Avslørt av mobilen

Metoderapport SKUP 2020

NRK Nyheter

NRK beta

Innsendere
Henrik Lied – redaksjonell utvikler og journalist – 404 55 897 – henrik.lied@nrk.no
Martin Gundersen – journalist – 477 56 515 – martin.gundersen@nrk.no
Trude Furuly – journalist – 454 16 528 – trude.furuly@nrk.no
Øyvind Bye Skille – journalist – 414 73 220 – oyvind.bye.skille@nrk.no
Harald K. Jansson – kartutvikler – 984 83 961 – harald.k.jansson@nrk.no
Mari Grafsrønningen – designer – 971 35 741 – mari.grafsronningen@nrk.no
Ståle Grut – journalist – 932 40 711 – stale.grut@nrk.no
Marius Arnesen – 982 30 516 – marius.arnesen@nrk.no

Takk til: Arbeidsledelsen ved Arve Bartnes og Marius Tetlie.
Silje-Lisette Tennøy, Tiril Mettesdatter Solvang, Øyvind Nyborg, Eskil Wie Furunes, Line Tomter, Håkon Vårhus Sagen, Johan Bull og Arild Eskeland.

Kontakt NRK: Arve Bartnes – 911 64 223

Redaksjon
NRK
Bjørnstjerne Bjørnsons plass 1, 0340 Oslo

Utvalgte saker

- Avslørt av mobilen (9. mai 2020)
- Guide: Slik begrenser du sporing av din mobil (9. mai 2020)
- Datatilsynet opnar gransking etter mobilsporing (10. mai 2020)
- 8300 mobiler sporet på sykehus og krisesentre (11. mai 2020)
- Norske offiserer og soldater avslørt av mobilen (18. mai 2020)
- Her avslører sminkeappen stortingspolitikerens jobbreise (1. juni 2020)
- Telefonen spionerte på meg. Slik fant jeg overvåkerne (3. desember 2020)
- Europeisk datatilsyn åpner granskning etter NRKbeta-avsløring (11. desember 2020)

Alle publiserte saker med lenke er lagt i vedlegg 1 i metoderapporten.

Innholdsfortegnelse

Innledning

Mobilen er med oss over alt. På jobb, når vi henter i barnehagen og når vi besøker venner. Med en selvsagt plass i livene våre bidrar den til at vi holder oss oppdatert og forenkler mange av hverdagens gjøremål.

Men mobilen kan også avsløre våre hemmeligheter. Den røper hvor vi beveger oss, hvem vi treffer og hva vi jobber med. For noen utgjør mobilen en risiko for egen sikkerhet.

Apper vi installerer på mobilen samler kontinuerlig inn våre bevegelsesdata. Denne informasjonen er så verdifull at den har skapt en helt ny industri. Den består blant annet av apputviklere og dataforhandlere som selger og formidler mobildata i et globalt nettverk.

I dette prosjektet har NRK avdekket data som viste de nøyaktige posisjonene til uvitende nordmenns mobiltelefoner. For 35.000 kroner kjøpte NRK informasjon av et britisk selskap. I dataene sporet vi de detaljerte bevegelsene til 140.000 mobiler i Norge gjennom 2019.

Informasjonen NRK kjøpte inneholdt ingen navn eller telefonnummer. Likevel kunne NRK ved hjelp av nye metoder og graving i åpne kilder, identifisere og kartlegge livene til et hundretalls nordmenn; offiserer, en stortingspolitiker og vanlige folk.

Én av dem var en småbarnsfar fra Stavanger. Vi kunne se at han hadde vært på sykehus, på et jobbintervju og hvilke dyr han oppsøkte under et helgebesøk i Dyreparken i Kristiansand. Mannen visste ingenting om at en av mobilappene sporet ham, og at informasjonen hadde blitt solgt på det åpne markedet.

Noen kan utsettes for denne typen mobilsporing når de er på sitt livs mest sårbare. NRK fant over 8300 mobiler inne på norske sykehus og krisesentre.

NRK har også avslørt hvordan denne globale industrien opererer, med våre egne mobildata som eksempel. De endte opp hos et selskap med amerikanske myndigheter på kundelisten.

Metode

1. Sporing av mobildata

Prosjektet «Avslørt av mobilen» har sitt utspring i en sak NRKbeta publiserte høsten 2019[1]. Den handlet om at Telenor og Telia tjente penger på å selge analyser av kundenes mobilbevegelser. Begge teleoperatørene understreket at de hadde gjort flere tiltak for at informasjonen ikke kunne misbrukes.

Ideen om å gjøre butikk på personlig informasjon er ikke ny, men som NRK avdekket i 2018, kan data om våre bevegelser være svært avslørende og føre til stor skade om de kommer i feil hender. NRK avslørte da at norske soldater ble sporet av treningsappen Strava mens de var stasjonert på skarpe oppdrag.[2]

Erfaringene vi hadde fra dette arbeidet, gjorde at vi spurte oss: «Finnes det andre aktører som hadde tilgang til store mengder lokasjonsdata?» Ved å gjøre søk på Google med fraser som «location data broker» og «mobile location data» fant vi nærmere 30 selskaper. Mange av dem tilhørte en kategori selskaper kalt dataforhandlere – selskaper som kjøper og selger store mengder personlig informasjon. Noen av disse selskapene spesialiserer seg på å samle inn data fra mobilapper.

Var noen av disse selskapene villige til å selge oss informasjon om nordmenn? Vi har tidligere forsøkt å lage journalistikk på dataforhandlerbransjen, men har møtt lukkede dører så snart selskapene forstod at vi ville bedrive kritisk journalistikk på dem. Erfaringene tilsa at det ville være svært vanskelig eller umulig å kjøpe data om vi oppga at formålet var å undersøke dataenes skadepotensial.

Etter grundige diskusjoner hvor etikkredaktøren i NRK var involvert, kom vi frem til at vi kunne kontakte disse 30 selskapene og opplyse at vi var journalister i NRK. For å sikre at vi skulle få kjøpt dataene og starte jobben med å teste våre hypoteser, besluttet vi å oppgi at dataene skulle brukes til et redaksjonelt prosjekt om byplanlegging. Vår vurdering var at dette var den eneste muligheten for at vi kunne få tilgang til mobildataene.

Tre selskaper oppga at de var interessert i å selge NRK detaljerte mobilbevegelser. Et av dem var det britiske selskapet Tamoco. Selskapet som er en London-basert dataforhandler som selger og videreformidler lokasjonsdata fra mobilapper. I en e-post oppga selskapet at de daglig fikk vite de presise bevegelsene til omtrent 30.000 mobiltelefoner innenfor Norges grenser.

Tamoco var den eneste av de tre selskapene som var basert i Europa, noe som gjorde at de var underlagt den felleseuropeiske personvernreguleringen GDPR. Geografisk nærhet og liten tidsforskjell gjorde også at vi trodde det ville være enklere å holde kontakt med selskapet og på sikt gjennomføre et intervju.

All kommunikasjon med Tamoco foregikk på e-post og selskapet stilte ingen krav til hvordan dataene skulle håndteres for å sikre mobileiernes personvern. For oss var det et rødt flagg. Hadde ikke selskapet rutiner for å beskytte den potensielt meget sensitive informasjonen?

[1] https://nrkbeta.no/2019/10/11/telia-og-telenor-selger-analyser-av-hvor-mobilbrukere-befinner-seg/
[2] https://www.nrk.no/urix/1.13891513

Etter utveksling av et par e-poster ble NRK bedt om å signere en konfidensialitetsavtale med selskapet for å få tilsendt en smaksprøve. Avtalen var at NRK skulle undersøke om et lite utvalg av dataene kunne brukes til det redaksjonelle prosjektet. Om de tilfredsstilte våre krav skulle NRK betale for en fullstendig datapakke.

Dette reiste flere dilemmaer: Hva forpliktet vi oss til ved å signere en slik avtale og hva kunne konsekvensene være om vi brøt den? Sammen med redaksjonsledelsen og en av NRKs advokater kom vi frem til at NRK kunne publisere eventuelle funn uten å bryte kontrakten.

Vi valgte å signere konfidensialitetsavtalen. En beslutning om å navngi selskapet eller ikke kunne vi gjøre på et senere tidspunkt, når vi visste mer om dataene det var snakk om.

2. Vi bygger dataverktøy

I november 2019 sendte Tamoco oss en smaksprøve på dataene i deres besittelse. Den var mer omfattende enn vi kunne håpe på, og kom i form av 13 datafiler i formatet CSV. Formatet brukes ofte til å dele filer med informasjon som passer inn i et regneark.

I datapakken var det tusenvis av rader med informasjon, fordelt på en rekke kolonner.
Vi mistenkte kjapt at det lå store muligheter for oss i denne smaksprøven:

- Kunne vi finne mobilnumre og identiteten til eierne som nå bare framsto som tall og tegn?
- Kunne vi deretter spore aktivitet og mobilenes fysiske bevegelser over tid?
- Hvor mye avslørte smarttelefonen om sine eiere?
- Lå det også sensitive data om personer innen politikk og forsvar i materialet?

