DET STORE DATAKAPPLØPET

Rapport om hvordan kommersiell bruk av personopplysninger utfordrer personvernet, november 2015

Datatilsynet

Innhold

Sammendrag

Det pågår et datakappløp i medie- og annonseindustrien. Ny teknologi og muligheten til å samle inn og analysere store datamengder om enkeltindivider er i ferd med å endre måten annonsører når forbrukerne på. En gang var forbrukerne inndelt i store målgrupper som kunne forføres gjennom massemediene. Nå kjøpes vi én og én på globale annonsebørser. Det fører til en markedsføring som er svært målrettet og som forutsetter at markedsførerne har inngående innsikt i våre vaner, interesser, smak og kontaktnett for å treffe best mulig.

Google og Facebook dominerer markedet for automatisert annonsehandel fordi de har så enormt mange opplysninger om oss. I Norge og i Europa er mediehus i ferd med å bygge opp sine egne plattformer for kjøp og salg av annonser.

Når vi går inn på en nettside, besøker vi ikke bare ett selskap, men mange selskap på én gang. I tillegg til publisisten som eier siden, er annonsebørser, kjøper- og selgerplattformer, annonsenettverk, analyseselskap, datahåndteringsplattformer og datameglere til stede med ulike sporingsverktøy. Vår rapport viser at i gjennomsnitt 43 ulike selskap er inne på norske nettaviser og registrerer hva vi gjør. Mellom 100 og 200 informasjonskapsler ble plassert på vår nettleser ved besøk på forsiden til seks norske aviser.

Som bruker legger du kanskje først merke til resultatet av at informasjonskapslene er plassert der, når den samme annonsen begynner å forfølge deg rundt på nettet. Opplysningene som samles inn brukes til å bygge opp omfattende profiler om oss. Jo mer detaljerte profilene er, jo høyere markedsverdi har de.

Hvis vi mister kontrollen over våre egne personopplysninger, mister vi også muligheten til å selv definere hvem vi er. Ingen bransje i verden vet mer om oss enn annonseindustrien. Samtidig har vi svært lite innsyn i hvordan disse selskapene behandler opplysningene om oss.

Personvernet skal gi enkeltindividet beskyttelse mot myndighetenes konstante blikk, men også beskytte oss mot at private virksomheter kan følge med på alt vi gjør. Enkeltindividet er lite i møte med store konsern.

Personvernlovgivningen skal bøte på noe av denne maktubalansen. Men fordi annonseindustrien er så lukket, har enkeltindividet begrensede muligheter til å utøve sine grunnleggende personvernrettigheter i møte med den.

Den informasjonsasymmetrien markedet preges av er en form for markedssvikt. Når forbrukeren ikke har kjennskap til hva som foregår, kan de heller ikke kreve tjenester som gir bedre personvern. Den ujevne fordelingen av informasjon resulterer i en konkurransesituasjon som oppmuntrer markedsaktørene til å ta i bruk mer og mer personverninngripende virkemidler. Når vi surfer på nettet, ønsker vi rask og enkel tilgang til tjenestene vi oppsøker. Vi vil nærmest på automatikk akseptere alt vi blir bedt om å akseptere. Å la behandling av personopplysninger være betinget av samtykke, fungerer derfor i mange tilfeller ikke etter sin hensikt. Ved å la den enkelte bestemme selv, lar man også den enkelte stå alene overfor store og mektige aktører som i realiteten kan diktere hva enkeltmennesket må samtykke til.

Datatilsynet vil jobbe for å øke gjennomsiktigheten og åpenheten i annonsemarkedet, for reell valgfrihet for brukerne, og enkle måter å utøve bestemmelsesretten på. De viktigste anbefalingene og tiltakene vi foreslår i rapporten er:

- Publisister (som aviser) må ta ansvar for tredjepartsaktørene de slipper til på sidene sine.
- Skal du samle inn personopplysninger til profilerings- og markedsføringsformål, må du ha aktivt samtykke.
- Publisister må gi alle brukere tilgang til tjenestene sine, også de som ikke samtykker til at deres opplysninger samles inn.
- Samtykkeerklæringene må bli bedre.
- Publisister, mediebyrå og annonsører må komme sammen og lage retningslinjer som bidrar til å skape større åpenhet om hvordan markedet for målrettet markedsføring fungerer.

Innledning

Det pågår for tiden et datakappløp i medie- og annonseindustrien. Ny teknologi og muligheten til å samle inn og analysere store datamengder om enkeltindivider er i ferd med å endre måten annonsører når forbrukerne på. En gang var forbrukerne inndelt i store målgrupper som kunne forføres gjennom massemediene. Den tiden er over. Nå kjøpes vi én og én på globale annonsebørser. Det fører til en markedsføring som er svært målrettet og som forutsetter at markedsførerne har inngående innsikt i våre vaner, interesser, smak og kontaktnett for å treffe best mulig.

I dag får du persontilpasset reklame på nett, men om ikke lenge får du det også når du ser på tv.

Google og Facebook dominerer markedet for automatisert annonsehandel fordi de har så enormt mange opplysninger om oss. I Norge og i Europa er mediehus i ferd med å bygge opp sine egne plattformer for kjøp og salg av annonser for ikke å tape i konkurransen med utenlandske aktører. Den som har mest data og best teknologi er vinneren i datakappløpet.

Innhøstingen av personopplysninger foregår i stor skala, og den foregår i det skjulte. Vi har ingen anelse om hva som foregår i kulissene når vi besøker en nettside. Markedet preges av informasjonsasymmetri. Hundretalls virksomheter vet svært mye om oss, mens vi ikke vet hvem som vet og hva de vet. Det er hovedårsaken til at Datatilsynet har valgt å se nærmere på annonseindustriens innsamling og bruk av personopplysninger. Vår rett til selvbestemmelse utfordres når vi ikke har kontroll over hvordan våre personopplysninger utnyttes.

I denne rapporten ønsker vi å rette søkelyset mot hvilke konsekvenser det har for personvernet at stadig mer informasjon om våre gjøremål og interesser blir samlet inn og omsatt som en handelsvare.

Formålet er å bidra til økt kunnskap om et komplekst og uoversiktlig marked. Dette markedet berører alle, men de færreste har innsikt i det. Økt kunnskap er første skritt på veien for å skape større åpenhet og gjennomsiktighet i annonsemarkedet og å gi enkeltindividet større kontroll over egne personopplysninger.

Økt kunnskap er også viktig for å sette i gang en debatt. Det er Datatilsynets ønske at rapporten skal bidra til en diskusjon om hvor langt markedsførere kan gå i kartlegge den enkelte for å selge varer og tjenester. Ønsker forbrukerne personalisert innhold og reklame for enhver pris?

I arbeidet med rapporten har vi vært i kontakt med Mediebedriftenes Landsforening, Annonsørforeningen og representanter fra mediebyrå, mediehus, markedsanalyseselskap og annonsører.

Personvern – vår rett til å være i fred

Markedsføring dreier seg om påvirke mennesker. Det er ikke i seg selv noe galt. Men hvor langt kan virksomheter egentlig gå i å påvirke andre før det ikke lenger er greit? Hvilke virkemidler er det greit å ta i bruk for å få et menneske til å handle, tenke eller mene på en bestemt måte?

Noe er enkelt å svare på: Det er selvfølgelig ikke greit å bruke tvang. Det er heller ikke greit å lyve. Men er det greit å samle masse informasjon om en person for å finne ut hvordan man best kan påvirke akkurat dette mennesket? Det er vanskeligere å svare på.

Fra Datatilsynets ståsted melder det seg en helt grunnleggende problemstilling: I hvilken grad respekterer et slikt virkemiddel den enkeltes rett til privatliv?

Respekt for den enkeltes privatliv er i vårt samfunn et helt grunnleggende prinsipp. Det er så grunnleggende at det anses som en menneskerettighet. Prinsippet er for eksempel uttrykkelig inntatt i Den europeiske menneskerettighetskonvensjonen og nedfelt i den norske Grunnloven. Grunnleggende sett handler retten til personvern om at hvert enkelt menneske er et selvstendig og fritt individ – vi har en iboende frihet i oss til å bestemme over eget liv, det er en del av vår integritet eller menneskeverd.

Det sentrale poenget med å beskytte privatlivet er å gi den enkelte rett og mulighet til å råde over seg og sitt, uten innblanding utenfra. Et viktig element her er at begrepet privatliv også omfatter den enkeltes identitet i videste forstand. Den enkelte skal ha frihet og rom for å utvikle sin identitet og personlighet, både i møte med seg selv og i møte med andre. En del av denne friheten dreier seg om fravær av det observerende blikk – enten det kommer fra staten eller private.

