er det en påstand. Jeg satt i Kripos den gangen og var leder for internasjonalt politisamarbeid, og jeg opplevde at jeg ble hørt.

– Er dere enig i at det strider med loven om man inkluderer registre uten klart formål, og uten å vite at det er den mest minimale behandlingen av personopplysninger som kan oppfylle formålet?

– Det har hele tiden vært gjort en vurdering opp mot legaliteten, svarer Dagestad.

13 millioner

Nå er det tre registre, de som kreves for å svare på Prüm-oppdraget om utveksling over landegrensene, som skal kobles til Omnia: fingeravtrykk, DNA og førerkort. Det foregår fortsatt testing av alle integrasjonene.

– Prosjektet ble forsert avsluttet på et tidspunkt da hverken Palantir eller deltagerne i prosjektet mente det var klart. Var det feil å sette godkjentstempel på det tidspunktet?

– Det var en ambisjon at systemet skulle fungere teknisk tidligere. Men av mange forskjellige årsaker er det blitt forsinkelser, sier Dagestad. Hun nevner blant annet at mange systemer under utvikling hos politiet er avhengig av tilkobling til for eksempel fingeravtrykkregisteret ABIS. Da må man prioritere tilgangen, og det kan bli kø for utviklerne.

Siden prosjektet ble avsluttet tidlig i 2020, har etterarbeid, lisenskostnader og annet arbeid forbundet med Omnia så langt beløpt seg til 13,7 millioner kroner, anslår POD.

– Det er nå brukt over 100 millioner kroner på et system for grunnleggende saksbehandling. Hva tenker dere om det?

– Det er jo ikke bare et saksbehandlingsverktøy. Vi har integrasjonene for Prüm, det vil si integrasjon mot de tre registrene, søkemuligheter til andre land. Du må se totalpakken, sier Dagestad.

– Vi oppfatter Omnia som et funksjonelt system som tilfredsstiller dagens behov. Det jobbes godt hos Kripos og PIT, i godt samarbeid med Palantir, for å få operasjonalisert Prüm-avtalen og for utvikling av systemene. Så får historie være historie, men vi skal få det på plass, vi skal ta det i bruk. Ting tar tid, men jeg velger å være positiv med tanke på fremdriften.

hj@morgenbladet.no

Palantir ville analysere norske helsedata under pandemien

Da pandemien traff Norge, fikk Direktoratet for E-helse tilbud om «pro bono»-bruk av teknologiselskapets verktøy.

I mars 2020 var det armer og bein i det norske helsevesenet – både som her på Haukeland, der selv nyankomne på akuttmottaket måtte sjekkes for koronasmitte, og også blant dem som styrer sykehusene og de andre delene av systemet. Samme måned tilbød Palantir seg å hjelpe med overvåkningen av pandemien. **(Foto: Marit Hommedal / NTB)**

Av **Hanne Østli Jakobsen, Journalist**

09/12/2021 06:55

Forrige uke skrev Morgenbladet om politiets innkjøp av programvare fra Palantir, det hemmelighetsfulle amerikanske selskapet som driver med dataanalyse og overvåkning. Det er fem år siden politiet kjøpte Gotham, et av Palantirs programmer – men systemet de fortsatt forsøker å få til å fungere, er noe helt annet: et saksbehandlingsverktøy skreddersydd for politiet. Saken har vært en verkebyll for alle involverte, selv om både Palantir og politiet nå skryter av et godt og konstruktivt samarbeid.

Les også: Slik ble politiets «supervåpen» en 100-millioners fiasko

Omnia, som prosjektet og programmet het, ble avsluttet rundt årsskiftet 2019/2020. Avgjørelsen ble likevel offentlig først fire måneder senere, i april. Da hadde pandemien inntruffet – og Palantir hadde begynt å se seg om etter nye muligheter i det offentlige Norge.

I slutten av mars 2020 tikket det nemlig inn en e-post til Direktoratet for e-helse, en av de mange delene av det norske helsevesenet som da jobbet på spreng for å forstå det nye viruset og dets virkninger på folk og samfunn. Avsender var Erik Ramstad, daværende «deployment strategist» for Palantir:

«Palantir Technologies og AWS (Amazon) samarbeider om en Pro Bono løsning for COVID-19 respons med en rekke offentlige aktører internasjonalt eksempelvis; CDC i USA og NHS i Storbritannia».

Ville det norske helsevesenet kanskje prøve gratis, de også?

«Integrering med minst mulig friksjon»

Tilbudet Palantir sendte ut, var en mulighet til å bruke programmet Foundry til å overvåke pandemien. Foundry er produktet Palantir selger til forretningsverdenen, til bedrifter som banker, bilprodusenter og flyselskaper. I e-postene Morgenbladet har fått innsyn i, beskrev Ramstad hvordan Foundry kunne hjelpe norske myndigheter til å «danne et mest mulig informert beslutningsgrunnlag» via et dashbord med nøkkeltall fra pandemien. Hans folk kunne starte arbeidet med å sette det opp umiddelbart.