Dataene kom ikke med en manual for hvordan de skulle tolkes, eller et program for å utforske dem. Og ifølge Tamoco selv var dataene anonymisert av personvernshensyn.

Vi måtte legge en plan, og bruke tid på å sette oss inn i dataene, for å forstå hvordan de kunne brukes til å utforske hypotesene våre. Mange av utfordringene handlet i stor grad om tekniske løsninger og programvare. I NRKbeta jobber vi daglig med datajournalistikk, og vi hadde derfor god oversikt over hvilke verktøy som ville egne seg til å gjøre de analysene vi trengte. Prosjektet ville forutsette kompetanse innen databaser, programmering og geografisk analyse.

Utenfor forsvars- og etterretningskretser er analyse av slike data uvanlig, og ikke noe som mange har gjort tidligere. For enkelte problemstillinger så vi at det manglet kommersielt tilgjengelige løsninger. Vi forsto at det ble nødvendig å utvikle egne dataverktøy for å kunne analysere dataene vi satt på. Selvlagde dataverktøy ble en av prosjektets avgjørende suksessfaktorer.

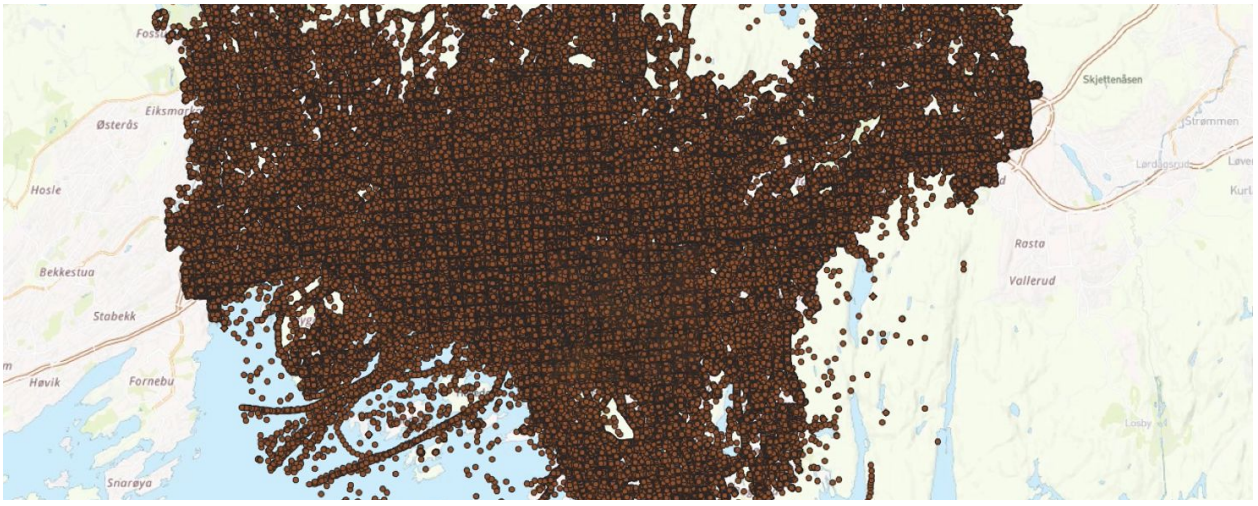
Da vi begynte å studere smakspøven så vi at fire av kolonnene pekte seg ut som spesielt interessante for oss. Tamoco hadde gitt dem navnene: **device_id**, **latitude**, **longitude** og **timestamp**.

- ***Device_id*** var en unik identifikator som avslørte *hvilken* mobiltelefon som hadde blitt sporet.
- ***Latitude*** og ***longitude*** var de geografiske koordinatene som fortalte hvor telefonen hadde vært.
- ***Timestamp*** var dato og tidspunktet da koordinatene ble registrert.

I tillegg inneholdt datapakken en egen kolonne som het ***app_name***. I denne kolonnen stod det i enkelte tilfeller navnet på mobilappen som hadde sendt dataene til Tamoco. Dette skulle senere bli nyttig for oss i arbeidet med å identifisere en stortingspolitiker og å kartlegge bransjen.

Device_id var helt avgjørende for å kunne følge én person. Ved å gruppere alle datapunktene til en spesifikk ***device_id*** kunne vi følge en enkelt mobils bevegelser over tid. Det var avgjørende for å kunne finne identiteten til telefonens eier. Siden dataene beskrev geografisk informasjon bestemte vi oss for å legge dem inn i dataprogrammet Qgis. Det er bransjestandarden for å visualisere geografiske data, og verktøyet støtter CSV-filer.

Da vi la datapakken inn i Qgis fikk vi opp 11 millioner prikker. Hver prikk indikerte at en mobil hadde vært på akkurat det stedet på et bestemt tidspunkt. Trykket vi på en av prikkene i Qgis fikk vi opp mer informasjon som for eksempel mobilens modell og hvor god nøyaktighet telefonens GPS hadde.



HVER PRIKK ER EN MOBIL*: Smaksprøven fra Tamoco ble til prikker som dekket hele Oslo kommune og deler av Bærum. Hver prikk viser hvor en norskeid mobil oppholdt seg september 2019.*

Detaljgraden i dataene forbløffet oss. Vi kunne se at registreringene typisk hadde en GPS-nøyaktighet på 4 til 20 meter. Datapakken omfattet bare Oslo og deler av Bærum over en tidsperiode på en måned, men det kilte i magen. Vi var inne på noe.

I dataene var det ingen navn eller telefonnumre. Tamoco hadde selv beskrevet dataene som anonymiserte. Skulle vi klare å identifisere noen av mobileierne med navn, nyttet det ikke å se på alle mobilenes bevegelser på et kart. Vi måtte finne en måte å følge bevegelsene til én og én mobil.

Siden vi ikke fant et dataprogram som løste akkurat denne utfordringen bestemte vi oss for å bygge et selv. Vi kalte det Gjerdeprogrammet.

Første steg var å lage en nettside som viste et kart over Oslo. Gjerdeprogrammet bygget vi som en intern nettside som leste inn smaksprøve-dataene fra en SQL-database. Denne nettsiden hadde kun prosjektets medarbeidere tilgang til. Vi utviklet Gjerdeprogrammet i programmeringsspråket Python. For å kunne gjøre det tok vi utgangspunkt i dataverktøyene Flask og Mapbox GL. De fungerer utmerket til å henholdsvis bygge servere og presentere digitale kart.

På Gjerdeprogrammets nettside kunne vi nå trykke på det digitale kartet og tegne en firkant rundt et område som interesserte oss. Alle mobiler som var innenfor dette området dukket opp i en liste i kartet. Der hadde de navn som «Mobil 1», «Mobil 2». Når vi nå klikket på for eksempel Mobil 2 sendte vårt Gjerdeprogram denne informasjonen videre til visualiseringsverktøyet Kepler.gl[3].

Kepler visualiserte alle bevegelsene til en mobil på et interaktivt kart. Dermed kunne vi følge mobilens bevegelser som prikker på et kart døgnet rundt i tidsrommet datapakken omfattet - september 2019. Gjerdeprogrammet spilte også her en nøkkelrolle. Kepler kunne ikke hente data fra en database. Derfor sendte vårt program en CSV-fil med en mobils bevegelser til Kepler.

En av de første mobileierne vi klarte å identifisere fant vi ved hjelp av nettopp Gjerdeprogrammet. Vi tegnet et digitalt gjerde rundt Telenor-bygget på Fornebu. Da fikk vi opp en liste med et titalls telefoner i programmet vårt. Ved å trykke på en tilfeldig telefon fikk vi denne mobilens bevegelser, og så at den hadde lagt bak seg en mengde prikker på to ulike steder i kartene over Oslo og Bærum: Fornebu og Nordstrand. Vi zoomet inn på prikkene på Nordstrand, og så at de lå innenfor en boligadresse.

Vi plottet adressen inn i nummeropplysningstjenesten 1881.no, og fikk navn på to personer som bodde på adressen. Google-søk på de aktuelle navnene førte oss til deres Facebook-profiler, som avslørte at mannen i huset jobbet i Telenor-bygget på Fornebu.

Dette var det første «wow-øyeblikket» i prosjektet. Med utgangspunkt i smaksprøven hadde vi lyktes med å spore og identifisere enkeltmennesker i dataene. Erfaringene så langt viste også at dataene som var til salgs om nordmenn var nærgående og sensitive – og på ingen måte anonyme som Tamoco hevdet.

Vi ville nå teste om vi kunne avsløre identiteten til norske maktpersoner, ansatte i Forsvaret, og mennesker i sårbare situasjoner. Det forutsatte at vi kjøpte den norske mobildataen som Tamoco tilbød på det åpne markedet. Redaktørene ga grønt lys.