Mennesker lever sine liv på ulike arenaer. Vi lever det på jobben, på skolen, hjemme, hos venner og familie, på vei til hytta, på trening og så videre. På alle arenaene har vi rett til privatliv. Vi lever også store deler av livet på internett. I denne verden føler vi oss fri. Vi føler ikke at noen står og ser på hva vi gjør. Vi opplever ingen ubehageligheter som vi kan ta eller føle på. Vi opplever oss ikke invadert eller begrenset.

Men på internett er det alltid noen som følger med. Svært mye informasjon om hva vi gjør i denne verdenen blir registrert, lagret og brukt – i mye større grad enn på noen annen arena. Så selv om vi føler oss fri, er det grunn til å spørre om vi egentlig er det. Er det frihet hvis nærmest alt vi foretar oss blir registrert? Er frihet det samme som fravær av opplevd ubehag eller følelse av å bli invadert?

Det er staten som har ansvaret for sikre retten til respekt for privatliv både etter Den europeiske menneskerettighetskonvensjonen (EMK) og Grunnloven. Dette ansvaret er todelt. Staten er for egen del forpliktet til å respektere den enkeltes privatliv i sine handlinger og aktiviteter overfor enkeltindivider. Men staten har også en forpliktelse til å sørge for at privatlivet blir respektert i forholdet mellom private. Staten har altså et ansvar for å forhindre at private aktører krenker privatlivet–til andre privatpersoner, aksjeselskaper eller andre rettslige subjekter. Dette ansvaret kalles gjerne for sikringsplikten. Staten skal sikre at privatlivet respekteres i utformingen og utviklingen av samfunnet.

Vi vil innlede rapporten med å gi en beskrivelse av markedet for automatisert annonsehandel. Så presenterer vi de viktigste aktørene i verdikjeden fra salg til kjøp av brukere på annonsebørser. I kapittel tre vil vi gå gjennom ulike teknikker for å spore og samle inn opplysninger om individer på nett. Vi vil deretter se på tredjepartsaktører i nettjenester som har reklame. Vi har undersøkt hvor mange tredjepartsaktører som er til stede og hvor mange informasjonskapsler (cookies) som plasseres ut på seks norske nettaviser. I kapittel fire ser vi på hvordan opplysningene som samles inn brukes til å bygge brukerprofiler. Hvilke opplysninger inneholder en profil, og hvor stor verdi har en bruker i kroner og øre? I kapittel fem gjennomgår vi det juridiske rammeverket som annonseindustrien er bundet av. I kapittel seks drøfter vi hvordan utnyttelsen av personopplysninger i annonseindustrien utfordrer personvernet. I kapittel syv oppsummerer vi de viktigste poengene i rapporten og kommer med noen anbefalinger som blant annet kan bidra til å øke åpenheten og gjennomsiktigheten i markedet.

Hva om du ble fulgt like tett ellers som på nett?

La oss ta et tankeeksperiment:

Du går inn i et stort kjøpesenter. Idet du kommer inn, blir du møtt av en mann som forklarer at han jobber for et stort selskap som hjelper kjøpesenteret med blant annet markedsføring og utvikling av senteret. Han forklarer deg at han kommer til å følge etter deg rundt på senteret for å registrere hvilke butikker du går inn i, om du møter noen underveis som du snakker med og mer generelt hva du foretar deg. Grunnen til dette er at senteret ønsker å lære kundene sine bedre å kjenne slik at de bedre kan innrette driften etter kundenes behov. Men slapp av, sier han, jeg skal holde meg på god avstand, du vil ikke merke at jeg er der. Han sier trenger noe mer informasjon om deg før du går videre. Han trenger å registrere noen ting om deg som gjør at senteret kan skille deg fra alle andre brukere. Han forklarer at de gjør dette for å kjenne deg igjen neste gang du kommer. Da vil du nemlig kunne få reklame og tilbud tilpasset deg og dine behov. Men vi registrerer ikke navn og sånne ting. Vi bare registrerer en del kjennetegn ved deg slik at du blir unikt gjenkjennelig for oss. Før du går videre, sier mannen, trenger jeg ditt samtykke. Du vegrer deg litt, og sier til mannen at du ikke ønsker all den registreringen og at du helst vil gå i fred. Mannen svarer da at du selvfølgelig ikke må hvis du ikke vil. Du står fritt til å velge, men ønsker du å gå inn på senteret, er du nok nødt til å akseptere at opplysningene blir registrert og brukt. Hvis ikke er du nødt til å gå ut døren.

Det er temmelig sikkert at du ikke ville akseptert dette i verden utenfor internett. Du ville i større grad følt deg invadert. Du ville også følt det på kroppen som dypt urettferdig og urimelig at du ikke var velkommen inn med mindre du ga ditt samtykke. Du ville følt deg krenket.

Automatisert annonsehandel: Prosesser og aktører

Metaforen «svart boks» er blitt brukt for å beskrive markedet for automatisert annonsehandel. Uttrykket blir brukt fordi det nesten er umulig å få innsikt i hvordan dette markedet fungerer for en utenforstående. De fleste har ingen anelse om at hver gang de besøker en nettside, så selges de samtidig på børs til høystbydende. I dette kapitelet vil vi forsøke å titte inn i den svarte boksen. Vi vil beskrive hvordan prosessen med kjøp og salg av brukere på annonsebørsene fungerer og hvilke aktører som er de mest sentrale.

Hva skjer?

Målretting av reklame er ikke et nytt fenomen. Det som er nytt nå, er at målrettingen ikke lenger retter seg mot grupper av individer, men mot det enkelte individ, og at prosessene automatiseres og overtas av datamaskiner og algoritmer. Aktører i markedsføringsbransjen sier det har skjedd mer i løpet av de siste to årene i annonseindustrien, enn i de foregående femti.[1]

Utviklingen av annonsebørser gjør det mulig å kjøpe og selge enkeltbrukere i sanntid. Publisistene legger unike brukere ut for salg på annonsebørser, og den annonsøren som byr høyest får vise vedkommende reklame. Den viktigste endringen annonsebørsene har ført med seg er at annonsørene ikke lengre kjøper *grupper av brukere* satt sammen av publisisten (for eksempel bil- og motorsportinteresserte). De kan nå kjøpe *en og en bruker av gangen*, og selv bestemme hvor mye de ønsker å betale for hver enkelt bruker. Dette fører til en markedsføring som er svært målrettet.

Automatisert omsetning av annonser foregår i dag på nett, men i løpet av få år vil datastøttet annonsering bli vanlig også i andre kanaler. Det betyr at også TV-reklamen om noen år også vil være personalisert, basert på opplysninger innhentet om våre seervaner.[2]

I Europa har markedet for automatisert annonsehandel vokst kraftig siden 2012. Storbritannia leder an, fulgt av Frankrike, Nederland og Sverige. Norge er foreløpig et stykke bak. Kun elleve prosent av den digitale annonseomsetningen i Norge fant sted på reklamebørser i 2014,[3] mot 46 prosent i Storbritannia.[4] Det norske markedet vokser imidlertid raskt. Enkelte prognoser viser at 25 prosent av det digitale annonsemarkedet i Norge vil være automatisert i 2016[5]. Tre av fire norske aviser legger ut deler av sine annonseflater og brukere for salg på børs.[6]

Hvordan fungerer annonsebørsene?

I det øyeblikket du ber om å bli vist en nettside, går startsignalet for en prosess som medfører at en lang rekke ulike selskap får tilgang til eller samler inn informasjon om deg.

Idet du (dame 40 år, glad i friluftsliv og hytteeier) går inn på en nettavis, blir det opprettet kontakt mellom nettleseren din og en annonseserver. Annonseserveren gir beskjed til publisistens selgerplattform om å fylle de ledige annonseflatene på siden du er i ferd med å laste ned med reklame. Selgerplattformen sender melding til en annonsebørs som inviterer kjøpere til å legge inn et bud på deg. Børsen sender ut informasjon om deg til mediebyråer og kjøperplattformer som er registrert på børsen. Det kan være opplysninger om din IP-adresse, geografiske plassering, inntekt, kjønn, interesser og nettsiden du besøker. På bakgrunn av denne informasjonen, kombinert med opplysninger om deg kjøperplattformen allerede har, sender de inn et bud til børsen. De vet for eksempel at du er på utkikk etter fjellsko og et godt tilbud på peisovn. Budgiveren med det høyeste budet vinner retten til å vise deg en annonse på nettsiden når den lastes opp.