«Fundamentet til Foundry ligger i eksisterende data og systemer så vi vil kunne jobbe simultant med etablering og integrering med minst mulig friksjon», skrev Ramstad.

Det samme tilbudet gikk på det tidspunktet til minst fem andre land i Europa, ifølge The Guardian. Sammen med gravejournalister fra land som Nederland, Tyskland og Hellas har de kartlagt hvordan Palantir bydde seg frem for europeiske myndigheter det første pandemiåret. Tyskland og Nederland fikk begge tilbud om å bruke Foundry, det samme fikk det europeiske smittevernbyrået ECDC – det tilbudet kom dem i hende ved hjelp av en introduksjon fra kolleger ved amerikanske CDC.

Les også: Palantirs systemer fanger stadig flere av oss i politiets søkelys

I Hellas takket myndighetene ja til tilbudet, som Morgenbladet omtalte i forrige uke. Avtalen ble først kjent flere måneder etter at den var inngått, da USAs ambassadør til Hellas, Geoffrey Pyatt, litt tilfeldig nevnte den i en tale han holdt på en helsekonferanse i Athen. Siden har både journalister og parlamentsmedlemmer kjempet for å få granske avtalen – som ifølge The Guardian inneholder både vidtrekkende og vage formuleringer om hvilke data Palantir skulle få tilgang til, og hvordan disse kunne brukes. Blant annet ble en bestemmelse om at dataene skulle være pseudonyme – og altså ikke mulig å knytte til konkrete borgere – tatt ut i en revidert versjon av avtalen.

Palantir sier til The Guardian at selskapet kun skulle bruke helsedata på aggregert og overordnet nivå.

Avvist som for langsiktig

Den første pandemivåren var det hektisk i Helse-Norge, og Direktoratet for e-helse forteller at de på den tiden mottok over 300 tilbud om hjelp fra ulike aktører. Et par dager etter henvendelsen fra Palantir svarte direktoratet, viser e-postutvekslingen: «Hei, og takk for henvendelsen. Vi får mange innspill og gode ideer for tiden. (...) Vi vil komme tilbake til dere dersom det blir aktuelt.»

To uker senere dumpet nok en e-post inn hos direktoratet:

«Hei,

Viser til tidligere korrespondanse 'Introduksjon av Palantir og AWS Covid-19' (...) Vi har til nå fokusert på krisehåndtering men vil fremover også rette fokus på mer fremtidsrettet konsekvensanalyse av tiltak og effekt. (...)

Om ønskelig demonstrer vi gjerne noe av arbeidet vi allerede har gjort over videomøte eller diskuterer aktuelle problemstillinger og eventuelt hvor vi best kan bidra.»

Siv Ingebrigtsen, som er avdelingsdirektør i Nasjonal styringsmodell-avdelingen hos Direktoratet for e-helse, forteller at direktoratet på den tiden hadde et sett av kriterier for å vurdere de mange tilbudene om hjelp som kom inn:

«Alle innspill ble vurdert etter om at de skulle støtte arbeidet med koronapandemien direkte og gi gevinster til innbyggere, helsepersonell og/eller myndigheter. Tiltakene skulle også kunne gjennomføres og gi gevinst i 2020, samt ha en høy grad av gjennomførbarhet. Det var også et krav at de ikke overlappet med andre tiltak som var i gang», skriver hun i en e-post til Morgenbladet.

«Denne løsningen ble vurdert av smittevernmiljøet som ikke aktuell på grunn av høyt ambisjonsnivå og langsiktig målbilde. Det var spesielt kriteriet om at vi ikke kunne ta ut gevinster allerede i 2020 som gjorde at denne løsningen ikke nådde opp.»

«Det var vår plikt å bidra»

Palantir, via kommunikasjonsmedarbeider Jan Hiesserich, skriver til Morgenbladet at Direktoratet for e-helse kunne brukt Foundry gratis i seks måneder dersom Direktoratet for e-helse hadde takket ja. Etterpå ville direktoratet stått fritt til å si opp avtalen.

«Vi er voldsomt stolt av rollen vi har hatt i å hjelpe myndigheter verden rundt håndtere pandemien», skriver Hiesserich.

– *Hva var bakgrunnen for denne henvendelsen?*

«Vi ga myndigheter og regjeringer mulighet til å bruke vår software kostnadsfritt for å håndtere covid-19-krisen, fordi vi grunnleggende sett mener at vår erfaring og teknologi, som allerede er utprøvd i kriser, gjorde at vi hadde en plikt til å bidra», skriver han.

Hiesserich understreker at Palantirs forretningsmodell *ikke* handler om å tjene penger på persondata: «Vi hverken samler, lagrer eller selger persondata, og vi bruker ikke persondata til å trene proprietære algoritmer eller maskinlæringsmodeller som vi deler eller selger videre til kunder.» Dette gjelder også tilbudene som gikk ut til verdens helsemyndigheter. Hos andre tok det «kun dager» å installere Foundry og ta verktøyet i bruk, skriver han.