3. Vi intervjuer Tamoco-dataene

Dermed kjøpte vi datapakken for 35.000 kroner. Den inneholdt mobilbevegelser for 140.000 mobiler fra 2019. Til sammen fortalte dataene hvor disse mobilene hadde oppholdt seg 460 millioner ganger innenfor Norges grenser. Vi hadde aldri håndtert så store datamengder før.

En journalists standardverktøy for å jobbe med strukturerte data er ofte Excel, men her var datamengden så stor at programmet ikke kunne brukes. Vi valgte å bruke databasemotoren PostgresSQL. Det er en avansert databasemotor som er gullstandarden for bruk av geografiske data, og flere av oss hadde brukt den tidligere. Slik kunne vi overføre de 460 millioner radene til en tabell i den nyopprettede databasen for Tamoco-dataene våre.

[3] https://github.com/keplergl/kepler.gl

device_id	timestamp	latitude	longitude
PW7OQWidQNRMw9Y	2019-12-14 11:41:43.698	59.01674000000001	10.0169
fkeNSSaFWB8QgIv	2019-12-05 23:37:04.47	69.64324	18.92993
FT08StyfSR8aK7W	2019-12-22 02:41:59.99	59.975597	11.042522
0k2pR7auwO5ND+i	2019-12-08 14:49:44.965	59.149	10.20802
JrWeSZynxCz1JE3	2019-12-05 23:37:06.96	59.669567	9.655268
p2WEQJaRWsBxDwB	2019-12-12 20:36:13.083	63.99118000000001	10.207008
+pcWRFqJGii3QiU	2019-12-09 14:45:59.599	69.95470999999999	21.883024

SLIK SER DATAENE UT: *Da dataene endelig var importert til databasen, så den essensielle informasjonen slik ut. Neste utfordring var å intervjue disse dataene.*

Med dette på plass kunne vi starte prosessen med å skrive SQL-spørringer. SQL-spørringer er måten man får ut systematisert informasjon fra en database. Hvis man ser for seg en database som et bibliotek, kan SQL-spørringen sammenlignes med bibliotekaren. Man kan spørre bibliotekaren om å få alle bøkene i biblioteket, men jo mer konkret forespørselen er på tema og tittel, jo bedre respons får man fra bibliotekaren. Det samme gjelder en SQL-spørring. Spesifikke spørsmål gir nyttige svar.

Slik vi hadde bygd opp Gjerdeprogrammet vårt, stilte vi rett og slett et spørsmål idet vi tegnet et digitalt gjerde på kartet. Svaret fikk vi i form av ei liste over alle mobilene som hadde vært i dette området.

4. Vi videreutvikler kartverktøy

Arbeidet med å identifisere enkeltpersoner i smaksprøven viste at vi måtte videreutvikle kartverktøyene. I Gjerdeprogrammet hadde vi ingen enkel måte å se hvilke mobiler som hadde oppholdt seg lenge innenfor områdene vi undersøkte. Det gjorde at vi i mange tilfeller identifiserte og kartla enkeltpersoner som var på besøk eller kun gikk forbi området.

Vi ville videreutvikle Gjerdeprogrammet slik at vi fikk mer informasjon om enkeltmobilene som hadde vært innenfor det digitale gjerdet. Ved for eksempel å legge til statistikk over antall dager en mobil hadde oppholdt seg innenfor området, klarte vi å sile bort mobiler som kun hadde vært innenfor området en dag. Informasjonen ble presentert i en tabell på Gjerdeprogrammets nettside.

Vi gjorde også kriteriet strengere for at et datapunkt kunne bli registrert innenfor det digitale gjerdet. Tamoco-dataene inneholdt informasjon om GPS-nøyaktigheten til hvert datapunkt.

Ved å inspisere dataene så vi at en mindre andel datapunkter hadde en usikkerhet på mer enn 200 meter. Ved å sette et krav om at datapunkt måtte ha en nøyaktighet innenfor 50 meter, fikk vi filtrert bort mange mobiler som oppholdt seg i nabobygg eller daglig passerte forbi området.

Når vi jobbet i Gjerdeprogrammet så vi at det ofte tok lang tid å finne områdene vi skulle undersøke, spesielt der journalistene ikke var lokalkjente. For å gjøre det enklere å finne privatadresser og institusjoner la vi til en søkeboks i programmets nettside. Med søkefeltet kunne vi nå skrive inn en adresse, for eksempel Bjørnstjerne Bjørnsons plass 1, og slik få Gjerdeprogrammet til å zoome inn på NRKs hovedkontor.

Disse forbedringene ble avgjørende for å forenkle det videre arbeidet. Nå ble vi mer treffsikre på hvilke mobiler vi ville undersøke.

For å komme i mål, måtte vi også videreutvikle Kepler, et gratis tilgjengelig dataprogram. Kepler var ikke helt tilpasset våre behov, og vi måtte gjøre tilpasninger.

Kepler baserte seg på kartdata fra Open Street Map (OSM). Disse var ikke helt oppdatert innenfor Norges grenser. Det førte til at vi noen ganger fikk feilaktig opplyst at en mobiltelefon oppholdt seg på steder hvor det verken var hus eller andre bygninger. Denne utfordringen løste vi ved å modifisere kildekoden til Kepler slik at programmet også kunne hente kartdata fra flyfoto-serveren til Statens Kartverk. Disse flyfotoene var mer oppdaterte. På denne måten kunne vi bytte mellom flyfoto og grafisk kart. Vi kunne nå visuelt inspisere bilder av områdene hvor kartdataene opprinnelig ikke var gode nok.

At vi hadde programmeringskompetanse i teamet var avgjørende. Slik kunne vi raskt utvikle nye verktøy og tilpasse åpne kildekodeløsninger etter behov.

Med det videreutviklede Gjerdeprogrammet, SQL-databasen og vårt tilpassede Kepler-program hadde vi nå gode verktøy. Vi kunne velge ut enkeltmobiler, følge deres reiser og slik kartlegge deler av livet til deres eier dag og natt.

Dette ble et gjennombrudd for å kunne undersøke om viktige og sentrale personer var utsatt for mobilsporing. Et av de sentrale funnene ble en stortingspolitiker.

5. Avslørt av sminkeappen

En av de første institusjonene vi undersøkte var Stortinget. Politikere som sitter tett på store beslutninger kan være mer utsatt for utpressing. Informasjon om hvor de oppholder seg kan være av stor interesse for andre. Dersom slik informasjon var tilgjengelig som salgsvare fra dataselgere - som Tamoco – var det helt klart problematisk.

Derfor gikk vi systematisk gjennom bevegelsene til mobiler som hadde vært på Stortinget. De fleste av dem viste seg å tilhøre tilfeldige privatpersoner, og noen ganger brukte vi timer på å følge opp det som viste seg å være blindspor. I et tilfelle fulgte vi en person som hadde oppholdt seg på Stortinget i over en time. Til slutt fant vi navnet på personen etter å ha undersøkt et hus i Nord-Norge. Personen var ikke politiker, men en pensjonist som sannsynligvis hadde vært på omvisning.

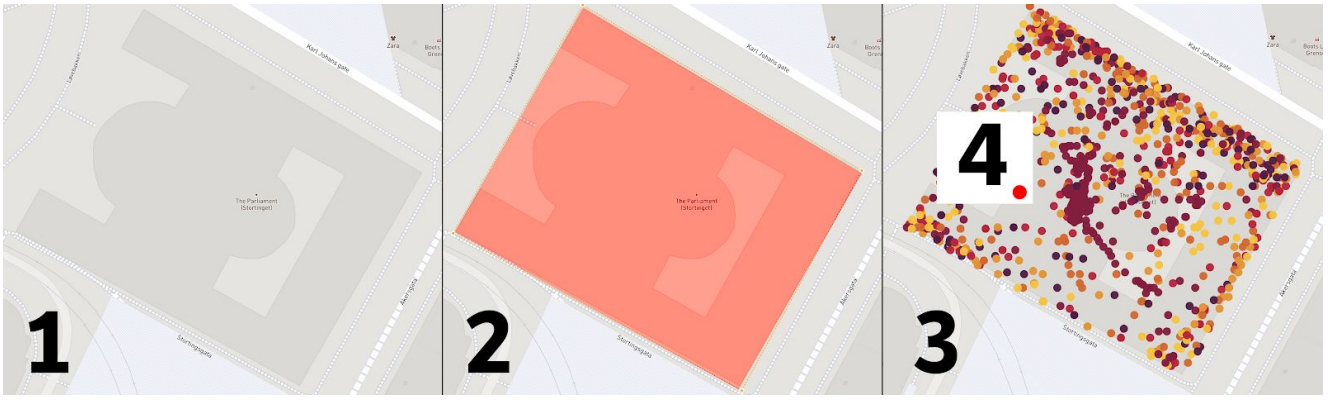
Etter at vi hadde gjennomgått de fleste mobilene hadde vi ingen fulltreffere. Vi fant ut at Stortinget også disponerer noen bygninger øst for Stortingsbygningen. Dette ble et gjennombrudd. Da vi undersøkte disse adressene dukket det opp en mobil med mange treff på et kontorbygg like i nærheten og noen få treff på Stortinget.

