

Hva vet de om deg?

Bruk av innsynsretten hos fire virksomheter
Mars 2018

Innhold

OM PROSJEKTET OG INNSYNSRETTE	4
DETTE VET DE FIRE VIRKSOMHETENE OM OSS	5
TV-EN DIN SER DEG	6
MEDIA FØLGER DEG PÅ TVERS AV NETTSIDER	8
NOEN VET HVA DU LEGGER I HANDLEKURVEN	10
TELEDATA	12
HVA NÅ?	14

Om prosjektet og innsynsretten

Vi legger alle igjen elektroniske spor – kanskje flere enn vi har tenkt over. Hva du gjør på nett, ser på TV, liker på Facebook og legger i handlekurven, registreres. Dataene lever videre – og noen ganger kan dataene avsløre mer enn man kanskje tror.

Mange virksomheter ønsker å samle inn flest mulig personopplysninger fordi de har en økonomisk verdi:

- Når virksomheter vet mye om oss, kan de tilpasse reklame, tjenester eller priser deretter.
- Mange virksomheter selger personprofilene våre til markedsførere.
- Personopplysninger kan brukes til å analysere hvordan kunder bruker en tjeneste. Dette kan brukes til å forbedre tjenesten.
- Personopplysninger om oss kan brukes til å utvikle datamodeller. Datamodeller kan blant annet brukes til å utvikle nye tjenester eller bli bedre på å profilere oss.

Virksomhetene har plikt til å gi informasjon om hvilke personopplysninger de behandler og hva de skal brukes til, men ofte er denne informasjonen begravd i lange og tunge personvernerklæringer eller tjenestevilkår.

Gjennom å be om *innsyn* kan du finne ut hva virksomhetene faktisk vet om deg. I denne rapporten

blir det sett nærmere på hva noen utvalgte virksomheter lagrer om sine kunder.

Hvordan har vi gått frem?

Datatilsynet har to roller: tilsynsorgan og ombud. I denne rapporten opptrer Datatilsynet som ombud. Det vil si at det ikke er utført tilsyn med eller kontroll av virksomhetene. Det er ikke tatt stilling til lovligheten. I stedet har to ansatte i Datatilsynet (heretter kalt testpersoner) brukt innsynsretten sin som privatpersoner, og resultatene omtales i denne rapporten.

Når testpersonene tok kontakt med virksomhetene, ble Datatilsynets brevark brukt for å være åpne om hvem vi er. Det ble også informert om at funnene ville kunne brukes i Datatilsynets arbeid. Det ble likevel understreket at testpersonene har brukt sin innsynsrett som privatpersoner og at innsynsbegjæringen ikke er å forstå som en kontroll fra Datatilsynets side.

For ordens skyld gjør vi oppmerksom på at Telenor Norge AS svarte på innsynsbegjæringen under forutsetning av at det ikke var snakk om tilsyn eller en formell henvendelse fra Datatilsynet.

Innsynsbegjæringene ble sendt første halvdel av 2017. Vi tar forbehold om at virksomhetene kan ha endret måten de behandler personopplysninger på siden den tid.

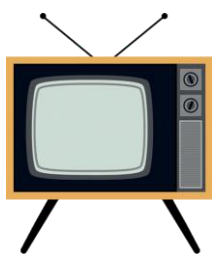
§ Innsynsretten

Personopplysningsloven sier at du kan henvende deg til norske virksomheter og offentlige organer for å få se hvilke opplysninger de har lagret om deg. Dette gjelder også opplysninger som bare *indirekte* kan kobles til deg. Du kan for eksempel få vite hvilket kundesegment du er plassert i eller hvor ofte posisjonen din lagres.

Du har også rett til å få vite hva formålet med opplysningene er, hvor de er hentet fra og hvem de eventuelt skal utleveres til.

Ønsker du å be om innsyn i dine personopplysninger? Du finner en mal du kan bruke på www.datatilsynet.no/innsyn.