1 The Economist, «Little Brother, Special Report on Advertising and Technology», 13.09.2014, http://www.ogilvydo.com/wp-content/uploads/2014/09/20140913_SR_MAILOUT.pdf

2 For å posisjonere seg i markedet for automatisert annonsehandel, kjøpte Europas største kringkastingsselskap, RTL, annonsebørsen SpotXchange i 2014, ref: McCafferty&co, «European Media Conglomerate RTL Group Purchases SpotXchange, Paving the Way for Broadcasters to Keep Traditional Ad Dollars without the Traditional Ad Model», 01.03.2015, http://mccaffertyco.com/european-media-conglomerate-rtl-group-purchases-spotxchange-paving-the-way-for-broadcasters-to-keep-traditional-ad-dollars-without-the-traditional-ad-model/

3 Delta Projects, «Nåværende Programmatic status i Norge», 2014 http://www.deltaprojects.com/assets/programmaticstatusnorway.pdf

4http://www.iabeurope.eu/files/8914/2789/7694/IAB_Europe_Introduction_to_Programmatic_Webinar_slides.pdf

5 Delta Projects, «Nåværende Programmatic status i Norge», 2014 http://www.deltaprojects.com/assets/programmaticstatusnorway.pdf

6 Delta Projects, «Nåværende Programmatic status i Norge», 2015, http://www.deltaprojects.com/assets/programmatic_norway_norska.pdf

Automatisert sanntidskjøp av brukere på annonsebørs

1 **Kari** (to barn, 41 år, pusser opp huset, friluftsinteressert og glad i å trene) skriver inn nettadressen til en nettavis hun ønsker å lese.

2 **Publisist**

3 **Annonsebørs/selgerplattform** Sender melding til kjøpere om at de kan by på en bruker med følgende karaktertrekk: Småbarnsmor, 40-50 år, friluftsinteressert og glad i å trene.

4 **Kjøperplattformer** beregner hvor høyt bud de vil legge inn på brukeren. Prisen baseres på grunnlag av opplysningene børsen sender over og opplysninger de selv har om denne brukeren.

200 millisekunder

Dataanalyseplattformer og datameglere tilbyr ytterligere opplysninger om Kari som kjøperne kan bruke for å finne ut hvor attraktiv hun er å by på.

5 **Kjøperplattformen** med det høyeste budet vinner budrunden. Annonsebørsen/selgerplattformen gir beskjed til vinneren om at de kan plassere reklame på siden.

6 **Vinneren** plasserer reklame på siden via sin annonseserver.

7 **Brukeren** ser reklamen når siden lastes ned på datamaskinen.

Publisist

Alt skjer i løpet av millisekunder. Prosessen kan høres enkel ut, men i virkeligheten er det mange hundre selskaper som konkurrerer med hverandre. Foruten selgere og kjøpere av reklame er også en stor gruppe av selskap som leverer data og dataanalyse involvert i prosessen (for en mer detaljert beskrivelse av prosessen, se boks side 16).

Aktørene

Annonsemarkedet på nett har alltid vært komplekst. Mange aktører er involvert i verdikjeden mellom selger og kjøper av annonseplass. Overgangen til datastøttet annonsering har imidlertid komplisert aktørbildet ytterligere. Det har i løpet av få år vokst frem en hel industri av selskap som lever av å bistå annonsører og publisister i prosessen med å levere rett annonse til rett bruker.

Det er utfordrende å lage klare skiller mellom aktørene i dette markedet. Mange av aktørene har flere roller i verdikjeden samtidig. Markedet er fortsatt i støpeskjeen, og flere av aktørene og funksjonalitetene vi ser akkurat nå, vil kanskje være borte eller ha endret seg om kort tid. Endringene skjer svært fort. Selv om de teknologiske løsningene skiftes ut eller endres, så vil det mest sentrale ved denne nye måten å drive annonsesalg på ligge fast, nemlig at brukere kjøpes en og en av gangen basert på målrettingskriterier utledet fra analyse av store datamengder samlet inn om den enkelte.

I tabellen på neste side har vi delt markedsaktørene inn i fire hovedkategorier; de åpne annonsebørsene, kjøpere av annonseplass, selgere av annonseplass, og tilbydere av data og dataanalyse. Enkelte selskap, som Google, har mange hatter og opptrer som både kjøper og selger av annonseplass og som tilbydere av dataanalyse. Dette gjør at Google skiller seg ut som den suverent mektigste aktøren i dette markedet.

Annonsebørser

En annonsebørs er en markedsplass for kjøp og salg av annonseplasser, bygget opp etter samme prinsipper som finansbørsene. Annonsebørsene er bindeleddet mellom annonsører og publisister, og er i ferd med å overta rollen som annonsenettverkene hadde tidligere.

Annonsebørsene ble introdusert i 2007 som en plattform for å drive med sanntidskjøp (real time bidding). Børsene fungerer som en nøytral plattform der kjøpere av annonseplasser kan by på brukere lagt ut av publisistene.

Et overveldende antall brukere er tilgjengelig for salg på annonsebørsene. Hvert sekund omsettes 1,3 millioner brukere på annonsebørser.[7] Antallet transaksjoner på annonsebørsene er tolv ganger større enn antallet transaksjoner på New York Stock Exchange.[8] Alle de største internettselskapene, Facebook, Yahoo!, Google og Microsoft, eier sin egen annonsebørs.

Selgere av annonseplass

Publisister lever av å selge annonseflater der markedsførere kan nå brukere med reklame for sine produkter. Publisister omfatter tradisjonelle avishus, nyhetsportaler og startsider, sosiale medier og søkemotorer.

De tradisjonelle mediehusene har de siste årene slitt økonomisk. De taper blant annet en stadig større andel av annonseinntektene til Google og Facebook. I USA er Googles annonseinntekter nå større enn alle avisene og magasinenes annonseinntekter til sammen.[9] Google og Facebook kan, takket være det enorme datagrunnlaget de sitter på om sine brukere, tilby annonsørene svært målrettet annonsering.

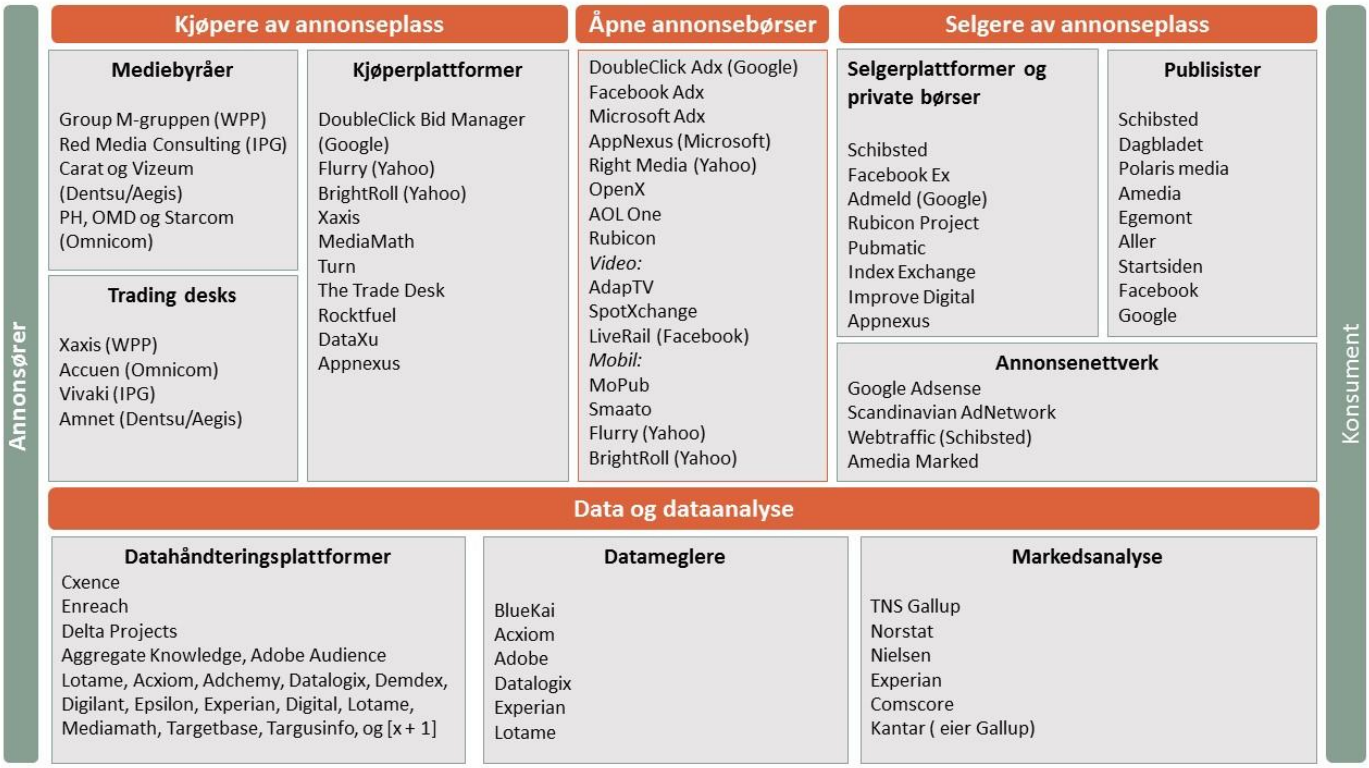
Mediehus i Europa og i Norge er i ferd med å investere tungt i teknologi i et forsøk på å ta opp kampen med de globale gigantene. De tre største norske mediehusene, Schibsted, Polaris Media og Amedia, har innført innloggingsløsninger som kan spore kundene på tvers av virksomhetens ulike tjenester. Ved å innføre innloggingsløsninger får avisen svært detaljert kunnskap om sine kunder. Dette er verdifulle data å tilby annonsører som ønsker å nå helt spesifikke målgrupper.