Vi hadde også skaffet en oversikt over adressene til flere av stortingshyblene, hvor flere stortingsrepresentanter bor. Det gjorde vi gjennom søk i Eiendomsregisteret og Stortingets egne årsrapporter. Mobilen vi undersøkte hadde også treff på en av disse adressene.

Vi følte vi var på sporet - mye tydet på at mobilen kunne tilhøre en stortingsrepresentant. Men hvem?

Da vi undersøkte bevegelsene nærmere i det digitale kartet så vi at mobilen hadde oppholdt seg flere helger og netter på en privatadresse i Larvik.

Vi søkte opp adressen i Eiendomsregisteret. Huset tilhørte høyrepolitiker Lene Westgaard-Halle, som sitter i energi- og miljøkomiteen på Stortinget.



SLIK BRUKTE VI GJERDEPROGRAMMET: ***1.*** *Slik fremstår Stortinget i det digitale kartet.* ***2.*** *Det digitale gjerdet tegnet i rødt over Stortinget.* ***3****. Hver prikk viser mobilbevegelser vi fant innenfor det digitale gjerdet.* ***4.*** *Den røde prikken ved 4-tallet viser et av stedene hvor vi sporet mobiltelefonen til stortingspolitiker Lene Westgaard-Halle (H).*

Vi la merke til at mobilen hadde lagt igjen punkter på Gardermoen - som dannet en rett linje. Det så ut som om mobilen hadde blitt sporet mens den var ombord i et fly under avgang eller landing. Sporene gikk videre ut av landet, retning sørøst. Da vi sjekket den offisielle kalenderen på Stortinget.no så vi at dataene og retningen ut av Norge sammenfalt med en komitéreise til utlandet samme dag. Westgaard-Halle var med på den aktuelle reisen.

Også ved en senere anledning hadde mobilen blitt registrert på Gardermoen, og deretter forflyttet seg til Longyearbyen på Svalbard. Da vi sjekket Westgaard-Halles instagram-profil hadde hun publisert flere bilder fra Svalbard i eksakt samme tidsrom som mobilen i datasettet hadde vært der.

Det var ikke lenger noen tvil om at vi hadde funnet en stortingspolitiker. Vi møtte Lene Westgaard-Halle til intervju på Stortinget og presenterte henne for hva vi hadde funnet. Vi lagde nettsak og TV-sak til Dagsrevyen. Hun var overrasket over hvilken app som hadde sporet henne, appnavnet stod nemlig oppført i kolonnen *app_name* i datasettet fra Tamoco.

I sin siste åpne trusselvurdering hadde PST slått fast at spionasje mot regjeringen, Stortinget og Forsvaret er blant de mest alvorlige nasjonale truslene. I saken om Westgaard-Halle uttalte PST på generelt grunnlag at det er svært viktig at myndighetspersoner er seg bevisste på hvordan de opptrer i det digitale rom, og at dette også gjelder stedsinformasjon.

Høyrepolitikeren sa at hun kanskje burde vært mer bevisst på denne typen sporing enn hun allerede var.

Kort tid etter at sakene ble publisert, sendte Stortingets administrasjon ut en felles e-post til alle stortingsrepresentanter hvor de henviste til NRKs saker og vår guide til hvordan man kan begrense sporing av mobilen sin.

Artikkelen Her avslører sminkeappen stortingspolitikerens jobbreise viste at det er mulig å identifisere, spore og kartlegge livet og gjøremålene til en sentral person i det norske demokratiet.

6. Vi sporer småbarnsfaren Karl

Mesteparten av mobilene i datasettet tilhørte ikke samfunnstopper eller maktpersoner. Vi ønsket å undersøke om, og i så fall, hvor inngripende denne overvåkingen kunne være selv for helt ordinære nordmenn.

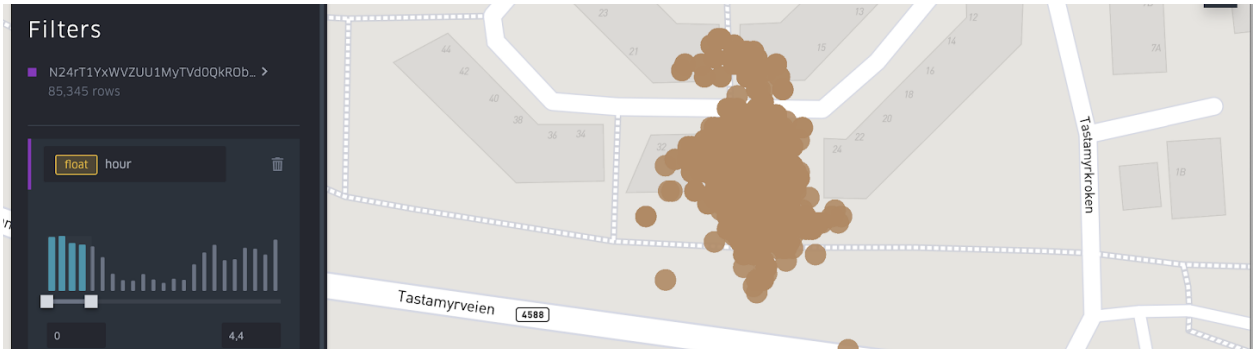
Vi regnet med at de beste kandidatene for å illustrere dette var mobileiere som hadde lagt igjen desidert mest spor. Den første SQL-spørringen vi gjorde i datasettet var å be om en liste med de 100 mobilene som hadde flest datapunkter totalt. Da vi først så listen ble vi opprømt. Det var en rekke telefoner som hadde over 100.000 datapunkter. Her måtte det være gode historier og store muligheter for å kunne identifisere eierne.

Gleden ble kortvarig. Listen var dominert av mobiler som sendte mye data under kjøreturer. Mange av disse var taxisjåfører, og mye tydet på at de hadde blitt sporet mens de kjørte bil og brukte en navigasjonsapp. Den omfattende mengden data over større geografiske områder, og til ulike tider på døgnet, vanskeliggjorde arbeidet vårt med å identifisere eierne. Vi måtte endre fremgangsmåte.

Vi stilte derfor en annen SQL-spørring: «Kan vi få en liste over mobilene som ble sporet over flest antall dager?» Ved å endre kriteriene fra antall punkter til antall dager fikk vi en liste med langt færre navigasjonsapper. Én av mobilene på listen hadde blitt sporet i mer enn 200 dager i Stavanger-området. Nesten hver eneste dag hadde den røpet bevegelsene, selv om det noen dager bare var noen få datapunkter.

Da vi skulle gjennomgå telefonens over 200 dager med bevegelsesdata, ble Kepler-funksjonen «punkt-klynger» et effektivt hjelpemiddel. Funksjonen grupperte nærliggende prikker sammen, slik at vi raskt kunne se hvilke steder mobilen hadde vært oftere enn andre. Et av disse stedene var i og rundt et rekkehus i Stavanger. Det var tre boenheter i rekkehuset, men det så ut som personen oppholdt seg i den midterste.

I vårt kartverktøy kunne vi også angi et tidsrom, for eksempel, kl. 00:00-06:00, og se hvor mobilen hadde vært i det aktuelle tidsrommet. Denne metoden brukte vi aktivt for å se hvor mobilene vi undersøkte befant seg nattestid. Hvis en mobil gjentatte ganger var på samme adresse om natten var det en sterk indikator på at det var hjemmeadressen til eieren av mobilen.



TELEFONENS BEVEGELSER OM NATTEN: *Med verktøyet Kepler.gl kunne vi isolere telefonens nattlige bevegelser. I bildet ovenfor har vi vist en avgrensning av telefonens bevegelser mellom midnatt og 04:40 på morgenen. Slik fant vi ofte eierens bosted.*

Et søk i Gule sider viste at en mann som het Karl Bjarne Rygg Bernhardsen og en kvinne bodde i rekkehuset. Vi fant Karls Facebook-profil. Der lå det offentlig informasjon om hvem han var kjæreste med. Ifølge Facebook-opplysningene var han sammen med kvinnen som også var registrert på adressen på Gule sider.

Nå var spørsmålet om mobilen tilhørte Karl eller kjæresten. Vi fortsatte å se på mobilbevegelsene og la raskt merke til to andre klynger med datapunkter. De var på forskjellige industriområder i utkanten av Stavanger, og mobilen var der på dagtid i ukedagene.

På Facebook-profilen til Karl var navnene på to arbeidsgivere offentlig tilgjengelig. Vi søkte opp firmaene i Google Maps for å sjekke hvor de hadde kontorer.