«Vår software og våre tjenester kontrolleres av organisasjonene som kjøper dem: det er organisasjonene som bestemmer hva som kan og ikke kan gjøres med deres data, de kontrollerer hvordan analysene gjøres og enhver Palantir-ingeniør som hjelper dem i arbeidet er underlagt organisasjonens regler. Vi hverken overfører eller gjenbruker våre klienters data for våre egne formål. Det ville undergravet den tilliten som kreves for å jobbe i de miljøene der vi har bygget opp vårt selskap.»

Endret loven for å passe til Palantirs programvare

OVERVÅKNING *Palantir-anskaffelsen til dansk politi er tilsynelatende blitt en suksess. Det som krevdes, var en lovendring som åpner for storstilt innsamling av persondata.*

HANNE ØSTLI JAKOBSEN

I 2018 ble en kvinne overfalt bakfra og voldtatt da hun var ute og gikk på Nord-Jylland i Danmark. Hun anmeldte overgrepet, og beskrev gjerningsmannen som «etnisk dansk i olabukser, 35–42 år gammel, halvhøy og slank». Men politiet fant ikke noen som passet beskrivelsen. Ti år tidligere var en annen jente blitt voldtatt, 50 kilometer lenger sør på den danske øya. DNA-et fra de to voldtektssakene matchet, men politiet hadde ikke noe navn å knytte til funnene.

Det danske nettmagasinet Zetland fortalte historien om de to voldtektene i mai i år, i en artikkel om revolusjonen som til slutt oppklarte dem. En tredje sak, fra 1999, viste seg nemlig å matche voldtektsmannens *modus operandi*. Der var gjerningsmannen kjent, og han hadde bodd i området i årene siden. Det hele var etter hvert nok til at politiet kunne kreve en DNA-prøve fra mannen – og den matchet.

Nøkkelen til den oppsiktsvekkende oppklaringen var sammenstilling av informasjon og det kraftige søket i Pol-intel, skriver Zetland. Det er et dataprogram danskene kjøpte i 2016, fra Palantir Technologies, og som i internasjonal utgave heter Gotham.

Både norsk og dansk politi har inngått avtaler med teknologiselskapet Palantir Technologies de siste årene. Som Morgenbladet tidligere har skildret, er den norske anskaffelsen blitt en verkebyll av forsinkelser, kostnadsoverskridelser, juridiske problemer og teknisk krøll. I dag bruker norsk politi bare en svært nedskalert versjon av Palantirs program.

Den danske anskaffelsen fremstår imidlertid som en suksesshistorie, i hvert fall om man leser danske medier flyktig. Det er verdt å forsøke å forstå: Hvordan ble broderfolkets Palantir-kjøp tilsynelatende vellykket, når det norske programvarekjøpet gikk så på tverke?

– Det har vært veldig lite offentlig diskusjon om Pol-intel. Det er ikke lett å vurdere programmet, kunnskapen vi har, er om enkeltsaker som politiet har valgt å vise frem. Vi får ikke vite når programmet plukker ut feil person, sier Jesper Lund, leder av IT-Politisk Forening i Danmark, som har fulgt programmet siden anskaffelsen ble kjent.

– På den måten fremstår det som en suksess, men det er vanskelig å si, for politiet styrer informasjonsflyten strengt.

Fra terrorforebygging til etterretning

Terror var bakgrunnen da det danske politiet og Palantir først fant hverandre. Danmark er også medlem av Prüm, den internasjonale avtalen om politisamarbeid, men Prüm-forpliktelsene er blitt oppfylt ved hjelp av andre teknologiske verktøy. I 2015 ble danskene imidlertid rystet av terrorangrepet på Krudttønden, der islamister angrep et arrangement om kunst og ytringsfrihet. Etterpå ble det oppvask: Burde ikke terroristene vært stanset før? Politiet kom frem til at de trengte nye og bedre våpen for å bekjempe ny kriminalitet.

Den første versjonen av Pol-intel ble offisielt tatt i bruk sommeren 2017. Fortsatt jobbes det internt i politiet med å koble nye registre og informasjonskilder til systemet.

– Palantir og datafiseringen av politiarbeid i Danmark begynte som en veldig ambisiøs plan. Man ser det i avisoppslagene, fra halvoffisielt hold kalles det et «supervåpen», forteller Vasilis Galis, som studerer Pol-intel i den danske grenen av det internasjonale forskningsprosjektet *Critical understanding of predictive politicing*.

– Men like etter anskaffelsen blir den delen tonet ned.

Det «forutseende» ble isteden til «etterretningsledet politiarbeid», forteller Galis. Det er nemlig umulig å lage solide spådommer om fremtidig kriminalitet ut fra de få hendelsene som skjer i Danmark hvert år.