---

[7] Smith, Mike, «Targeted. How Technology Is Revolutionizing Advertising and the Way Comnpanies Reach Consumers», Amacom, 2015.

[8] Le Monde Diplomatique, «Reklamerevolusjonen», november 2013, http://www.lmd.no/?p=13010

[9] Business Insider, «Google Is Now Bigger Than Both The Magazine And Newspaper Industries», 12.11.2013, http://www.businessinsider.com/google-is-bigger-than-all-magazines-and-newspapers-combined-2013-11



Tabell 1: Oversikt over de ulike aktørene, gruppert etter rolle.

Publisister som ønsker å legge ut ledig annonseflate og brukere for salg på annonsebørsene må benytte en **selgerplattform** (supply side platform). Selgerplattformer er programvare som er spesielt utviklet for dette formålet. Admeld (Google), Rubicon Project, Pubmatic og Index Exchange er eksempel på selskaper som tilbyr slik programvare og som benyttes av norske avishus for å legge ut brukere for salg på de åpne annonsebørsene.

Selgerplattformer kan også fungere som annonsebørser som handler direkte med inviterte kjøperplattformer. De kalles da private børser. Det er en voksende trend at publisister oppretter slike for å få større kontroll over eget annonsesalg og for å hente ut verdien av egne kundedata. Man antar at private børser og åpne børser fremover vil bli omtrent like store når det gjelder antallet transaksjoner som gjennomføres. Schibsted er i full gang med å utvikle sin egen børsplattform. Selskapet jobber med å få andre norske mediehus til å slutte seg til denne børsen i stedet for å legge ut sine brukere for salg på de åpne annonsebørsene.[10] Jo flere aktører de klarer å samle, jo flere brukere vil de kunne tilby for salg og jo mere brukerdata vil de kunne samle inn og utnytte til analyse i forbindelse med målretting av reklame. Lignende allianser der publisister samarbeider om teknologi og data etableres over hele Europa. [11] Foreløpig har Amedia og Polaris Media meldt interesse for Schibsteds annonsebørs. Dagbladet, TV2, Nettavisen og Egmont har uttalt at de vil fortsette å benytte Googles plattform for annonsesalg. [12]

En annen strategi for mediehusene er å utvikle løsninger for målretting av innhold som går hånd i hånd med målrettingen av reklame. For å øke verdien av sine annonseflater kan mediehusene friste annonsørene med muligheten til å vise reklame for slalåmski til brukere ved siden av innhold som reflekterer denne interessen.

---

[10] Dagens Næringsliv, «Kjemper om reklamebørs», 01.05.2015, http://www.dn.no/etterBors/2015/05/01/2052/Reklame/kjemper-om-reklamebrs.

[11] I Storbritannia har The Guardian tatt et lignende initiativ som Schibsted. Sammen med CNN International, the Financial Times, Reuters og The Economist har The Guardian etablert den private børsen The Pangaea Alliance. Initiativtagerne sier at deling av data er en vesentlig del av samarbeidet. http://advertising.theguardian.com/pangaea-alliance/

[12] Dagens Næringsliv, «Kjemper om reklamebørs», 01.05.2015, http://www.dn.no/etterBors/2015/05/01/2052/Reklame/kjemper-om-reklamebrs.

Kjøpere av annonseplass

Annonsørene er avhengig av publisistene for å markedsføre sine produkter til potensielle kjøpere. Mange annonsører sitter etter hvert på store mengder kundedata, samlet inn gjennom bruk av for eksempel lojalitetskort. Dataene brukes til å bygge profiler slik at markedsføringen kan målrettes mest mulig. Mange annonsører velger å benytte et mediebyrå som bistår virksomheten med å plassere reklame på en optimal måte.

Fem store **mediebyrå** dominerer bransjen internasjonalt og i Norge: Public Omnicom Group, Denstu/Aegis, WPP, Interpublic Group (IPG) og Havas Group. For å møte konkurransen fra Google, Facebook, Microsoft og Yahoo, er mediebyråene i ferd med å utvikle seg i retning av teknologiselskap med ekspertise på dataanalyse, profilbygging og datainnhøsting.[13] Alle de store mediebyråene har foretatt flere strategiske oppkjøp av teknologi- og dataanalyseselskap de siste årene.[14]

Fordelen mediebyråene har, sammenlignet med Facebook og Google, er at de ved å ha annonsører som kunder har tilgang til deres kundedata. Kundedata er verdifulle data i arbeidet med å målrette reklamen mest mulig fordi de gir faktiske opplysninger kundene og hvilke produkter de har kjøpt og er interessert i. Den globale forskningsdirektøren i Starcom (Public Omnicom Group) har uttalt at mediebyråene bør bli eksperter på å forvalte data på tvers av selskaper.[15] Kjell Gabrielsen, leder i Xaxis (kjøperplattformen til WPP) har uttalt: «Gjennom vår DMP (datahåndterings-plattform, red anm.), samler vi inn og bearbeider dataene slik at vi kan kjøpe annonsevisninger kun mot de personene annonsøren ønsker å treffe. (...) Dataene som Xaxis bearbeider kommer fra flere kilder. Vi kjøper tredjepartsdata, demografiske variabler innkjøpt fra eksterne aktører; annenpartsdata, typisk interessedata som er basert på erfaringer av tidligere kjøp; og førstepartsdata, data som kommer fra kundene. Data fra kundesiden benyttes aldri på tvers av kunder.»[16]

For å kjøpe brukere på en annonsebørs er det nødvendig å gå via en såkalt **kjøperplattform** (*demand side platform*) som er programvare spesielt utviklet for dette formålet. Mediebyråene har opprettet egne kjøperplattformer. Xaxis er for eksempel kjøperplattformen til WPP. Det er ikke kun mediebyråer som har etablert kjøperplattformer. Google og Yahoo har utviklet kjøperplattformer, samt flere datameglere (som vi vil komme tilbake til i neste punkt) som for eksempel MediaMath.

Kjøperplattformen kjøper brukere basert på målrettingskriterier, en algoritme utviklet i samarbeid med kunden. Algoritmen er basert på sammenstilling av data fra flere ulike kilder: kundedata som annonsøren er i besittelse av, data samlet inn av kjøperplattformen ved hjelp av informasjonskapsler og data innhentet fra tredjeparter, som opplysninger hentet fra sosiale medier. Når en børs sender over en bruker som møter kriteriene i algoritmen, vil kjøperplattformen automatisk avgjøre hvor stor verdi brukeren har og legge inn et bud på vegne av annonsøren. Teknologien som gjør dette mulig kalles cookie-matching. For at kjøpersiden skal kunne avgjøre hvorvidt de vil legge inn et bud, og *hvor mye* de vil by, må de vite hvem brukeren er. Cookie-matching gjør dette mulig (mer om cookie-matching på side 20).

Hvis kjøperplattformen vinner budrunden, plassere de en informasjonskapsel i nettleserne til brukeren når de serverer vedkommende reklamen. Dette gjør det mulig for kjøperplattformen å måle hvor effektiv målrettingsalgoritmen er. Hvis brukeren ikke responderer på annonsen kan de justere kriteriene i algoritmen slik at de ikke kjøper tilsvarende bruker en gang til. Utplassering av informasjonskapsler benyttes også for å kunne følge samme bruker over tid. Dette gjør det mulig å nå samme person med tilsvarende reklame på andre nettsteder samt å bygge opp en profil på vedkommende.

Datahåndteringsplattformer, datameglere og markedsanalyse

Den mest uoversiktlige delen av aktørbildet består av alle selskapene som befinner seg i midten av verdikjeden og som lever av å selge brukerprofiler og dataanalyse til markedsførere og publisister. Som vi kommer tilbake til i kapittel fire, utgjør disse selskapene den største gruppen av tredjepartsaktører som er inne på en nettside.