Det ble fulltreffer. Firmaenes adresser var på eksakt samme sted som mobilen hadde lagt fra seg klynger med data. Det måtte være Karls mobil.

I kartverktøyet bladde vi gjennom livet hans dag for dag. Etter hvert la vi merke til mønstre, som for eksempel at han kjørte den samme ruta til og fra jobb og omtrent når han kjørte hjemmefra om morgenen.

En dag i mai la vi merke til noe uvanlig. Ved lunsjtider kjørte han fra arbeidsplassen og til et industriområde. Det så ut til at Karl kjørte feil fordi mobilbevegelsene viste at han kjørte inn en vei, før han snudde og kjørte tilbake til en annen vei. Karl befant seg i et kontorlokale i omtrent en time før han så kjørte tilbake igjen til arbeidsplassen.

Noen uker fremover i dataene så vi et tydelig brudd i mønsteret hans. Han sluttet å kjøre den faste ruten til arbeidsplassen om morgenen og begynte å kjøre et annet sted - til industriområdet hvor han hadde vært en times tid i lunsjen i mai.

Konklusjonen var klar: Karl hadde vært på et jobbintervju og fått jobben. Mobilens bevegelser hadde også vist oss at han slet litt med å finne frem på vei til intervjuet.

Dataenes detaljnivå var forbløffende. Samtidig gjorde vi en ny oppdagelse som satte en støkk i oss.

Vi så at Karls mobil hadde vært flere dager på Stavanger universitetssykehus. Vi visste ikke hvorfor og ingenting vi kunne finne åpent i sosiale medier tilsa at han eller samboeren hadde vært syke. Det skulle vise seg at vi hadde observert en milepél i Karl og samboerens liv: Fødselen av deres første barn.

Et annet eksempel på hvor detaljerte dataene om Karl var, ble tydelig en dag han og familien besøkte Dyreparken i Kristiansand. Gjennom flere timer kunne vi se mobilens bevegelser gjennom den store fornøyelsesparken. Ingen av oss hadde inngående kunnskap om dyreparkens områder. Men Dyreparken har et svært detaljert kart besøkende kan bruke når de skal navigere seg gjennom parken. Kartet ligger åpent på Dyreparkens nettsider. Ved å bruke kartet kunne vi forstå bevegelsene hans gjennom parken på en ny måte. Vi kunne se akkurat hvilke boder han stod utenfor til gitte tidspunkt og vi kunne fastslå at like før klokken 12.00 var han i området kalt «Jungelen» og så på apekatter.

Første gang vi tok kontakt med Karl på telefon var vi usikre på hvordan han ville reagere. Han stilte seg først litt spørrende til hva vi snakket om og hvorfor vi ringte ham. Da vi forklarte at han hadde blitt sporet av mobilen sin ble han overrasket. Han hadde ingen anelse om at en app på mobilen hans kunne spore ham på denne måten. Eller at mobildataene hans var til salgs på det åpne markedet.

Han opplevde dette som invaderende, og sikkerhetsaspektet bekymret ham. Derfor gikk Karl med på å medvirke åpent, og han ble hovedcase i prosjektets første sak. Artikkelen Avslørt av mobilen traff en nerve. Den ble meget godt lest, og utløste debatt på sosiale medier om personvern og om myndighetenes manglende kontroll med dataindustrien.

7. Mobilbruk avslørte offiserer og soldater

Vi hadde nå dokumentert at mobildata kunne brukes til å avsløre folks identitet, jobbrelasjoner og familieliv. Hva med de yrkesgruppene som er avhengig av hemmelighold for å minimere risiko i yrkesutøvelsen, for eksempel politifolk og forsvarsansatte? Hvor lett kan utenlandsk etterretning kartlegge denne type personell?

Vi tegnet digitale gjerder rundt flere militærleire med vårt egenutviklede Gjerdeprogram. Slik fant vi en rekke mobiler vi undersøkte nærmere i kartverktøyet Kepler. Metoden ga hurtig resultater. Snart hadde vi identifisert en rekke soldater og offiserer. Kunne vi kartlegge dette mer systematisk?

Nasjonal Sikkerhetsmyndighets (NSM) omdiskuterte[4] kart over forbudssoner ble publisert i 2018. Det skulle forhindre droneflyvning i områder som «krever beskyttelse mot overvåkning og kartlegging av hensyn til rikets sikkerhet».[5] Kunne vi bruke kartet for å få en liste over alle mobiler som har vært innenfor områdene?

Kartet var kun tilgjengelig som et interaktivt element på NSMs nettsider, men ved å høyreklikke på artikkelen på nettsiden, og deretter klikke på menyens «Vis sidens kildekode» så vi hvilken teknisk løsning som var brukt på kartet. Det var en standard kartløsning fra produsenten ESRI ArcGIS. Ved å lese åpent tilgjengelig dokumentasjon[6] om løsningen fant vi ut at vi kunne skrive inn spesielle URL-er som ga oss rådataene bak kartet.

[4] https://www.nrk.no/norge/eksperter-kritisk-til-publisering-av-kart-med-militaere-anlegg-1.14222413
[5] https://nsm.no/fysisk/luftbarne-sensorsystemer/
[6] https://pro.arcgis.com/en/pro-app/latest/tool-reference/conversion/features-to-json.htm

Dermed fikk vi lastet ned alle forbudssonene i Norge som en geodata-fil. Denne filen gjorde det mulig å lage en SQL-spørring med oversikt over alle mobilbevegelser innenfor forbudssonene.

Resultatet ble en tabell som viste at over 7500 mobiler hadde lagt igjen 636.000 datapunkter innenfor forbudssonene. Tabellen ble et viktig arbeidsverktøy for å velge ut hvilke mobiler vi skulle undersøke nærmere. Ved å se på antall dager mobilen ble sporet, hvilke områder mobilen hadde oppholdt seg på, og hvor mange ganger mobilen hadde blitt sporet, kunne vi fokusere på de mest datarike profilene.

Tabellen ga oss også mer oversikt over mobilenes bevegelser. Ved å undersøke hvilke mobiler som hadde vært innom mange forbudssoner, kom vi på sporet av en offiser som vi fulgte bevegelsene til i 10 måneder. Etter søk i Forsvarets mediearkiv kunne vi slå fast at offiseren hadde ledet et militært utenlandsoppdrag i en krigssone. Mobilbruken viste også hvor han oppholdt seg dag og natt, hvor han reiste og hvilke militære installasjoner han oppholdt seg på i Norge.

Den systematiske jobbingen ga resultater. Offiseren ble en av hovedcasene i en reportasje om hvor enkelt det var å identifisere militært personell ved hjelp av lokasjonsdata.

	device_id	count	location_name	from_date	to_date	num_days
1	‹+6QxP4xA==	15059	Rygge flystasjon	2019-04-12	2019-07-23	26
2	6LkPcteUw==	15052	Rygge flystasjon	2019-08-12	2019-10-30	20
3	EnOpHaMQ==	13701	Bardufoss flystasjon	2019-04-23	2019-10-31	115
4	5umMdo9fA==	12403	Evenes flystasjon	2019-04-10	2019-07-02	20
5	57QFTx00A==	11065	Harstad	2019-02-27	2019-10-14	101
6	JCEDeflnA==	10426	Sola Flystasjon	2019-04-11	2019-04-20	4

FORBUDSSONER: Telefonene i tabellen ovenfor har vært innenfor militære områder. NRK har laget tabellen ved å samkjøre NSMs forbudssonekart med mobilsporingsdataene NRK kjøpte.

I de fleste tilfeller var det like enkelt å identifisere mobileierne innen forbudssonene som det hadde vært å identifisere Karl. De fleste i Forsvaret reiste hjem til adresser registrert på dem selv eller nære slektninger. Ved å gjøre søk på de registrerte navnene i Atekst, Forsvarets egne informasjonssider, nummeropplysningstjenester, og sosiale medier var det ofte mulig å bekrefte om en person hadde en tilknytning til Forsvaret.

Vi så at mange av soldatene og offiserene sto oppført i telefonkatalogen og selv skrev på Facebook om yrke eller arbeidsplass. Det var også en tendens til at yngre personer gjerne var mer aktive på Facebook og Instagram, mens de godt voksne hadde en fyldig LinkedIn-profil.

Noen mobileiere var likevel langt vanskeligere å identifisere. Det var tydelig at de hadde gjort tiltak for å minimere hvor mye informasjon de la ut om seg selv.

En av dem var en høytstående offiser i Forsvaret som hadde slettet alle sine profiler i sosiale medier. NRK klarte kun å verifisere hvem vedkommende var gjennom en LinkedIn-profil som hadde blitt slettet. Søk på personens navn i LinkedIn ga ingen treff, men da vi gjorde et Google-søk på

arbeidsplassen og navnet fikk vi et lite tekstutdrag fra det sosiale mediet. Søkegiganten hadde nemlig indeksert nettsiden på et tidligere tidspunkt, og vi kunne lese Googles oppsummering av LinkedIn-profilen. Der fant vi bekreftelsen på at vi hadde rett person i kikkerten.