– I det etterfølgende er programmet bare blitt omtalt som et redskap for politiet, på linje med alt annet: en søkemaskin, noe som er mer brukervennlig for politiet, forteller Jesper Lund.

– Og de har noen virkelig gamle IT-systemer, så det siste stemmer nok.

Gordisk løsning på lovproblemet

I Danmark, som i Norge, innså man at Palantirs metode ville utfordre personvernlovgivningen: Dersom all informasjon politiet har lagret, kan dumpes inn i én søkemotor og brukes for all fremtid, er det vanskelig å snakke om «minimal håndtering av persondata», slik både dansk lov og den europeiske personvernforordningen GDPR krever. I 2017 ble dermed «Lov om endring av lov om politiets virksomhet og tolloven» vedtatt i Danmark, med følgende formulering:

«Politiet foretager tværgående informationsanalyser på grundlag af de oplysninger, politiet behandler, når det er nødvendigt af hensyn til udførelsen af politiets opgaver.»

Og videre:

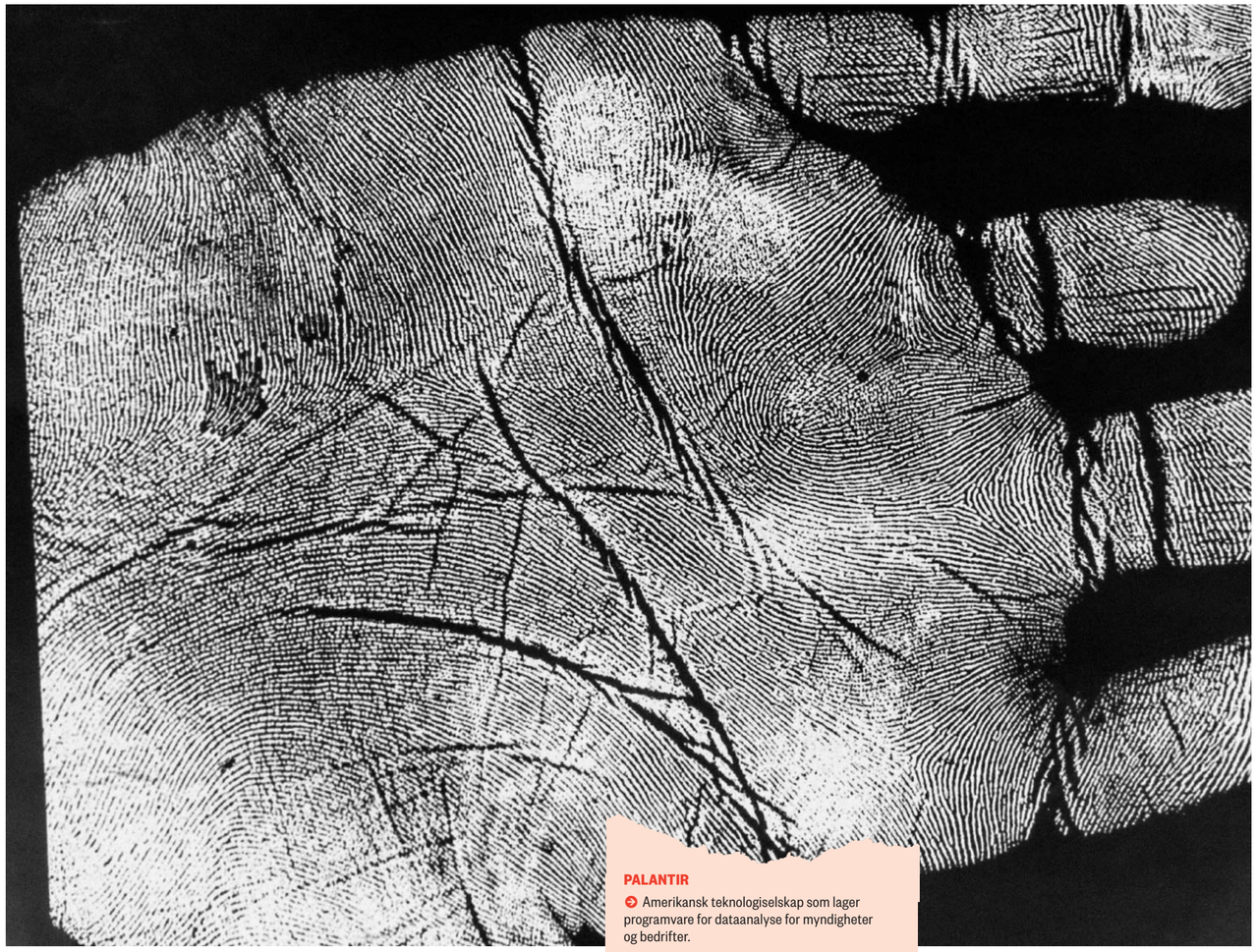
«Politiet kan indsamle og behandle oplysninger fra offentligt tilgængelige kilder, når det er nødvendigt af hensyn til udførelsen af politiets opgaver.»