---

[13] WPP, verdens største kommunikasjonsselskap har for eksempel kjøpt opp verdens største markedsanalyseselskap Kantar. http://www.wpp.com/wpp/companies/kantar/

[14] The Economist, «Little Brother, Special Report on Advertising and Technology», 13.09.2014, http://www.ogilvydo.com/wp-content/uploads/2014/09/20140913_SR_MAILOUT.pdf

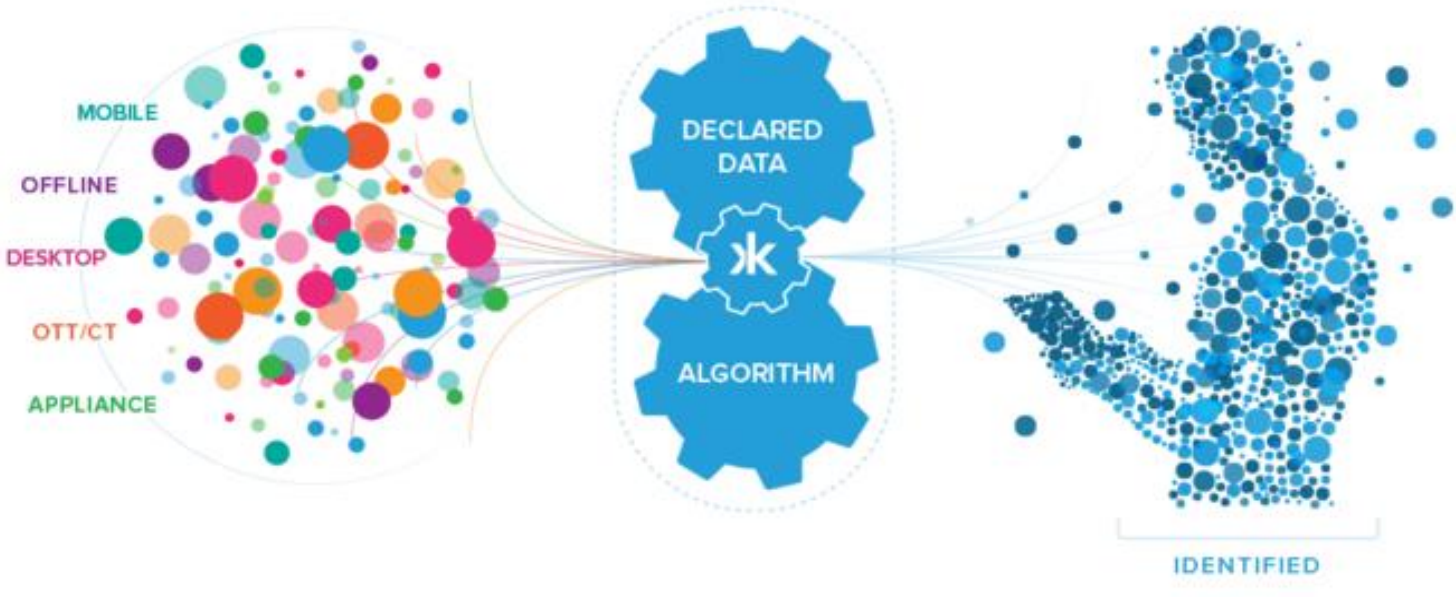
[15] «The Future of the Data Driven Media Agency - A perspective from Starcom MediaVest Group», http://cimm-us.org/wp-content/uploads/2012/07/The-Future-of-the-Data-Driven-Media-Buying-Agency_Kate-Sirkin_SMG.pdf

[16] http://www.analysen.no/latest-news/regular-news/item/intervju-kjell-gabrielsen-xaxis-programmatic-buying

Datameglere (engelsk: data brokers) er selskap som lever av å samle inn personopplysninger som selges videre som brukerprofiler.[17] Profilene selges til markedsførere som ønsker å nå spesifikke brukere med sine produkter, eller publisister som ønsker å berike egne data. Det spesielle med datameglere er at de ikke har et direkte kundeforhold til dem de samler inn opplysninger om, slik for eksempel en annonsør eller en publisist har. Få forbrukere kjenner derfor til at disse selskapene eksisterer og at de behandler personopplysninger om dem som utnyttes videre til kommersielle formål.

De største datameglerne er amerikanske, blant annet Acxiom, Experian og Datalogix. Selv om selskapene opererer fra USA, innhenter de opplysninger om forbrukere uavhengig av nasjonale grenser. Opplysninger hentes inn ved bruk av informasjonskapsler og fra sosiale medier og offentlig tilgjengelige registre. Acxiom har for eksempel lagret opplysninger i sine registre om 700 millioner brukere verden over. I gjennomsnitt er det registrert over 3000 opplysninger på hver person i deres registre.[18] Acxiom har i dag kontorer over hele verden, også i Europa.[19]

Experian og Bisnode er eksempel på datameglere som etablert i Norge. Så langt Datatilsynet er kjent med bygger disse selskapene målgrupper og profiler basert adresselister og aggregerte og anonyme data hentet fra offentlige registre og offentlig tilgjengelig statistikk. Vi er ikke kjent med at disse selskapene bygger opp profiler ved bruk av for eksempel informasjonskapsler. På grunn av konkurransen fra internasjonale konkurrenter vil nok datameglerselskap etablert i Norge og Europa fremover trolig være interessert i å undersøke muligheten for å hente inn og sammenstille opplysninger på flere måter og fra flere kilder enn i dag.



Kilde: Krux Identity Management

17 Definisjon hentet fra Federal Trade Commission, «Data Brokers. A Call for Transparency and Accountability», 2014, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

18 Ibid.

19 Acxiom har blant annet bistått det britiske mediehuset The Guardian med å identifisere og integrere 75 ulike kilder med kundedata som skal brukes for å tilby annonsører best mulig målrettet annonsering, ref: Acxiom, «Casestudy: The Guardian, Boosting audience engagement across the globe», 2014, http://dq2quoj6xxb34.cloudfront.net/wp-content/uploads/2014/02/The-Guardian.pdf

Datahåndteringsplattformer (data management platforms (DMP)) er big data-løsninger utviklet spesielt for å målrette innhold og reklame på nett. Teknologien brukes for å organisere, sammenstille og analysere data fra mange ulike kilder. Formålet med en datahåndteringsplattform er å analysere data på en slik måte at det gir et mest mulig rikt bilde av den enkelte forbruker.[20] Kunnskapen brukes til å predikere sannsynligheten for at de vil kjøpe bestemte produkter.

For å bygge opp et mest mulig detaljert bilde av den enkelte bruker, benytter datahåndteringsplattformene hva de kaller «identitetshåndteringssystemer». Dette er teknologi som gjør det mulig å knytte sammen data innhentet fra mange ulike kilder til én unik person. For eksempel kan en datahåndteringsplattform koble sammen opplysninger en annonsør har samlet inn om en kunde via et lojalitetskort, med opplysninger om denne kunden innhentet fra sosiale medier eller ved bruk av informasjonskapsler. På denne måten kan man ved hjelp av et «identitetshåndteringssystem» bygge opp hva bransjen omtaler som et 360 graders bilde av den enkelte forbruker.

Mange selskap tilbyr datahåndteringsplattformer, mediebyrå for eksempel. Det finnes også frittstående datahåndteringsplattformer, for eksempel Aggregate Knowledge og Adobe Audience. Cxense er et norskeid selskap som leverer slik teknologi. I løpet av få år har de blitt leverandør av målrettingsteknologi til publisister verden over.21 I Norge samarbeider de blant annet med Amedia og Polaris Media.

Stadig flere selskaper tilbyr både datahåndterings-teknologi og kjøperplattformfunksjonalitet. Slike selskap blir referert til som konsoliderte mediakjøperplattformer.

Flere av datameglerne over faller i denne kategorien, blant annet Acxiom, Blue Kai, eXelate, Datalogix, Demdex (eid av Adobe), Epsilon, Experian, Digital, Lotame og Mediamath. Det betyr at de både tilbyr verktøy for å analysere data og for å kjøpe annonsevisninger.

Ved å opptre som kjøperplattform i tillegg til å være datahåndteringsplattform, har selskapene mulighet til å samle inn enda mer opplysninger om enkeltbrukere. Kjøperplattformer har, som tidligere omtalt, mulighet til å høste inn opplysninger om enkeltbrukere i forbindelse med budgivningsprosessen på annonsebørsene og ved utplasseringen av informasjonskapsler ved plassering av reklame. Opplysningene selskapene henter inn via kjøperplattformen kan de gjenbruke i utviklingen av målrettingsalgoritmer som foretas av datahåndteringsplattformen.