Da vi ringte offiseren og la frem hva vi visste om hans bevegelser fikk vi som svar:
– Ja, jeg har vært der i fjor en gang, men du har jo datoen, tydeligvis.

Da vi markerte et digitalt gjerde rundt Rena leir kom vi over en mobil som oppholdt seg på det strengt bevoktede området til spesialstyrkene i Forsvarets spesialkommando (FSK).

FSK er en spesialavdeling som utfører hemmelige og krevende oppdrag i krigsområder. Mye om avdelingens virksomhet og personell er underlagt strengt hemmelighold. Et svært begrenset antall mennesker har adgang til leiren. Ved å følge denne mobilens bevegelser i dataprogrammet Kepler, kunne vi se at personen besøkte en privatadresse et annet sted i landet. Søk i sosiale medier ga ingen indikasjon på at personene registrert på adressen var tilknyttet Forsvaret.

Nye søk på mobilen viste at den over en periode hadde oppholdt seg utenfor det adgangsbegrensede området. Vi startet med å lese oss opp på FSK. På Forsvarets nettsider lå det ute en offentlig kalender om datoer knyttet til opptakene for å komme inn i FSK og tilstøtende avdelinger. Da vi kryssjekket datoene med mobilens bevegelser i leiren så vi at det var svært sannsynlig at personen hadde deltatt i et opptak. Vi kunne også se at personen om natten oppholdt seg på en brakke brukt under opptakene. En av journalistene i teamet hadde gjennom førstegangstjenesten fått kjennskap til hva brakken ble brukt til.

Vi undersøkte nå nærmere mobil-eierens opphold på den private adressen. Åpne kilder viste at to av familiemedlemmene i boligen aldersmessig kunne deltatt på opptaket. Vi sammenliknet aktiviteten til personene i forskjellige sosiale medier. Hadde en av dem flere offentlige venner med bilder fra militæret? Sluttet de å oppdatere sosiale medier under opptaket, eller oppholdte de seg på steder som utelukket at de kunne være i militæret? Funnene pekte mot den yngste av søsknene.

Da vi ringte personen fikk vi bekreftet at vedkommende var tilknyttet Forsvaret i Rena leir og brukte samme type mobil som den som var blitt sporet.

Samme metoder brukte vi til å kartlegge bevegelsesmønsteret til en person tilknyttet den militære Etterretningstjenesten.

Vi kunne nå publisere saken Norske offiserer og soldater avslørt av mobilen. Saken viste hvor lett det var å identifisere og kartlegge Forsvarets personell. Vi hadde flere eksempler, øverste militære grad på de omtalte var oberst. Vi brukte ikke identifiserende informasjon.

Eksperter mente NRKs funn viste hvor lett utenlandsk etterretning kan kartlegge norsk militært personell. De fryktet at slike data kan brukes til utpressing og spionasje. Forsvaret skjerpet sine mobilrutiner etter NRKs avsløring.

8. Kartlegging av mobiler på sykehus

For å undersøke hvor sensitive mobildataene var, valgte vi å undersøke om folk kunne spores mens de oppholdt seg på sykehus og krisesentre. Tidligere erfaringer med å koble mobilsporingsdata sammen med offentlige datakilder gjorde oss i stand til å utvikle en bra metode.

Karttjenesten Open Street Map (OSM) er litt som Wikipedia, et samfunn der entusiaster står for brorparten av datagrunnlaget. I vårt tilfelle var vi heldige - noen hadde manuelt lagt inn sykehus i Norges-kartet på OSM. Gjennom en maskinell dataspørring om bygningstyper,[7] kunne vi hente ut alle sykehus i Norge, og importere dem til databasen vår. Vi stusset over noen av innlastingene, det virket som at enkelte omriss av sykehus kunne være upresise.

For sikkerhets skyld inspiserte vi derfor alle sykehusområdene visuelt i kartverktøyet Qgis. Vi lastet inn filen fra OSM, og aktiverte flyfoto som bakgrunnskart. Slik kunne vi visuelt sjekke at omrisset til bygningene i OSM-filen stemte overens med de fysiske områdene til sykehusene. Slik fikk vi justert feilene.

Da dette var gjort lastet vi filen opp til databasen vår. Vi kjørte så en SQL-spørring der vi ba om en liste over antall mobil-registreringer innenfor sykehusområdene. Resultatet av denne spørringen ble en tabell som viste alle mobiltreff innenfor hvert enkelt sykehusområde. Til sammen sporet vi 8243 unike mobiltelefoner til norske sykehus.

For å lete etter adressene til krisesentre benyttet vi andre metoder. Vi fant fram til flere institusjoner som hadde skjult adresse. Vi kunne også avdekke at vi med utgangspunkt i mobildataene kjøpt fra Tamoco sporet 130 ulike mobiltelefoner til norske krisesentre i 2019.

En inngående beskrivelse av metodene kan fungere som en guide for personer som er på leting etter barn eller voksne bosatt ved krisesentre med skjult adresse. Vi forklarer derfor ikke metodene nærmere.

NRK valgte å ikke viderespore telefonene til områder utenfor sykehus, krisesentre og psykiatriske institusjoner. Besøk og oppholdt på sykehus og institusjoner er sensitive personopplysninger som krever særskilt vern.

Vi publiserte saken: 8300 mobiler sporet på sykehus og krisesentre. I ingressen skrev vi at bevegelsene til tusenvis av mobiler på norske helseinstitusjoner finnes i materialet samlet inn av et britisk firma.

Vi fortalte også at informasjonen gjør det mulig å avsløre identiteten til personer som har oppholdt seg på sykehus, psykiatriske institusjoner og krisesentre. Opplysningene skapte kraftige reaksjoner blant pasienter, pårørende, helsepersonell, i Krisesentersekreteriatet og Pasientombudet.

[7] https://overpass-turbo.eu/

9. Vi må gjenopprette brutt kontakt

Vi mente at vi hadde gjort en rekke funn som dokumenterte det potensielle skadepotensialet i Tamocos data.

I et videomøte og en e-post i mars 2020 la vi frem våre journalistiske funn for Tamoco, og vi ga uttrykk for at vi ønsket at selskapet skulle komme med sin versjon. Vi informerte også om at det ikke var riktig at vi brukte dataene i et byplanleggingsprosjekt, men at vi brukte dem i et journalistisk prosjekt om sporing av mobildata. Representanten kunne ikke svare på spørsmålene våre på stående fot, og vi ble enig om å sende en detaljert e-post. Den ble sendt samme dag. Videomøtet var siste gang vi hadde direkte kontakt med noen fra Tamoco før prosjektets første publisering.

Selskapet hadde tilsynelatende brutt kontakten. For å få Tamoco i tale sendte vi en rekke e-poster til direktører og andre ansatte. Vi ringte telefonnummeret deres fra både norsk og britisk nummer, sendte tekstmeldinger og banket på døra til forretningsadressen deres i London. Da disse forsøkene ikke førte frem, forsøkte vi å oppnå kontakt med ledelsen i Tamoco gjennom tidligere ansatte og selskapets rådgivende styre.

Etter flere uker med gjentatte forsøk på å gjenopprette kontakt, konkluderte vi med at Tamoco ikke ønsket å bidra med sin versjon. Spørsmål og informasjon sendt til e-postadresser hvor vi underveis hadde hatt fått raske svar, ble ikke lenger besvart. Retten til samtidig imøtegåelse var oppfylt etter at vi hadde lagt frem vår informasjon på videmøtet og fulgte opp med e-poster som avtalt i møtet. Vi bestemte oss for å publisere prosjektets første sak. I publiseringen var NRK åpne om at vi hadde kjøpt lokasjonsdata fra Tamoco. Vi var også åpne om at vi hadde kjøpt dataene under dekke av å bruke informasjonen til et redaksjonelt prosjekt om byplanlegging.

I saken gjorde vi det tydelig at Tamoco ikke hadde besvart våre henvendelser.

Via en britisk journalist, som hadde fulgt opp våre saker i The Times, fikk vi tak i en talsperson som hevdet at Tamoco følte seg ført bak lyset, og at det var grunnen til at de ikke hadde besvart våre henvendelser. På Tamocos vegne krevde talspersonen at selskapets svar på våre spørsmål skulle gjengis i sin helhet. De krevde også at vi lenket til Tamocos nettsider. Det ville i praksis frata oss redigeringsretten til vår egen journalistikk.

Dette førte til en ukeslang dialog for å komme i havn. Den 28. mai, over to måneder etter våre første forsøk på imøtegåelse fikk vi svar fra Tamoco, som vi kunne publisere i en nettsak. For oss hadde det hele tiden vært et mål å få Tamocos versjon av historien, og få gjennomført tilsvar og imøtegåelse. Vi oppdaterte nå vår første publisering.