– Loven nærmest avskaffer formålsbegrensningen for dansk politi. Alle databaser politiet har adgang til, kan brukes i Pol-intel, og de kan brukes på kryss og tvers, sier Lund.

Den nye loven åpner altså for at alle danske registre kan sammenkobles, dersom politiet mener at de trenger det. Offentlig tilgjengelig informasjon kan også hentes inn dersom politiet sier de har behov for det. Det gjelder informasjon fra det åpne nettet, fra sosiale medier og fra såkalte «data brokers», selskaper som selger persondata på nettet. Deres kunder er vanligvis annonsører, men det hender også at myndigheter i ulike land benytter muligheten til å kjøpe persondata på det frie markedet.

I Danmark er det også mulig for politiet å gjøre dette, og deretter legge dataene inn i Pol-intel. Dermed kan info fra Facebook-profiler eller informasjon som Holger Danske har lagt igjen i en nettbutikk, ende i politiets registre – uten at han nødvendigvis vil vite om det.

Loven nærmest avskaffer formålsbegrensningen for dansk politi. Alle databaser politiet har adgang til kan brukes i Pol-intel, og de kan brukes på kryss og tvers.
JESPER LUND, LEDER AV IT-POLITISK FORENING I DANMARK.



Alt er lov: Fingeravtrykk, DNA, bostedsadresser, meldinger på sosiale medier og shoppingmønstre. Alt det kan fôres inn i det danske politiets versjon av Gotham.
ILLUSTRASJONSFOTO: CHRISTIAN BELGAUX

PALANTIR

- Amerikansk teknologiselskap som lager programvare for dataanalyse for myndigheter og bedrifter.
- Palantirs programmer lar en organisasjon samle og sammenstille ny og gammel informasjon i ett felles arbeidsområde.
- Der kan dataene analyseres og visualiseres, slik at organisasjonen kan få bedre oversikt.
- Palantir har laget Omnia, et saksbehandlingsverktøy for internasjonalt politiarbeid, for det norske politiet. Pol-intel, den danske versjonen av programmet Gotham, brukes av dansk politi.

Denne uken deltok Lund på en konferanse om forutseende politiarbeid i København, i regi av CUPP-prosjektet. Der luftet han sin bekymring for at dansk politi med Pol-intel har stadig flere insentiver til å samle inn data om borgerne, og frykten for at dataene kan bli brukt feil. I panelet deltok også Courtney Bowman, som har tittelen *Global Director of Privacy and Civil Liberties Engineering* i Palantir. Han svarte ikke direkte på bekymringene til Lund, men understreket i sitt foredrag at Palantir ikke er et dataselskap, men heller et selskap som selger software. Dersom programmet brukes til for eksempel for vidtrekkende overvåkning, skyldes det valgene til organisasjonen som har kjøpt det:

«Teknologien bidrar med verktøyene – det er menneskene, politibetjentene, som kan sørge for god bruk», sa Bowman.

«Man kan ikke stanse Pol-intel»

I dag har alle danske politioffiserer tilgang til Pol-intel, som et søkeverktøy når de trenger informasjon om en mistenkt eller arrestert.

– Så finnes det ulike nivåer av tilgang over det. Etterforskere har for eksempel tilgang til funksjoner som lar dem sammenstille informasjon, forteller Galis, som i disse dager studerer hvordan danske politibetjenter bruker programmet.

Det er vanskelig å vite nøyaktig hvilke data som finnes i systemets mage. Lund sier han ikke vet om data fra persondataselgere er tatt inn i Pol-intel – det skulle komme en offentlig kunngjøring dersom slike data ble inkludert, forteller han, men den kan ha blitt sendt ut uten at han har fått det med seg. Dansk politi har ikke besvart Morgenbladets henvendelser om Pol-intel til denne artikkelen

I Norge er det et åpent spørsmål om den fulle versjonen av Palantirs programvare noensinne vil bli tatt i bruk. I Danmark er den katten ute av sekken, tror Jesper Lund.

– Jeg tror ikke man kan stanse Pol-intel. Men kanskje kan offentlig debatt skape noe mer oppmerksomhet om hvordan det brukes og hvilke risikoer det har ved seg.

I mai i år spurte en representant fra Folketinget hvordan politiet jobber for å forhindre såkalte *feedback loops* i systemet. Det er mekanismen der noen personer blir stoppet av politiet oftere, for eksempel på grunn av etnisitet eller fordi de befinner seg i et belastet område, og deretter blir sett på som mer mistenkelige nettopp *fordi* de har vært i kontakt med politiet mange ganger. I svaret meldte Justisministeriet at politiet ikke benytter feedback loops – men også at det å sette inn mer politiressurser i områder med mer kriminalitet er et viktig arbeidsverktøy.