Dette vet de fire virksomhetene om deg



Hva du ser på TV



Hvor du har vært



Hvilke nyhetsartikler du leser og
hva du kjøper og selger på finn.no



Hva slags utdanning du har



Inntekt og formue



Hvem du ringer og tekster
og når du bruker mobilen



Hva du legger i handlevogna –
dette kan igjen si noe om helsen din

TV-en din ser deg

Den første virksomheten det ble bedt om innsyn hos, var Canal Digital Kabel (formelt en del av Telenor Norge AS).

De tilsendte opplysningene viser for det første at Canal Digital lager en profil av kundene sine. Profilen til testpersonen inneholder antagelser om personens inntekt, hvor mange barn vedkommende har og hvilken utdannelse personen har gjennomført.

For det andre viser det seg at Canal Digital lagrer hva kundene har sett på TV.

Hver gang testpersonen har brukt TV-boksen til å starte programmer forfra, har sett på programmer fra ukesarkivet eller leid film, blir det laget en oversikt over hvilke programmer det er sett på, når de ble sett og hvor lenge. I testpersonens tilfelle gikk denne oversikten tilbake til oktober 2015 og inneholdt 281 setteprogrammer.

Hvorfor har Canal Digital disse opplysningene?

Testpersonen valgte å sende Canal Digital noen oppfølgingsspørsmål: Hvor henter virksomheten opplysningene om livssituasjonen hans fra? Hvor lagres personens TV-vaner?

Canal Digital svarte at vurderingene av testpersonens livssituasjon, for eksempel hva personen tjener og hvor mange barn han har, er hentet fra Bring. Opplysningene brukes til segmentering av kundemassen, og formålet er å tilpasse dialogen med kundene.

Når det gjelder formålet med å lagre hva brukeren ser på, viser Canal Digital til sine vilkår. Der står det at de vil bruke dataene til å sikre god kvalitet på tjenestene, gi relevant informasjon om produkter, samt å yte kundeservice. Canal Digital understreker at de mener dette er noe testpersonen har samtykket til på TV-skjermen når TV-boksen ble tatt i bruk.



Hvem er testpersonen?

Ifølge Canal Digital har personen som ba om innsyn «560» (560 000 kroner?) i inntekt, «330» i formue, bor i blokk, har humanistisk utdannelse fra universitet og er en enslig mann uten barn.

Ikke alle av disse gjetningene treffer like godt, men helhetsinntrykket stemmer likevel godt overens med virkeligheten.

Canal Digital har videre lagret at testpersonen har sett mye på *Keeping Up with the Kardashians* på TV2 Bliss. Det er kanskje noe ikke alle ønsker å dele med andre?



Gyldig samtykke

Et samtykke skal være frivillig, informert og uttrykkelig. Det betyr blant annet at du skal få tydelig informasjon om hva du samtykker til og at du skal kunne si nei uten negative konsekvenser, slik som for eksempel å bli utestengt fra en tjeneste.



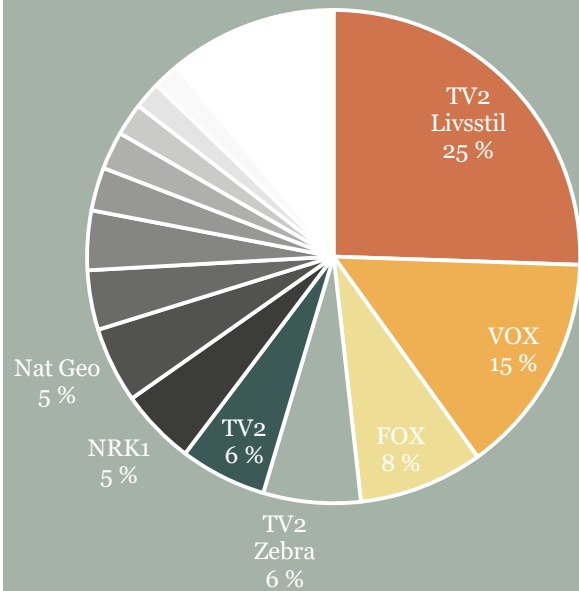
Testpersonens mest sette TV-programmer

1. Keeping Up with the Kardashians
2. The Good Wife
3. Alaska siste utpost
4. Ødemarkens menn
5. Mord og mysterier

Testpersonen har også sett mye på serier om interiør og veterinærer.