Samme dag mottok vi et brev fra Tamocos juridiske avdeling og grunnleggeren av selskapet, med anmodning om å umiddelbart slette dataene vi hadde kjøpt. Dette var et prosjekt av stor samfunnsmessig betydning, og vi avslo denne anmodningen. Siden har vi ikke hørt mer fra Tamoco om mulige søksmål. Se vedlegg 2 for å lese anmodningen og vårt svar i sin helhet.

Vi hadde så langt i prosjektet vist hvordan mobildataene til 140.000 norske mobiler ble solgt til kommersielle aktører. Vi hadde avdekket hvordan dataene kan misbrukes til å kartlegge bevegelser, dagligliv og yrkesliv til vanlige folk, og til personer med utsatte stillinger i politikk og forsvar.

Men hvordan jobber selskapene i denne storindustrien som oppsto i kjølvannet av smarttelefonens inntog i 2007? Og hvordan får disse selskapene tak i våre mobildata for kjøp og videresalg?

10. Vi finner ut hvordan handelen med mobildata foregår

Arbeidet vårt med Tamoco-sakene viste at mobilappene var selve kjernen i denne delen av dataindustrien. De fleste apper som brukes til mobilsporing er gratis å laste ned for mobileieren, men det koster å utvikle og drifte dem. Derfor legger mange apputviklere inn datakoder i appene. Disse kodene sender informasjon om mobilens bevegelser til dataforhandlere i selskaper som har spesialisert seg på å motta og videreselge denne type data. Apputvikleren kan slik tjene penger på en gratis app.

For å kunne spore dataflyten trengte vi å identifisere apper som delte mobildata med bransjens dataforhandlere. I arbeidet med Tamoco-dataene hadde vi allerede fått navnene på noen av appene. Selskapet hadde med en feiltakelse lagt ved noen appnavn i datapakken vi kjøpte – dette er informasjon de normalt holder tett til brystet.

I denne næringskjeden finnes det også et lite knippe selskaper som spesialiserer seg på å analysere mobilapper. Vi spurte tre av disse selskapene om en oversikt over apper som delte lokasjonsdata med dataforhandlere. Fremstøtet lyktes – to av selskapene ga oss informasjon som gjorde at vi fant omtrent 30 nye apper.

Alle mobilapper har en personvernerklæring som sier hvilke typer personlig informasjon de samler inn og hva de bruker den til. Disse erklæringene er ofte publisert på nett og dermed indeksert av søkemotoren Google. Ved å gjøre strukturerte søk på fraser som ofte brukes i disse erklæringene, kombinert med navn på dataforhandlere, fant vi minst seks apper til.

I arbeidet med å kontakte folk vi sporet opp i Tamoco-dataene, fant vi ut at de færreste var klar over at de ble sporet og overvåket av apper på mobilen. Det var derfor viktig for oss å undersøke hvordan mobileierne ble informert av apputviklerne. Vi installerte derfor alle appene vi trodde var relevante på en Android-mobil. Mobilen ble kun brukt til vårt prosjekt. For å dokumentere hva vi gjorde tok vi skjermbilder av hvert trinn i installasjonsprosessen.

Vi kjente til at innføringen av personvernforordningen (GDPR) i 2018 ga nordmenn nye rettigheter til å be om innsyn i sine persondata. Vi bestemte oss for å prøve ut den nye innsynsmuligheten på bransjen.

I juli sendte vi 29 innsynsforespørsler til selskaper som solgte data eller som var mulige sluttkunder.

I innsynsforespørslene ba vi selskapene utlevere alle data de hadde om vår Android-mobil. Personvernforordningen ga oss også rett til å stille spørsmål om selve databehandlingen, derfor stilte vi selskapene en rekke inngående spørsmål som:

- Hvor fikk de mobildataene fra?
- Hvem delte de mobildataene med?
- Hva var deres rettslige grunnlag for å behandle dataene?

Vi møtte fort på en rekke hindringer som dro prosessen ut i tid. Ifølge GDPR har selskaper inntil 30 dager på å besvare en innsynsforespørsel. Dette var noe mange av selskapene benyttet seg av.

I flere tilfeller oppga selskapene ingen e-postadresse å kontakte dem på. Selv om adressene ikke er publisert på nettsiden, kan de likevel være i bruk. Derfor sendte vi først e-poster til adresser som typisk brukes for personvernhenvendelser. I vårt tilfelle var det privacy@firmanavn.com og DPO@firmanavn.com.

Når vi fikk beskjed om at e-posten ikke nådde frem, forsøkte vi e-postadresser for generelle henvendelser som info@firmanavn.com, hello@firmanavn.com, og support@firmanavn.com.

Dette nyttige knepet ga uttelling, slik nådde vi endelig frem til alle dataforhandlerne vi hadde på lista. Nesten alle svarte på våre henvendelser.

For å holde oversikt over det voksende antallet innsynshenvendelser ble løsningen å lage et regneark med datoer for første henvendelse, tidsfrist for svar, og hvilke e-postadresser vi hadde forsøkt.

Selv om mange svarte oss, slet vi. I starten av august hadde kun en dataforhandler oppgitt å ha data fra vår mobil. Vi fortsatte letingen.

Ved å følge med i relevante bransjenettsteder og nyhetskilder fant vi stadig flere selskaper som var aktive i lokasjonsdataindustrien. Avisen Wall Street Journal omtalte at amerikanske immigrasjonsmyndigheter (ICE) hadde kjøpt tilgang til lokasjonsdata data fra selskapet Venntel.

Kunne det være at Venntel hadde fått data fra vår Android-telefon? Vi sendte dem en GDPR-innsynsforespørsel. Dagen etter ble vi bedt om å legge ved eksempler på gateadresser mobilen hadde oppholdt seg på. Vi ettersendte den nye informasjonen. Nesten en måned senere fikk vi et svar som viste at vi var på rett spor.

Venntel hadde over 75.000 ganger fått vite den presise posisjonen til vår Android-mobil. Venntel bekreftet også at de hadde delt mobildata fra vår mobil med kunder, men nektet i sitt innsynssvar å gi oss navnet på dem. Selskapet ville heller ikke oppgi akkurat hvilke formål kundene kunne bruke dataen til.

I innsynssvaret fra Venntel fant vi også en referanse til noe som kunne være et appnavn. Et enkelt søk på navnet viste at det dreide seg om appen Funny Weather. Det var en av appene som vi hadde installert på Android-telefonen vår. Kunne dette være appen som røpte bevegelsene til mobilen vår?

Vi ville kartlegge mer av ferden til mobildataene våre. I svaret fra Venntel fant vi en annen interessant ledetråd. De hevdet at dataene kom fra morselskapet Gravy Analytics. Vi sendte en innsynsforespørsel til selskapet. De oppga å ha mottatt informasjon fra to selskaper, Predicio og Complementics.

Gjennom nye GDPR-innsynsforespørsler fikk vi vite at disse selskapene mottok data fra en polsk apputgiver kalt Sygic.

Vi kunne nå følge mobildataene fra vår mobil, trinn for trinn:

- Vi installerte den slovakiske navigasjonsappen Sygic på mobilen vår.
- Navigasjonsappen sporet mobilens bevegelser.
- Appen videresendte sporingsdataene til dataforhandleren Predicio i Frankrike.
- Predicio videresolgte dataene til Gravy Analytics i USA.
- Gravy Analytics delte mobildataene med underselskapet Venntel.
- Venntel delte deretter våre mobildata med sine kunder.

Venntel nekter å oppgi til oss hvem disse kundene er. Offentlige dokumenter viser at Venntel har amerikanske myndigheter på kundelisten, blant andre ICE (immigrasjonsmyndighetene) og Customs and Border Protection (toll- og grensemyndighetene). Venntel nekter for å delt våre mobildata med disse kundene.

For hundretusener av nordmenn foregår denne handelen og transporten med sporingsdata fra deres mobiler uten at de er klar over det eller forstår hva de har samtykket til. De har heller ikke den minste kontroll på hvilke selskaper som mottar deres mobildata og hva selskapene bruker den til.

Metodene vi brukte i denne kartleggingen er ikke tidligere blitt brukt til å systematisk dokumentere hvordan bransjen opererer. Vi avdekket også at apputviklerne Sygic og Funny Weather ikke selv visste hvor dataene endte opp.

Vi tok skjermbilder da vi installerte mobilappen Sygic på mobilen vår. Dermed hadde vi dokumentasjon på hva appen egentlig hadde bedt oss samtykke til – å dele våre mobildata til markedsføringsformål.

Likevel vet vi gjennom våre innsyn at mobildataene havnet hos Venntel, som ikke driver med markedsføring. Her mener tre uavhengige jurister at Sygic trolig har begått et brudd på GDPR når de likevel delte informasjonen med Venntel.