– På den ene siden sier de altså at de ikke har feedback loops i Pol-intel, og i den neste setningen sier de at det er et grunnvilkår for hvordan de arbeider. Det er bekymringsverdig, sier Jesper Lund.

hj@morgenbladet.no

– Det er en veldig vidtrekkende lov. Var det offentlig debatt da den kom, eller nå?

– Det er helt klart noen prinsipielle problemstillinger knyttet til datavern i loven, men det er det ingen som bryr seg veldig om. Den generelle bekymringen om at politiet samler inn mange flere opplysninger via Pol-intel, ved hjelp av et amerikansk firma, den skaper ikke videre oppmerksomhet, sier Lund.

Vil åpne for storstilt nettovervåking fra PST

Et nytt lovforslag vil la Politiets sikkerhetstjeneste lagre og analysere store mengder informasjon fra nettet. Forslaget slaktes av Advokatforeningen og beskrives som et kraftig inngrep i personvern og privatliv av kontrollorganet for de hemmelige tjenestene.

HANNE ØSTLI JAKOBSEN
OG IDA LYNGSTAD WERNØ

Justisdepartementet vil gi Politiets sikkerhetstjeneste (PST) mulighet til å lagre store deler av det du og jeg sier på det åpne internett. Det kommer frem i et lovforslag som nå er ute på høring:

«Det foreslås (...) en ny bestemmelse i politiregisterloven som åpner for at PST kan lagre, systematisere og analysere store mengder åpent tilgjengelig informasjon til etterretningsformål, selv om den enkelte opplysning isolert sett ikke er nødvendig for dette formålet.»

Forslaget ligner på den danske lovendringen fra 2017, som Morgenbladet skrev om før jul. Den ga dansk politi adgang til å lagre, systematisere og analysere data fra både politiregistre og det åpne nettet.

– Loven nærmest avskaffer formålsbegrensningen for dansk politi, sa IT-ekspert Jesper Lund til Morgenbladet om den endringen.

«Forslaget vil bidra til at PST kan avdekke ukjente trusselaktører, kartlegge utviklingen i trusselbildet og oppdage nye fenomener som kan medføre nye trusler». Slik beskriver Justisdepartementet bakgrunnen for det norske lovforslaget. Som eksempel nevnes at PST trenger å kunne følge med i de såkalte«chan-ene» – ulike fora som befolkes av både ekstremister og andre, mer harmløse nettbrukere.

Men departementet innrømmer at forslaget innebærer «betydelige personvernmessige betenkeligheter»: Om forslaget blir til lov, trenger ikke PST lenger å vite at den enkelte opplysningen de henter inn – en kommentar på nettet, en brukerprofil – er nødvendig for å forebygge terror eller hindre annen alvorlig kriminalitet. For å si det med høringsnotatets ord: PST vil behandle store mengder informasjon, og mye av den «vil være av mindre interesse for PST».

Det kalles «dragnet policing», eller tråling på godt norsk: Samle alt, se hva du trenger etterpå. Departementet vil at dataene skal kunne lagres i 15 år.

Kritisk til forslaget: Elisabet Line Haugsbø, visepresident i Tekna. FOTO: MIKKEL MOE / TEKNA

Er datainnbrudd greit?

– Forslaget er veldig diffust. De sier ikke mye for eksempel om hvilke åpne kilder de har tenkt til å bruke. Allerede der begynner problemene, sier Elisabet Haugsbø, visepresident i fagforeningen Tekna. Hun jobber til daglig med havstordata i stiftelsen C4IR Ocean.

Lovforslaget nevner noen eksempler på åpne kilder, som avisartikler og blogger, men har ingen uttømmende oversikt over hvilke kilder PST ønsker å tråle. «Det man ikke kjenner til, vet man heller ikke hvor man skal lete etter», skriver Justisdepartementet om hvorfor det nøyaktige kildetilfanget holdes åpent.

– Alle sosiale medier er åpne kilder, uansett om du har lukket konto eller ikke. Det tror jeg ikke alle er klar over. Det samme gjelder informasjon som andre legger ut om deg. Det er ikke nødvendigvis noe du vet om eller har oversikt over, påpeker Haugsbø.

Forslaget sier ikke noe om hvordan befolkningen skal informeres om at åpen informasjon fra nettet kan lagres, eller hvordan myndighetene vil sikre at folk vet hva som er en åpen kilde. Et annet uavklart spørsmål er om informasjon fra datainnbrudd kan regnes som åpen. Nylig ble kundedata fra hotellkjeden Nordic Choice spredt på nettet – slike data kan formodentlig også sankes inn i fremtiden.

– Jeg kan ikke se, ut fra det de skriver, om dette er noe de har tatt høyde for, sier Haugsbø.

Jon Wessel-Aas, leder i Advokatforeningen, peker på det samme: Hva er egentlig «åpent tilgjengelig informasjon»?