Testpersonens mest sette TV-kanaler



Media følger deg på tvers av nettsider

Schibsted eier mange av de mest leste avisene i Norge slik som Aftenposten og VG, samt tjenester som finn.no, prisjakt.no, lendo.no og letsdeal.no.

Schibsted har i alle fall lagret følgende opplysninger om testpersonen:

- hvilke nyhetsartikler han har lest
- når han leste dem
- hvor langt ned på siden han har bladd
- hva han har søkt etter på finn.no (noen ganger virker det som om alt testpersonen har skrevet inn i søkefeltet har blitt registrert selv om han ikke har trykket Enter)
- korrespondanse med andre på finn.no
- hvor han har befunnet seg
- teknisk informasjon om mobiltelefonen og datamaskinen hans
- IP-adressene hans
- hvilke interesser han sannsynligvis har
- kontaktinformasjon og opplysninger om abonnementet hans

Opplysningene var fordelt på svært mange Excel-dokumenter som det tok lang tid å tolke.

Schibsted lagrer opplysninger om både abonnenter og ikke-abonnenter. Dersom man er betalende abonnent, er det imidlertid mye lettere å knytte opplysningene til navne og adresse. Testpersonen som ba om innsyn er abonnent.

Med mindre man bruker spesialprogramvare for å beskytte seg, er det ikke mulig å lese nyhetsartikler på Aftenposten.no eller kjøpe bruktmøbler på finn.no uten at elektroniske spor lagres.

Schibsted bruker en påloggingsløsning som heter SPiD og som brukes på nettavisene og finn.no. I personvernerklæringen til SPiD står det at personopplysninger kan deles mellom de ulike

Schibsted-virksomhetene. Opplysningene kan også bli overført til land utenfor EU-/EØS-området. Formålene med å samle inn personopplysningene er blant annet å selge dem til markedsførere som kjøper annonseplass.

Schibsted har også eksperimentert med å tilpasse og personalisere hvilke nyhetsartikler som dukker opp hos brukerne, men Datatilsynet kjenner ikke til om Schibsted fortsatt gjør dette.

Det er trolig svært vanlig at nettaviser samler inn mange opplysninger om leserne sine.



Store datamengder

Datamaterialet som ble tilsendt fra Schibsted etter at det ble bedt om innsyn, inneholdt over **7 millioner datapunkter** (målt i antall Excel-celler). Datamaterialet viser at testpersonen sannsynligvis har interagert med Schibsted-sider over 400 000 ganger.

Disse dataene kan kombineres og aggregeres. Hvilke artikler vi leser og hva vi gjør på finn.no kan for eksempel si noe om:

- Hva som engasjerer oss
- Hva vi liker
- Hvordan vi skriver
- Livssituasjonen vår
- Livsstilen vår
- Konsentrasjonsevnen vår

Datasettene til Schibsted kan derfor gi et rikt og helhetlig bilde av hvem den enkelte er.

Maskinlæring og kunstig intelligens vil trolig også kunne avdekke skjulte sammenhenger og åpne for nye bruksområder.



Hvem er testpersonen?

Datamaterialet fra Schibsted ga detaljert informasjon om testpersonen:

- Han har sett mye på boligannonser i Oppegård og Ski.
- Likevel har han lest mange Oslo-relaterte artikler på aftenposten.no.
- Han har søkt etter barnevogn på finn.no. Er det familieforøkelse på gang?
- Han leste en stillingsannonse på finn.no på en Samsung-mobil den 8. september 2015 klokken halv ti om morgenen. (Vi håper selvsagt at vedkommende ikke planlegger å bytte jobb.)
- Vi kan se hvor ofte testpersonen bommer på tastene når han skriver inn søkeord på finn.no.
- Han brukte bare 53 sekunder på å lese en artikkel om hvorfor man bør dusje rett etter trening. Til sammenlikning brukte han 10 minutter og 43 sekunder på en artikkel om Magnus Carlsen.
- Han var våken og leste nyheter klokka 06.06 den 8. november 2016. Han var fremdeles våken klokka 22.23.
- Søndag 26. juli 2015 var han i Strømstad. (Lurer på hva han gjorde der?)