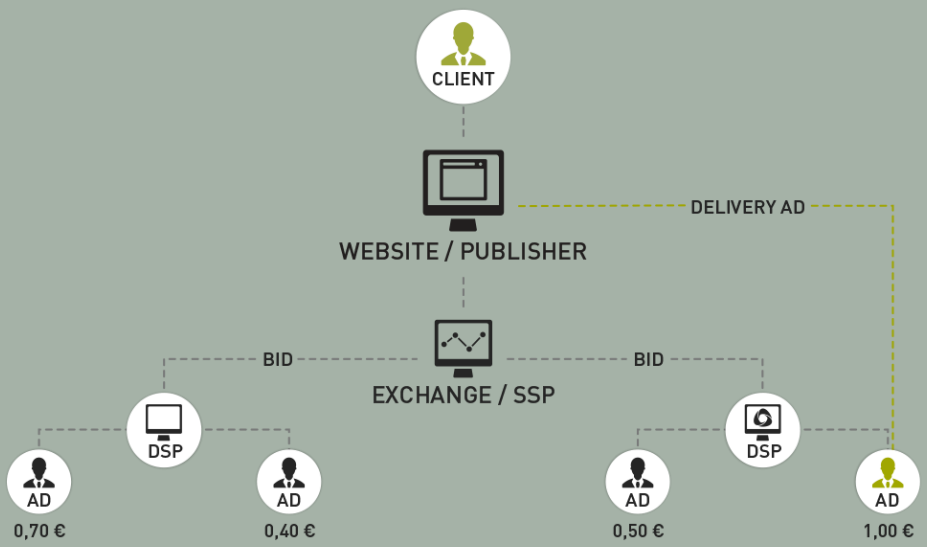
Markedsanalyseselskap har tradisjonelt vært viktige for annonsører og mediebyrå i forkant og etterkant av reklamekampanjer for å finne rett målgruppe og for å evaluere effekten av kampanjen. Markedsanalyseselskapene har i hovedsak hentet inn data ved å bruke telefonintervjuer eller webpaneler. Omleggingen til sanntidskjøp av annonser gjør det nødvendig å kunne evaluere effekten av målrettingen i sanntid, slik at målrettingskriteriene kan justeres fortløpende hvis de viser seg å ikke fungere optimalt. For å ikke bli utkonkurrert av mediebyrå og andre aktører som leverer dataanalyse, er markedsanalysebransjen også tvunget til å utvikle løsninger som gjør sanntidsanalyse mulig.[22]

20 IAB Europe, «Programmatic Trading. An IAB Europe White Paper», 2014, http://www.iabeurope.eu/files/8614/0776/0957/IAB_Europe_Programmatic_Trading_White_Paper_July_2014_v2.pdf

21 https://www.cxense.com/

22 Analysen, «Vil markedsførerne ha behov for markedsanalyse i fremtiden?», Analysen nr. 3, 2013, http://www.tns-gallup.no/tns-innsikt/vil-markedsforerne-ha-behov-for-markedsanalyse-i-framtida

Sanntidskjøp skritt for skritt



1. Du setter seg foran datamaskinen for å lese nyheter. Du skriver inn adressen til nyhetsmediet du ønsker å lese øverst på siden, for eksempel www.morgenavisen.no.

2. Straks du har trykket på enter sender nettleseren en henvendelse til Morgenavisens dataserver om hvilken side du ønsker å se på. Denne henvendelsen består av en HTML-kode.

3. Morgenavisen sender tilbake en kode til din datamaskin som setter opp det publisistiske innholdet til siden du vil se på.

4. Sammen med innholdet sender Morgenavisen også over en kode som kalles *ad tag*. Denne koden er knyttet til annonsene som også skal være på siden. Når denne koden når datamaskinen din, sender den umiddelbart videre et varsel til annonsebørsen som Morgenavisen har en avtale med. Dette varselet, som sendes fra Morgenavisens server via din nettleser til annonsebørsen, kalles en *ad call*. Den varsler annonsebørsen om at de tomme annonseplassene på nettsiden du er i ferd med å laste opp, må fylles med reklame.

5. Ad callen gir beskjed til annonsebørsen om at de må gjennomføre en auksjon for å fylle annonseplassene med reklame. Dette varselet gir også børsen *tilgang til deg*.

6. Børsen har nå mulighet til å lese cookiene som de tidligere har installert på din datamaskin (om du ikke har slettet dem). Cookiene plasserte de der i forbindelse med at de har servert deg reklame tidligere. Disse informasjonskapslene gjør det mulig for børsen å gjenkjenne deg som en bruker de allerede har en profil på. Børsen har opprettet en unik kode på deg på sin server, for eksempel ABCD. Ved bruk av cookies installert på din datamaskin, har de bygget opp en profil på deg. Profilen inneholder for eksempel opplysninger om hvilke reklamer du har sett tidligere, hvilke nettsider du har besøkt, tekniske opplysninger om din datamaskin (type maskin, nettleser, programvare og så videre), IP-adresse, lokasjonsdata. Koden inneholder ikke navnet ditt eller andre direkte personidentifiserbare opplysninger.

Sanntidskjøp forts.

7. Når kjøperplattformene mottar ad callen, gjør dette varselet det mulig for dem å gjenfinne eventuelle cookies som *de* har plassert på din datamaskin i forbindelse med tidligere børstransaksjoner der de har fått tilgang til å servere deg reklame. Dersom du har slettet disse informasjonskapslene, fremstår du som en bruker de ikke har vært i kontakt med tidligere.

8. Børsen sender din unike kode til alle kjøperplattformene som er tilknyttet børsen. Også dette kalles en ad call. Ad callen varsler potensielle budgivere om at de har mulighet til å sende reklame til bruker ABCD med de karaktertrekkene som ligger i din profil.

9. Kjøperplattformene som ønsker å delta i budrunden prøver nå å finne ut som mye som mulig om deg for å avgjøre hvor høyt bud de skal legge inn. De kombinerer opplysninger hentet fra cookiene på nettleseren din med data hentet fra andre kilder, eks kundedata levert av annonsøren de jobber for. Cookiene gir informasjon om hvor ofte de har annonsert til deg tidligere, hvilke reklamer du har blitt servert og typer nettsider du har besøkt (hvilke nettsider du har besøkt vet de fordi de har informasjon om på hvilke nettsider reklamen du har blitt vist tidligere har havnet).

10. Alle de ulike kjøperplattformene som deltar i budgivningen har bygget opp en profil på deg. De kjenner ikke ditt navn, men de vet svært mye om dine interesser og kjøpsvaner, og profilen bygges stadig mer detaljert etter hvert som nye opplysninger om deg blir samlet inn. Din profil har en unik kode, for eksempel 1234. *Kjøperplattformen vet også en annen ting: de vet at brukeren som de kjenner som 1234 er den samme som børsen identifiserer som ABCD*. Fordi de vet at bruker 1234 og bruker ABCD er den samme brukeren, er de i stand til å vurdere *hvor mye* du er verdt. Teknikken med å koble sammen de to brukeridentitetene kalles «cookie-matching» og er en avgjørende mekanisme i systemet med sanntidskjøp.

11. Alle kjøperplattformene som vurderer å delta i auksjonen foretar en cookie-match. Ved å foreta en cookie-match er de i stand til å avgjøre hvor høyt bud de er villige til å gi for akkurat deg. Hvis din profil viser at du stadig vekk surfer på luksusbiler og at du gjentatte ganger har kjøpt dyre klokker eller smykker, har DSP-en utviklet en algoritme som automatisk vil legge inn et bud på deg slik at de kan vise deg reklame for eksklusive eiendommer eller luksus-cruise.

12. Alle budgiverne oppgir en sum de vil betale for retten til å vise deg reklame.

13. Auksjonen finner sted i sanntid. Sanntidsauksjoner er såkalte secondprice-auksjoner. Det vil si at deltakerne kun gir ett bud og at budgiveren med det høyeste budet vinner.

14. Børsen sender et varsel til den kjøperplattformen som vant auksjonen.

15. Kjøperplattformen som vant sender en kode som setter opp annonsen i nettleseren din. Den plasserer samtidig en cookie på din maskin slik at den kan kjenne deg igjen ved neste korsvei, og slik bygge videre på din profil.

16. Annonsen vises på nettsiden i det den lastes opp på skjermen din. Antageligvis er du helt ukjent med alle aktørene og alle prosessene som har vært involvert i denne prosessen, som har tatt i underkant av et millisekund.

Beskrivelsen er hentet fra Smith, Mike, « Targeted. How Technology Is Revolutionizing Advertising and the Way Companies Reach Consumers», Amacom, 2015.

Innsamling av data

Mange tror annonsefinansiert innhold på nett er gratis. Dette er feil. Vi betaler med våre personopplysninger for å få tilgang til tjenestene. Personalisert innhold og markedsføring krever innsamling av mange personopplysninger. Ordet *relevans* er hyppig brukt av medie- og annonseindustrien. Jo mer data som samles inn om den enkelte, jo lettere er det å servere brukerne relevant reklame og innhold. Alle aktørene i verdikjeden, fra publisist til annonsør og markedsførere og analyseselskap, henter inn data om kunder og brukere i prosessen med å målstyre reklamen. I all hovedsak foregår denne datainnsamlingen i det skjulte.