– Det er åpenbart at det enhver kan lese på nettet, vil anses som åpent tilgjengelig, men så kommer for eksempel spørsmålet om lukkede grupper, som kanskje har såpass mange medlemmer at de ikke er helt private – hva vil de gjøre der? Skal de kunne gå inn med falske profiler for å samle data derfra? spør Wessel-Aas.

– Lovforslaget definerer ingen reelle grenser for innsamlingen og sier svært lite om hvordan dataene kan behandles når det samles inn.

Risiko for formålsutglidning

Det norske forslaget går ikke fullt så langt som den danske loven: Justisdepartementet skriver blant annet at opplysningene skal forbeholdes «bemyndigede personer», og legger som forutsetning at opplysningene skal være «sperret». Det betyr at de kun kan brukes til det formålet de er hentet inn for, og ikke kan søkes i av PST-folk som jobber med andre oppgaver eller når det kommer henvendelser fra andre organer.

Senere i samme høringsnotat åpner Justisdepartementet likevel for mer bruk av dataene.

Åpne data fra nettet skal kun hentes inn til «etterretningsformål», skriver departementet. Men de vil *også* at allerede innsamlet informasjon skal kunne brukes til ytterligere to formål, nemlig i såkalt forebyggende saker, og i forbindelse med PSTs etterforskningsoppgaver. EOS-utvalget, kontrollorganet for de hemmelige tjenestene i Norge, har levert en kritisk høringsuttalelse om lovforslaget. De mener formuleringene innebærer en klar risiko for formålsutglidning: «Denne typen bruk av opplysninger fra masseinnsamlingen i konkrete saker vil utgjøre et nytt og kraftigere inngrep i de berørtes personvern og privatliv.»

ILLUSTRASJONSFOTO: CHRISTIAN BELGAUX

DIGITAL ETTERFORSKNING

- De siste månedene har Morgenbladet undersøkt hvordan nye digitale verktøy påvirker arbeidsmetodene for politi og etterretningstjenester.
- 3. desember fortalte vi hvordan politiets anskaffelse av analyseprogrammet Omnia fra Silicon Valley-selskapet Palantir har utviklet seg til en fiasko.

- 17. desember rapporterte vi fra Danmark, som har endret loven slik at den gir politiet mulighet til å bruke Palantirs verktøy – og samtidig åpner for omfattende digital overvåkning, ifølge kritikere.

Det er heller ikke noe krav om at «så få personer som mulig» skal ha adgang til opplysningene som samles inn. Justis- og beredskapsdepartementet nøyer seg med å anta at det er slik det vil bli i praksis.

«Høflig formulert slakt»

Fredag 7. januar går høringsfristen til departementets høringsforslag ut. Advokatforeningens leder Jon Wessel-Aas kaller foreningens høringssvar «en saklig og høflig formulert slakt» av forslaget. Han mener departementet i «svært liten grad» begrunner hvorfor endringene er nødvendige og forholdsmessige, til tross for at de erkjenner at lovendringen vil innebære en klar inngripen i folks personvern og kan ha en «nedkjølende effekt på ytringsfriheten».

– Vi forventer at departementet konkretiserer og begrunner hvorfor det er nødvendig og forholdsmessig at PST skal få en så inngripende hjemmel for å kunne utføre oppdraget sitt. Hvis departementet skal fremme et lovforslag i denne retningen, gjenstår det mye arbeid før dette kan godtas, sier Wessel-Aas.

– Vi synes også departementet tar altfor lett på at både EU-domstolen og menneskerettsdomstolen har tatt stilling til andre typer masseinnsamling av elektroniske kommunikasjonsdata fra befolkningen, og lagt noen klare begrensninger på adgangen til å gjøre det for myndighetene.

Skitt inn, skitt ut

Justisdepartementet er klar over at endringene de foreslår, er kontroversielle. Lovforslaget vil i praksis bety et inngrep i retten til respekt for privatlivet, og det kan virke nedkjølende på ytringsfriheten, skriver departementet i høringsnotatet. Men som de skriver: PST trenger å lagre internettopplysninger på denne måten for å kunne «følge med» på nettet. Dermed må privatliv- og ytringsfrihetsbekymringen vike, slik departementet tolker det.

Notatet beskriver ikke hvilken teknologi PST vil bruke til å samle inn og systematisere informasjonen. Som Morgenbladet har skrevet tidligere, kan PST hverken bekrefte eller avkrefte om de allerede bruker Gotham, programvaren til Silicon Valley-selskapet Palantir.

Uansett vil PST trenge maskinhjelp for å behandle dataene, understreker Elisabet Haugsbø i Tekna. Intet menneske vil kunne prosessere den mengden informasjon som PST vil kunne hente inn med denne lovendringen. Dermed burde lovforslaget også inkludere refleksjoner om betenkelighetene ved slik automatisert behandling, sier hun:

– Noen grupper har høyere risiko for å bli plukket ut av en algoritme enn andre. Slik er det alltid, for grunnlaget for å utvikle en algoritme vil aldri være fritt for skjevheter, sier Haugsbø.