Tilpasset reklame i mediebransjen

Gratis tjenester på nett er ofte ikke gratis. Prisen er våre personopplysninger.

Nettavisene samler inn store mengder informasjon om brukerne. Denne informasjonen tilbyr de til annonsørene slik at de kan målrette reklamen sin.

Det er for eksempel vanlig at nettaviser profilerer leserne sine basert på blant annet hvilke nyhetsartikler de leser, hvilket utstyr de bruker og hvor de er når de leser artiklene. Den tilpassede reklamen vises i annonseplassene på nettavisene.

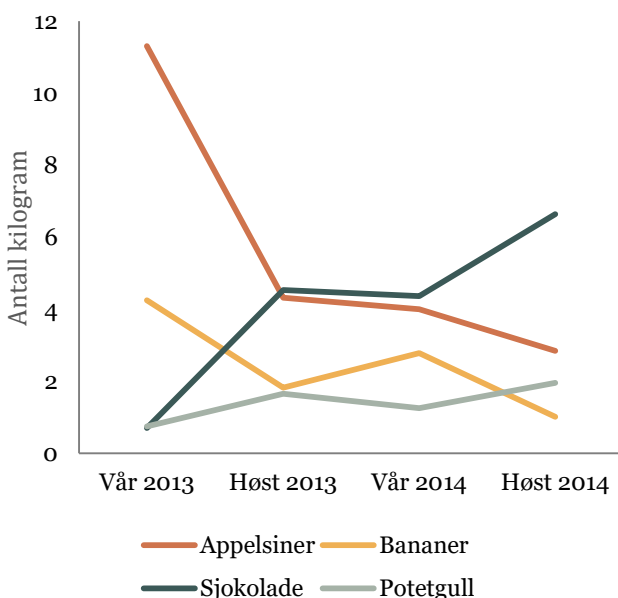
Noen vet hva du legger i handlekurven

Den neste virksomheten det ble bedt om innsyn hos, var Trumf. Trumf er et fordelsprogram tilknyttet NorgesGruppen, som står bak dagligvarekjedene Kiwi, Meny, Spar og Joker. Oversikten fra Trumf viste hva testpersonen hadde kjøpt på 396 handleturer de siste fem årene.

Dersom du bruker Trumf-kortet eller har registrert bankkortet ditt hos Trumf, registrerer virksomheten alle kjøp du gjør hos NorgesGruppens butikker. Det vil si at når og hvor du handler, samt hvert eneste produkt du har kjøpt, lagres i fem år (på grunn av bokføringsplikten).

Hvilke matvarer du legger i handlekurven sier noe om kostholdet ditt og dermed også helsa di. Videre kan valg av matvarer noen ganger si noe om religion. Kjøp av tobakks- og alkoholprodukter, kondomer og smertestillende tabletter kan også avsløre sensitive forhold. Heldigvis bruker ikke Trumf sine data til å avdekke helseforhold eller religion. Det er likevel viktig å være oppmerksom på at dette er personopplysninger som sier mye om deg. Slike personopplysninger bør bare deles med virksomheter man stoler på.

Ved å se nærmere på hvordan testpersonens forbruk av appelsiner og bananer har utviklet seg i forhold til forbruket av sjokolade og potetgull, kan man se visse trender:



Grafene i diagrammet viser forbruk av disse matvarene fra 2013 til 2014, målt i kilogram. Ut fra diagrammet kan det se ut til at testpersonens kosthold er i endring. Hva sier dette om vedkommendes helsesituasjon?

Profilering og tilpassede tilbud

Hos Trumf kan man velge å få tilpasset informasjon, tilbud og kuponger. Det betyr at man for eksempel får gratis kuponger på varer som man sannsynligvis er interessert i, i stedet for å få kupong på en tilfeldig vare. Trumf analyserer kjøpshistorikken for å regne seg frem til hvilke varer du sannsynligvis er interessert i.

For noen vil det være helt greit at Trumf analyserer deres handlemønstre, for eksempel fordi de ønsker mer relevante tilbudskuponger. Andre vil synes at dette er ubehagelig.