I dette kapittelet vil vi først gå gjennom de ulike teknikkene som brukes for å samle inn opplysninger om brukeren. Deretter vil vi undersøke hvilke aktører som er til stede og som samler inn opplysninger om norske brukere på et utvalg av norske nettaviser.

Ulike typer sporingsteknologi

Informasjonskapsler, IP-adresse, sporingsbilder og digitale fingeravtrykk

En annonse for en vaskemaskin invaderer alle nettstedene du besøker etter at du har sjekket prisene på andre modeller. Dette er tegnet på at du blir sporet via **informasjonskapsler** eller cookies[23]. Bruk av informasjonskapsler er den mest utbredte teknologien for å spore brukere på nett. En informasjonskapsel er en liten fil som blir lagret i brukerens utstyr når brukeren besøker et nettsted. Hver gang brukeren besøker nettstedet, sender nettleseren informasjon tilbake til nettstedets server for å varsle nettsiden om brukerens aktivitet på siden. Selskap kan plassere ut informasjonskapsler som ligger lagret på folks utstyr over flere år, også mer enn ti år, eller bruke informasjonskapsler som slettes umiddelbart når nettsesjonen avsluttes.

Det er vanlig å skille mellom såkalte førsteparts-cookies og tredjeparts-cookies. Førsteparts-cookies er informasjonskapsler som nettstedeier selv har plassert ut og har kontroll over. Tredjeparts-cookies er informasjonskapsler som nettstedeier har sluppet til på siden, men som andre selskap enn nettstedeier har kontroll over. [24] Tredjeparts--cookies er hovedsakelig plassert ut av selskap som driver med markedsanalyse og målrettet markedsføring. Selskap som er til stede med tredjeparts-cookies er vanligvis ikke bare til stede på ett nettsted, men på hundrevis av nettsteder. Dette gjør det mulig for selskapene å følge den samme brukeren fra nettsted til nettsted og å bygge opp omfattende profiler på vedkommende basert på surfehistorikken.

Bruk av informasjonskapsler har flere svakheter sett fra annonseindustriens ståsted: For det første egner ikke informasjonskapsler seg til å spore den samme brukeren *på tvers* av de ulike plattformene (mobil, nettbrett, datamaskin) en bruker har. For det andre krever bruk av informasjonskapsler samtykke fra brukeren. For det tredje er det mulig for sluttbruker å takke nei til installering av informasjonskapsler og å slette informasjonskapsler. Endelig så gir informasjonskapsler upresise data. Opplysninger samlet inn via informasjonskapsler gir ikke faktisk kunnskap om et individ. Ved å analysere opplysninger innhentet ved bruk av informasjonskapsler kan selskap utelukkende gjøre *antagelser* om hvem brukeren er, for eksempel om hvilket kjønn eller alder brukeren har. Å samle inn data om brukerne ved hjelp av innloggingsløsninger gir mer korrekte data. Google har annonsert at de i framtiden muligens vil slutte med informasjonskapsler.[25]

Nettbrukere kan også spores ved å samle inn deres **IP-adresse**. En IP-adresse er en unik identifikator som viser til en enhet, som en pc eller et nettbrett, i et nettverk som Internett. IP-adressen kan blant annet gi informasjon om lokasjonen til brukeren og hvilket nett den kommer fra. De fleste brukere har samme IP-adresse over et visst tidsrom, og den kan derfor benyttes til å følge en bruker over tid. Den er likevel ikke veldig godt egnet til å spore sluttbrukere over lang tid, slik det er mulig med informasjonskapsler. Fordelen med en IP-adresse er allikevel at den er så tilgjengelig. IP-adressen innhentes i første rekke av nettstedeier. Tredjeparter som er tilstede på nettsiden kan hente inn IP-adressen

23 Vi bruker både «informasjonskapsler» og «cookies», da de begge er i bruk i norsk dagligtale. Begrepene er helt synonyme.

24 Tredjeparter plasserer ut cookies på nettleseren til brukerne av nettstedet ved først å ha plassert et sporingsbilde (webbeacon) på siden. Det er nettstedeier som lar tredjepartene plassere disse sporingsbildene. Sporingsbildet gjør det mulig for virksomheten å innhente IP-adressen til brukeren. IP-adressen er nødvendig å ha for å kunne plassere en cookie på brukerens nettleser.

25 USA Today, «Google may ditch «cookies» as online ad tracker», 17.09.2013

til brukerne ved å benytte sporingsbilder (web beacons).[26]

Sporingsbilder (web beacons) brukes alene eller i kombinasjon med cookies for å skaffe mer informasjon om de besøkende til nettsiden. Et sporingsbilde er vanligvis et usynlig grafisk bilde (vanligvis 1 pixel x 1 piksel) som er plassert på nettsiden. Sporingsbilder brukes også av tredjeparter til å samle inn opplysninger om brukerne og som en mekanisme for å plassere ut cookies. Sporingsbilder kan brukes til å samle inn opplysninger om blant annet brukerens IP-adresse, tidspunktet for når nettstedet ble besøkt, hvilken nettleser brukeren har med mer.

Det er ikke mulig å reservere seg spesifikt mot bruk av sporingsbilder. Stiller man inn nettleseren til ikke å akseptere informasjonskapsler, vil man allikevel bli sporet av sporingsbilder. Personopplysningslovens krav til behandlingsgrunnlag gjelder også ved bruk av sporingsbilder.

For å komme rundt svakhetene til ip-adresser og informasjonskapsler som sporingsverktøy, har annonseindustrien begynt å bruke **digitale fingeravtrykk** (*«device fingerprint»).* Digitale fingeravtrykk er det unike elektroniske avtrykket enhver datamaskin har når den er koblet til internett. IP-adressen, sammen med opplysninger om type nettleser, språkvalg, ulikheter i elektronikken og liknende til sammen kunne gi et tilstrekkelig unikt avtrykk til å kalles et digitalt fingeravtrykk. Slike avtrykk blir av annonseindustrien betraktet som et alternativ til informasjonskapsler. I motsetning til informasjonskapsler kan ikke brukeren motsette seg bruk av digitale fingeravtrykk. Digitale fingeravtrykk representerer derfor en alvorlig trussel for personvernet til den enkelte. EU-kommisjonens rådgivende organ i personvernspørsmål, Artikkel 29-gruppen, har laget en anbefaling om digitale fingeravtrykk. Artikkel 29-gruppen konkluderer med at cookie-reglene også gjelder for digitale fingeravtrykk. Dette betyr at samtykke skal innhentes før det samles inn informasjon om brukerens utstyr. Fra industriens ståsted er ulempen med digitale fingeravtrykk, som for informasjonskapsler, at teknologien ikke er velegnet til å spore brukeren på tvers av plattformer.

Unik ID – fremtidens sporingsløsning

På grunn av alle svakhetene til sporingsløsningene vi hittil har gjennomgått, har de store internettaktørene utviklet nye metoder for å følge brukeren på nett og mobil. Alle de største internettselskapene har etter hvert utviklet **innloggingsløsninger** som kan spore brukerens unike identitet (navn, adresse, telefonnummer). Bruk av innloggingsløsninger gir mer korrekte data om brukerne, og dermed også mer verdifulle data for aktørene, enn data samlet inn ved bruk av cookies. Innloggingsløsningene holder brukeren kontinuerlig pålogget og gjør det mulig å følge brukeren fra plattform til plattform gjennom dagen. Facebook var det første store selskapet som innførte kontinuerlig innlogging for å samle inn brukerdata. Andre store aktører som Google, Microsoft og Amazon har kommet etter. I Norge har alle de tre største mediehusene, Schibsted; Polaris Media; og Amedia, innført innloggingsløsninger. Ved å innføre innloggingsløsninger ønsker publisistene å få mer kontroll over egne kundedata slik at de kan innhente forspranget annonsørsiden har i å samle inn og å utnytte brukerdata til profilering.

Overgang til innloggingsløsninger representerer en trussel for aktører som baserer sine analyser på innsamling av data hentet inn gjennom tredjeparts-cookies. Mediebyråer og datatilbydere som Bluekai og eXelate vil, hvis noen få innloggingsløsninger blir dominerende i markedet, få tilgang til færre data. Det er kjent at mediebyråene derfor planlegger å bygge opp sine egne løsninger for å kunne følge unike brukere på tvers av plattformer.[27]

En annen metode for å få kunnskap om brukerne er å foreta nødvendige registreringer via apper. Ikke bare er det lettere å holde brukeren konstant pålogget, det er også mulig å benytte appens identifisering. Dette gir ikke mulighet til sporing på kryss av plattformer, om man da ikke identifiserer brukeren med for eksempel navn eller mobilnummer. En ulempe med app-registrering sett fra annonsørenes side er at brukerne ønsker å begrense antall apper.