Vi publisere funnene våre om dataforhandlere og mobildataflyt i artikkelen Telefonen spionerte på meg. Slik fant jeg overvåkerne. Avsløringen ble sitert internasjonalt i en rekke medier og på flere språk. Slovakisk datatilsyn åpnet en granskning av dataflyten til Venntel som en følge av NRKs saker.

Spesielle erfaringer

1. Datasikkerhet

Det ble tidlig klart for oss at den meget omfattende datapakken fra Tamoco inneholdt sensitiv informasjon om et stort antall personer. I vårt redaksjonelle arbeid var det derfor viktig å lagre dataene sikkert. Vi valgte å lagre alle data lokalt på en maskin i redaksjonens lokaler. Det ble i tillegg gjennomført en rekke sikkerhetstiltak på selve maskinen[8], harddisken ble kryptert, og tilgang til hele

[8] https://madaidans-insecurities.github.io/guides/linux-hardening.html

databasen ble begrenset til én person. Maskinen ble også frakoblet NRKs interne nettverk like etter publisering, for å gjøre det vanskelig for uvedkommende å få tilgang til data.

2. Justering av kart

Nettsaker og tv-reportasjer ble illustrert med kartgrafikk hvor vi viste punktene til et tusentalls telefoner. Sakene handlet om at nordmenn kompromitterte sitt personvern uten å være klar over det. Ville disse illustrasjonene bidra til at *vi* kompromitterte intetanende nordmenns bevegelser? Hvis vi skulle bruke dataene til mennesker vi ikke hadde fått samtykke fra, måtte de anonymiseres. Løsningen ble å lage en kopi av databasen vår, og legge til tilfeldig støy på de geografiske koordinatene. Det førte til at en prikk som egentlig var registrert på et bolighus, ble flyttet et godt stykke unna. Slik unngikk vi å vise så eksakte bevegelser og oppholdssteder at de kunne brukes til å spore opp uidentifiserte mennesker i datasettet vårt.

3. Anonymisering

I artiklene valgte vi ikke å identifisere soldater og offiserer og heller ikke publisere informasjon som kunne bidra til å identifisere dem. Det var systemet og dets omfang og sårbarhet som var det sentrale for oss – ikke handlingene til den enkelte soldat eller offiser, som ga fra seg bevegelsesdata gjennom normal bruk av mobiltelefonen.

4. Skjult identitet

I startfasen forsøkte vi en framgangsmåte som ikke endte i publisering, men som vi likevel vil nevne. Relativt få av de omlag 30 dataforhandlerne vi kontaktet svarte på henvendelsen fra NRK. Ville de svart annerledes dersom det ikke var NRK, men et kommersielt selskap som tok kontakt med dem? I samråd med redaktører opprettet vi et fiktivt selskap. Vi kontaktet de samme 30 dataforhandlerne, men denne gangen under dekke av å være dette selskapet. Kun ett av selskapene svarte annerledes på henvendelsen nå enn da vi kontaktet dem som NRK, og vi skrinla hypotesen og framgangsmåten.

5. Dataforhandler navngis

Før publisering av første sak gjorde vi grundige juridiske og publisistiske vurderinger rundt kontrakten vi hadde inngått med Tamoco. Kunne vi risikere at NRK pådro seg et erstatningsansvar under britisk jurisdiksjon? NRK konkluderte med at det var av stor allmenn og journalistisk interesse å avdekke hvordan data fra titusener av norske mobiler ble samlet inn og omsatt. Disse hensynene ble også førende for at vi valgte å navngi Tamoco, selskapet vi hadde kjøpt dataene fra.

Konsekvenser

- Forsvaret har etter NRKs mobilsporingssaker sendt ut nye retningslinjer for bruk av sosiale medier til sine ansatte. Her beskrives blant annet hvordan apper kan spore mobilbrukerens bevegelser.

- Datatilsynet startet granskning av Tamoco etter NRKs saker. Granskningen pågår fortsatt og skjer i samarbeid med det britiske datatilsynet, ICO.

- Det slovakiske datatilsynet har åpnet en uavhengig granskning for å avdekke hvordan det slovakiske selskapet Sygic samarbeidet med det amerikanske selskapet Venntel. Granskningen pågår fortsatt.

- Distrikts- og digitaliseringsminister Linda Hofstad Helleland kalte avsløringen «dypt urovekkende», og følger opp saken på ministernivå i EU.

- Mobilsporingssakene skapte stort engasjement i sosiale medier, og ble omtalt av Danmarks radio og den engelske avisen The Times. NRK-saker ble også omtalt i Hacker News, et av verdens største forum for IT.

- Som en del av prosjektet utarbeidet vi også en guide til leserne om hvordan de med konkrete grep kunne begrense sporing av sin egen mobil. Denne saken ble lest av nærmere en halv million og var en av sakene som skapte størst engasjement i sosiale medier.

Vedlegg

Vedlegg 1: Fullstendig liste over publisering

Publisert fra 9. mai 2020. Arbeidet fortsetter inn i 2021.

Nettsaker:

- Avslørt av mobilen (9. mai 2020)
- Guide: Slik begrenser du sporing av din mobil (9. mai 2020)
- Datatilsynet opnar gransking etter mobilsporing (10. mai 2020)
- 8300 mobiler sporet på sykehus og krisesentre (11. mai 2020)
- Ber to norske selskaper stanse datainnsamling (12. mai 2020)
- Smittestopp samler inn samme type data som i NRK-avsløring (13. mai 2020)
- Norske offiserer og soldater avslørt av mobilen (18. mai 2020)
- Britisk datatilsyn starter undersøkelser etter NRK-avsløring (27. mai 2020)
- Venstre-leder skremt: – Vi er ikke i stand til å sikre våre egne (28. mai 2020)
- Digitaliseringsministeren om mobilavsløring: – Dypt urovekkende (20. mai 2020)
- Her avslører sminkeappen stortingspolitikerens jobbreise (1. juni 2020)
- Britisk dataselger varsler intern gransking etter NRK-avsløring (3. juni 2020)
- Secret Service kjøpte data om amerikanske mobilers bevegelser (24. august 2020)
- Telefonen spionerte på meg. Slik fant jeg overvåkerne (3. desember 2020)
- Reagerer på amerikansk overvåkning: – Sjokkerende (7. desember 2020) – PDF
- Europeisk datatilsyn åpner granskning etter NRKbeta-avsløring (11. desember 2020)

TV-innslag:

- Hovedsak i Dagsreveyn – Forbrukerrådet reagerer på salg av mobildata (9. Mai 2020)
- Dagsrevyen hovedsak – Leder i Justiskomitéen krever svar fra tre statsråder (10. mai 2020) Digitaliseringsministeren ble intervjuet direkte i studio
- Hovedsak i Dagsrevyen - Så lett kunne NRK spore norske offiserer og soldater (18. mai 2020)
- Sak i Dagsrevyen - Leder av forsvarskomitéen krever klarere retningslinjer for forsvarsansatte (18.mai 2020)
- Sak i Dagsrevyen - Høyrepolitiker avslørt av sminkeapp (1. juni 2020)
- Sak i Dagsrevyen 21 - Tamoco varsler intern granskning - hevder de ikke har gjort noe galt (3. juni 2020)

Radio-innslag:

- Nyhetsmorgen – Krisesenter- og sykehusbesøk kan kartlegges (11. mai 2020)
- Debatt i Dax18 - Kritisk til salg av stedsinformasjon (12. mai 2020)
- Oppdatert – Avslørt av mobilen (15. mai 2020)

Vedlegg 2: NRKs svar på juridisk henvendelse fra Tamoco

For Sam Amrani, director of Tamoco,

The data licensed to Norwegian Broadcasting Corporation (NRK) from Tamoco is currently being used for research and documentation purposes in an editorial process.

In the email requesting the deletion of the licensed data, you substantiate that request on the fact that the data has been used for purposes outside of the intended use case.

Neither the Statement of Work nor the NDA dictates the explicit use cases in which NRK may use the data.

As a publicly funded broadcaster it is our mandate to raise a debate around matters concerning potential breaches of laws and regulation. There has been a profound interest in this specific story from politicians, several European data protection agencies and the public as a whole.

Part five of the Statement of Work defines that Tamoco has sole responsibility for the legality of the licensed data. It is the view of NRK that there is reason to question the legality of said data, how it has been collected and the process of selling raw location data.

It is therefore NRK's view that this data is important for research and documentation purposes and NRK will not comply with your request.

NRK follows the ethical guidelines of the Norwegian press and relevant GDPR regulations. Under no circumstances have NRK shown the raw data purchased from Tamoco to anyone outside our editorial staff. The articles published by NRK uses illustrations and graphics based on the data, and geographical coordinates have been altered to preserve the privacy of the individuals whom the data is collected from.

We believe that this data is regarded as personal information according to General Data Protection Regulation (GDPR) regulations. For journalistic purposes, NRK’s storage and processing of personal information is backed by Article 85.2 of the GDPR. NRK will destruct the data when the editorial purpose of said data is fulfilled.