Det bør være opp til hver enkelt å bestemme om man ønsker slik personalisering. Datatilsynet har tatt dette opp med Trumf, og Trumf har vært lydhør.

Virksomheten har innført nye løsninger slik at kundene kan velge selv. Nye medlemmer må aktivt samtykke til tilpassede tilbud og analyse. Eksisterende medlemmer kan reservere seg mot analyse. På denne måten varetas personvernet.

Noen fordelsprogrammer har samme løsning som Trumf. Andre fordelsprogrammer gir imidlertid ikke den enkelte mulighet til å velge.

Da testpersonen ba om innsyn hos Trumf, kom det frem at han var blitt plassert i bestemte segmenter.

Segmentene Trumf hadde brukt var:

- De kvalitetsbevisste
- Enkelt og raskt
- Hjemmelaget er best
- Kiosk og småhandel
- Moderne familier
- Prisbevisste familier
- Tradisjonell husmannskost

Datatilsynet vet at Trumf har gjort endringer i måten de behandler personopplysninger på, så det er ikke sikkert

at Trumf fremdeles bruker disse segmentene. Likevel finnes det mange andre virksomheter som bruker denne typer segmenter.

Personvern for familiemedlemmer

Trumf-medlemmer i samme husstand har mulighet til å spare bonus sammen. Da testpersonen ba om innsyn hos Trumf ble det samtidig gitt innsyn i alle varekjøpene til det andre husstandsmedlemmet, slik som hvor og når vedkommende har handlet de siste fem årene.

Det er ikke vanskelig å tenke seg at denne muligheten misbrukes. Overivrige foreldre kan sjekke hvor tenåringer *egentlig* henger. Tilsvarende kan kontrollerende ektefeller overvåke sine familiemedlemmer på en lite legitim måte.

Retten til privatliv er en menneskerett. Det vil si at også ektefeller og barn har personvern innad i familien.



Data kan si mye

Hvilket segment du plasseres i hos en virksomhet kan si mer enn bare hvilke produkter du er interessert i. Dersom du for eksempel blir plassert i segmentet «Prisbevisste familier», kan det antyde at du kanskje ikke har like god råd som «De kvalitetsbevisste».

Et forsikringselskap som tilbyr helseforsikring kan være mer interessert i kunder fra «Hjemmelaget er best» enn «Enkelt og raskt» – i dette tilfellet kan segmentene antyde noe om hvor sunt du spiser.

Teledata

De fleste vet nok at teleselskapene lagrer mange opplysninger om sine brukere, men kanskje ikke at teleselskapene lagrer data hver gang man aktivt bruker telefonen sin.

Da testpersonen hos Datatilsynet ba om innsyn i opplysningene sine hos Chess (formelt Telia Norge AS), fikk han en oversikt som viste all kommunikasjon og mobildatabruk tre måneder tilbake i tid. Oversikten inneholdt opplysninger om:

- geografisk posisjon (lokasjonsdata),
- når telefonen hadde vært brukt,
- hvilke telefonnumre det var ringt og sendt SMS til,
- hvem som hadde ringt eller sendt SMS til ham,
- hvor lenge telefonsamtalene varte,
- hvor mye mobildata som var brukt,
- hva slags mobiltelefon det gjaldt, og
- telefonens IMSI-nummer (et ID-nummer som brukes til å unikt identifisere telefonen i nettverket).

I Chess' personvernerklæring skriver virksomheten at den også lagrer IP-adresser. Det ble ikke gitt innsyn i disse den første gangen, og derfor sendte testpersonen et oppfølgingsbrev for å få tilgang til også disse opplysningene.

Metadata

Opplysningene som teleoperatørene sitter på, er en form for *metadata* (data om dataene), for eksempel hvor man var når man brukte en tjeneste, hvem man snakket med eller hvilket utstyr man brukte.

Moderne etterretningstjenester er stadig mer opptatt av metadata fordi analyse av slike tilsynelatende uskyldige opplysninger kan si mye om den enkelte. At man har ringt hjelpelinjen for spilleavhengige eller senter for seksuelt misbrukte menn *kan* for eksempel si vel så mye som innholdet i selve samtalen. Når man i tillegg vet

IP-adresser

Alle enheter som er tilkoblet internett må ha en IP-adresse for å fungere. IP-adressen er enhetens ID.