– Så la oss si at det i tillegg er noen grupper i befolkningen som har mindre oversikt over hva som er åpen informasjon som kan samles inn, enn andre. Hva gjør man hvis det er sammenfall mellom de to gruppene? Skal man veie opp for det, eller blir dette – som man sier i bransjen – *shit in, shit out?*

Haugsbø deler bekymringen til EOS-komiteen om at lovforslaget er for åpent formulert.

– Generelt mener jeg man bør avklare prosessene først: Hvordan har man tenkt å gjøre innhentingen? Hva er formålet. Det bør avklares før loven er vedtatt, sier hun.

– Jeg har all forståelse for at intensjonen er god, men jeg er usikker på om de har tenkt ordentlig gjennom fallgruvene.

Justis- og beredskapsdepartementet er blitt forelagt kritikken fra Tekna og Advokatforeningen. Kommunikasjonsrådgiver Andreas Bjørklund viser til at høringssvarene etter høringsfristen vil bli behandlet i departementet.

– Høringen skal nettopp få frem ulike problemstillinger som må vurderes nærmere, sier Bjørklund.

hj@morgenbladet.no
ida.werno@morgenbladet.no

PST: Lovendringen er «helt nødvendig»

– Det kan virke skummelt og stygt, dette, men jeg mener at det ikke er noen dramatisk endring i lovverket, sier PST-sjef Hans Sverre Sjøvold.

IDA LYNGSTAD WERNØ

For kunne PST følge med på at Boot Boys-medlemmer demonstrerte i gatene – i dag opererer «personene som utgjør en fare for sikkerheten», på internett, sier Sjøvold. Han kaller lovendringen «en tilpasning til den digitale verden».

– I dag er det veldig strenge regler for å lagre data fra åpne kilder. Vi kan jo følge med på slike data i sanntid, men har ikke mulighet til å lagre eller systematisere opplysningene. Det er en umulig oppgave for en organisasjon å skulle følge med på alle flater på den måten, sier han.

Etterretningstrender

Selv om PST i teorien vil kunne hente ned all «åpent tilgjengelig informasjon» dersom lovendringen går gjennom, mener Sjøvold at det ikke vil bli aktuelt.

– Vi kommer til å målrette innsamlingen av dataene. Det er jo ikke sånn at vi vil lagre alle dataene fra åpne kilder – det har vi hverken interesse av eller kapasitet til. Det vi ønsker, er å kunne følge med på aktivitet på ulike flater vi mener det er nødvendig for oss å følge med på.

– Flere kritikere mener endringene vil gripe inn i folks privatliv. Det erkjenner også Justisdepartementet selv. Kan du forstå bekymringen?

Nye tider: Lovforslaget er en «tilpasning til den digitale verden», sier PST-sjef Hans Sverre Sjøvold. FOTO: KNUT EGIL WANG

– Ja, det gjør vi. Det som er viktig for oss å få frem, er att dette i første omgang dreier seg om å innhente data fra åpne kilder som kan gi oss svar på etterretningstrender. Skulle vi i vårt arbeid med åpne kilder komme over en situasjon eller en person som gjør det nødvendig å jobbe videre, vil vi gjøre det ut fra klare hjemler. Det gjør vi jo uansett ellers.

Dette er hjemler som allerede finnes, ifølge Sjøvold.

– Skal vi lagre data i våre registre, er det egne regler. Skal vi jobbe med en forebyggende sak, er grunnlaget regulert i politiloven og politiregisterloven. Er det en straffesak, er det regulert i straffeprosessloven – det er ikke noen endring i disse reglene, sier PST-sjefen.

– Vi sitter ikke med en stor database over masse mennesker som er lagret i våre registre. Men når vi skal analysere større mengder data, må vi nødvendigvis også hente inn data fra personer vi ikke har noen interesse av. Det er bare i etterretningsøyemed, altså for eksempel for å beskrive en trend.

Ikke bekymret

Sjøvold vil ikke si noe om hvilke teknologiske løsninger PST vil bruke, eller hvordan de ser for seg at datainnsamlingen- og bearbeidelsen skal gjennomføres rent praktisk.

– Det legale rammeverket må på plass først. Vi legger primært ikke opp til noen diskusjon knyttet til teknologiske løsninger, sier han.

PST-sjefen mener det er liten grunn til å bekymre seg for at en eventuell lovendring vil ha «en nedkjølende effekt» på ytringsfriheten.

– Vi er iallfall ikke interessert i å dempe det på noe vis – vi er ikke noe meningspoliti. I den grad vi oppdager noe som skulle dreie seg om mulige straffbare forhold, har vi en plikt til å undersøke det uansett. Det er jo vårt hovedoppdrag.

ida.werno@morgenbladet.no