Det er vanlig at nettstedet logger IP-adressene til de besøkende. IP-adressen kan altså potensielt avsløre hvem som har sett og gjort hva på en nettside. Teleselskaper og nettilbydere har imidlertid taushetsplikt om IP-adresser, så derfor er det vanskelig å vite hvem som skjuler seg bak en IP-adresse.

Som hovedregel fornyes IP-adresser ofte og regelmessig av teleoperatøren eller nettilbyderen.

hvor personen var når vedkommende ringte og hvem man ringte før og etterpå, kan man få et enda rikere inntrykk av en persons situasjon.

Metadata genereres automatisk når man bruker digitale tjenester, og siden de fleste bruker slike tjenester i stadig større grad, lagres det mer og mer metadata om den enkelte.

Forskere ved Massachusetts Institute of Technology (MIT) og Université Catholique de Louvain i Belgia har vist at lokasjonsdataene til en person er unike og at det ikke skal så mye til for å skille oss fra hverandre. For 95 % av befolkningen er fire oppføringer av når en person var hvor, unikt for den personen. Med andre ord er fire oppføringer av lokasjonsdata nok til å lage et unikt metadata-avtrykk for de fleste av oss. Til sammenlikning kreves det 12 punkter på fingeren for å lage et unikt fingeravtrykk.

Det er forskjeller mellom hvor lenge de ulike teleoperatørene lagrer teledata. Teledata kan dessuten havne på avveier.

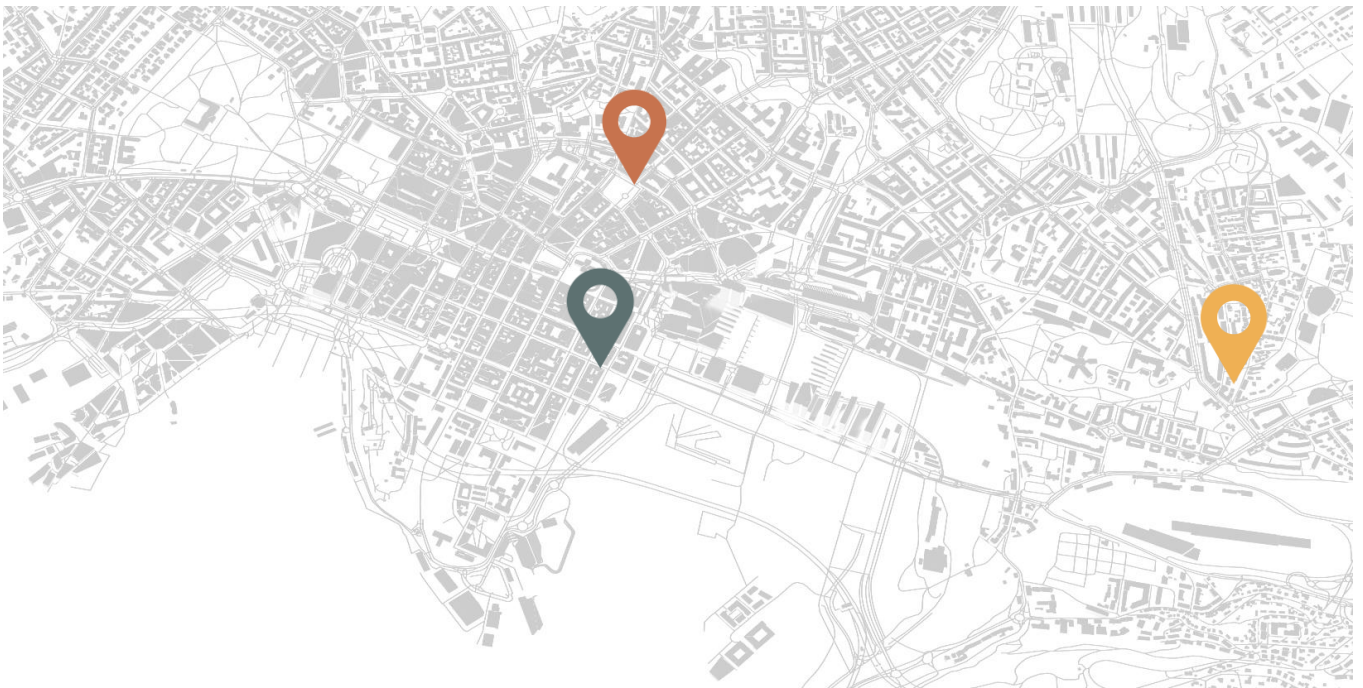


En av verdens mest berømte hackere om teledata

Kevin Mitnick skriver om hvordan teledata kan havne på avveier og misbrukes i boken «The Art of Invisibility».

I 2014 ble det oppdaget at telenettet kan hackes ved hjelp av en svakhet i noe som heter Signaling System 7. Svakheten innebar at det var mulig å avlytte telefonsamtaler og se hvor mobilbrukere befant seg. Mitnick skriver også om hvordan Hellas' telenett ble avlyttet av hackere i 2004 – og vi vet fortsatt ikke hvem som sto bak. Forfatteren peker også på at krypteringen som sikret 2G-nettet (forløperen til 3G og 4G – og fortsatt i bruk) etter hvert ble knekt. Dette illustrerer at ingenting er sikkert, heller ikke når det gjelder teledata.

Selv klarte Mitnick å skaffe seg tilgang til telelogger hos et teleselskap. Mitnick ville se hvilke telefonnumre som ringte til en FBI-informant. Ved å følge med på disse telefonnumrenes ringemønstre, klarte han også å spore opp informanten hver gang han ble flyttet til en ny lokasjon og fikk et nytt telefonnummer.



Ved å se på teledataene til testpersonen kan man få detaljert kunnskap om ham og hans livsstil:

- Ved å se på hvor han vanligvis er på dagtid på hverdager, kan man skjønne hvor han jobber (grønn markør).
- Den gule markøren viser det siste stedet vedkommende er om kvelden og det første stedet han er om morgenen – det er rimelig å anta at det er her han bor.
- Sjekker man nærmere, kan man også skjønne hvilket fremkomstmiddel han bruker til jobb.
- Dataene avslører videre om vedkommende står opp tidlig, jobber sent, er mye på besøk eller sitter mye hjemme.
- I løpet av februar tilbrakte testpersonen tre sene kvelder i nærheten Torggata (oransje markør). Mange av Oslos utesteder finnes i dette området. Teledataene kan altså potensielt fortelle hvor vedkommende liker å gå ut, hvor ofte han går ut og hvor sent det blir.
- Teledataene avslører dessuten når vedkommende var på utenlandsreise og hvilket land han dro til.

Hva nå?

I mai 2018 får vi en ny og strengere personopplysningslov i Norge. Da må virksomhetene informere på en mer forståelig og åpen måte. Dessuten vil kravene til gyldig samtykke skjerpes. Alt i alt må virksomhetene ta mer ansvar.

En av Datatilsynets oppgaver er å føre tilsyn med virksomheter og offentlige organer for å sikre at de følger loven. Disse oppgavene vil tilsynet selvsagt jobbe med også etter at den nye loven blir gjeldende. Det kan bli aktuelt å følge opp noen av virksomhetene i denne rapporten, eller det vil kunne være aktuelt å kontrollere andre virksomheter.

Datatilsynet har imidlertid ikke mulighet til å kontrollere alle virksomheter, men det er mye man kan gjøre selv for å ivareta sine egne rettigheter. Det første steget er å be om innsyn. Da ser du hvilke personopplysninger virksomheten lagrer og behandler om deg. Dersom opplysningene er uriktige, kan du kreve at de rettes.

Med de nye reglene får dessuten alle større mulighet til å reservere seg og be om at egne opplysninger slettes.



Besøksadresse:

Tollbugata 3, 0152 Oslo

Postadresse:

Postboks 8177 Dep.,
0034 Oslo

postkasse@datatilsynet.no

Telefon: +47 22 39 69 00

datatilsynet.no

personvernbloggen.no

twitter.com/datatilsynet