Store selskap som Google, Apple og Microsoft tilbyr annonsører å spore brukere via **annonse-ID** (AD-ID). Ved å benytte denne sporingsløsningen kan

[26] En IP-adresse kan indirekte kobles til en person, og IP-adresser behandles derfor som personopplysninger i tråd med europeisk personvernlovgivning. I USA er imidlertid ikke IP-adresser å regne som personopplysninger og den amerikanske annonseindustrien står derfor mye friere til å benytte IP-adresse til profileringsformål.

27 Adweek, «Google's Latest Role: The Cookie Monster. Ad tech firms are on alert», 11.11.2013, http://www.adweek.com/news/technology/google-s-latest-role-cookie-monster-153712.

annonsørene følge samme bruker fra nett til apper. Microsoft måtte tåle kritikk ved lansering av Windows 10, da det ble kjent at brukerne automatisk ble tildelt en AD-ID ved nedlasting av det nye operativsystemet.[28]

Apples «Unique Device Identifier (UDID), som er en unik identitet tildelt hvert enkelt Apple-produkt, var tidligere tilgjengelig for andre selskaper. Dette er ikke lenger tilfelle. Identiteten er knyttet til Apples «identifikator for annonsører,» (Identifier for advertisers, (IDFA.)). Det er en unik streng med tegn som er tilordnet til hver bruker som benytter en iOS-enhet. For eksempel når annonsene kjøres på Apples annonsering nettverk iAd vil Apple finne ut hvem som får annonsen, og potensielt koble det tilbake til alt vedkommende gjorde andre steder i Apples system. Det er mulig for brukeren å nullstille Apples Advertisement ID. Det er også mulig å slippe målrettet reklame ved å skru av tillatelsen for tilpasset reklame.

Google har tilsvarende annonseidentifikator. Brukeren kan slå av bruken av dette sporingselementet og velge bort målrettet reklame i Googles Play-apps.

Norske medier med innloggingsløsning

- **Schibsted** samler inn informasjon om sine brukere gjennom identitets- og betalingssystemet SPiD**. S**PiD ble innført i 2013 og har 2,3 millioner brukere.
- **Polaris Media** benytter SPiD for sine aviser, der i blant Adresseavisen.
- **Amedia** har innført innloggingstjenesten Aid som selskapet benytter på tvers av sine 60 lokalaviser samt 1881.no, Nettavisen, deler av Blogg.no og en rekke nisjesider. Selskapets annonsenettverk omfatter 2,5 millioner brukere.

Cookie-matching som teknikk for datainnhøsting

Det har i utgangspunktet ikke vært mulig for et selskap å lese innholdet i cookies som tilhører andre selskap. Ved å bruke en teknikk kalt cookie-matching – på norsk kan vi kanskje kalle det «kapselkobling» – er dette imidlertid mulig. Cookie-matching er en avgjørende funksjonalitet i forbindelse med sanntidskjøp av unike brukere på børs (real-time bidding). For at kjøpersiden skal kunne avgjøre hvorvidt de vil legge inn et bud, og ikke minst *hvor mye* de vil by, må de vite hvem brukeren er. Cookie-matching gjør det mulig å koble sammen cookie-data som befinner seg i databaser hos to ulike selskap. Når en bruker legges ut for salg gir børsen kjøperplattform tilgang til cookie-data om denne brukeren. For eksempel så legger Doubleclick ut bruker 1234 for salg med tilhørende cookie-data som forteller at brukeren har besøkt nettstedene *pets.com* and *pinknews.co.uk*. Kjøperplattformen AppNexus gjennomfører en cookie-matching som viser at bruker 1234 er den samme som bruker xys som de allerede har en brukerprofil på. Appnexus vet at denne brukeren har besøkt *foxnews.com* og *cnn.com*. Etter gjennomføring av cookie-matchingen har Appnexus fått ytterligere informasjon om bruker xyz som de kan oppdatere brukerprofilen med.[29]

Cookie-matching fungerer altså ikke utelukkende som en metode for å kunne identifisere og estimere rett verdi på en bruker i forbindelse med sanntidskjøp. Forskere som har undersøkt hvordan cookie-matching brukes, hevder at teknikken også benyttes som en metode for datahøsting for å bygge opp brukerprofiler. Google på sin side sier imidlertid i sine brukervilkår at de ikke tillater at cookie-matching brukes for dette formålet.[30] Datatilsynet vil se nærmere på bruk av cookie-matching for å få større innsikt i hvordan denne teknikken fungerer og til hvilke formål den benyttes i forbindelse med sanntidskjøp.

Nettvarder – kobler sammen den analoge og den digitale verden

Annonseindustrien har hittil manglet en måte å koble folks aktiviteter ute i den virkelig verden med folks aktiviteter på nett. Bruk av beacons (på norsk «nettvarder») gjør dette mulig. Beacons eller nettvarder er en liten sensor som benytter blåtann-teknologi for å

[28] TechRepublic, «Windows 10 violates your privacy by default, here's how you can protect yourself», 4.8.2015, http://www.techrepublic.com/article/windows-10-violates-your-privacy-by-default-heres-how-you-can-protect-yourself/

29 Olejnik, Lukasz, Tran Minh-Dung og Claude Castelluccia, Selling Off Privacy at Auction», 2013, HAL Id: hal-00915249, https://hal.inria.fr/hal-00915249

30 https://developers.google.com/ad-exchange/rtb/cookie-guide

sende informasjon som kan mottas når en person kommer i nærheten av dem. Bruk av teknologien krever at brukeren har utstyr som kan lese den utsendte informasjonen.[31] Ved å plassere ut beacons er det for eksempel mulig å registrere hvilke produkter kundene ser på i butikkhyllene. Denne informasjonen kan plukkes opp av en app i en smarttelefon, og kan senere benyttes til å sende brukeren målrettet reklame for det produktet vedkommende så på i butikken. Ved å koble sammen beacons i store nettverk kan de fungere som en analog cookie som sporer brukeren på hans eller hennes ferd mellom butikker, restauranter, treningssenter og museer. Tomas Walle Jensen i Unacast, et norsk selskap som er verdensledende innen beacons-teknologi uttaler følgende på selskapets hjemmesider:

«Retailers and brands have a limited customer view today. As soon as the customer leaves their store, he or she becomes invisible, until they resurface in the same location. What the customer did before and after the visit is unknown. By working with Unacast and sharing data into the Unacast PROX network, retailers and brands can ensure that in-store campaigns can take into account the total physical profile, thus fulfilling the promise of proximity as the offline cookie.»[32]

Massiv tilstedeværelse av tredjeparter

Når vi går inn på en nettside, så besøker vi ikke bare ett selskap, men mange selskap på én gang. I tillegg til publisisten som eier siden, er annonsebørser, kjøper- og selgerplattformer, annonsenettverk, analyseselskap, datahåndteringsplattformer og datameglere til stede med ulike sporingsverktøy for å samle inn opplysninger om hva vi ser på. Aktørene som er der uten å være publisisten som eier siden, kalles tredjepartsaktører.

En nettavis kan deles inn i to deler:

Publisistens del: Denne delen av nettstedet består av det journalistiske innholdet i avisen. Her bestemmer publisisten hvilke tredjepartsaktører som får tilgang og hvilke personopplysninger disse aktørene samler inn. Disse tredjepartsaktørene behandler ofte personopplysninger på vegne av publisisten og har derfor status som databehandlere.

> *«Et nettsted er ikke kun ett selskap. Et nettsted er et flere hundre selskaper som alle sammen vet hvor du er og hva du ser på.»*
>
> *Chris Babel, TRUSTe[33]*

Det kan for eksempel være analyseselskap som er til stede på sidene for å levere statistikk og analyse til nettstedseierne slik at de kan få kunnskap om hvordan brukerne benytter tjenesten deres. Opplysningene analyseselskapet henter inn brukes også til å brukertilpasse innhold og annonsering. Publisisten har også avtaler med annonsebørser og kjøperplattformer. Eksempel på selskap som brukes av publisistene er Cxense, Google Analytics, Google Doubleclick, TNS, Rubicon og Appnexus.

Markedsførernes/annonseselgernes del: Denne delen av nettstedet består av annonseflater som er satt av til eksterne aktører. Her slippes markedsførerne til. Publisisten kan ha en avtale med ett eller flere mediebyrå/selgerplattformer som kjøper brukere av publisisten på vegne av ulike kunder. I forbindelse med kjøp av brukere og plassering av annonser trekker mediebyråene en hale av andre selskap med seg inn på siden. Disse selskapene er på en måte mediebyråenes tredjeparter, eller tredjepartenes tredjeparter, om du vil. Dette er selskaper de benytter for å måle hvor mange brukere som har klikket på annonsen og til å spore brukere fra ett nettsted til et annet. Publisisten har ikke kontroll over tredjepartsaktørene som befinner seg i den delen av nettsiden som er satt av til annonseflater. Publisisten vet ikke hvilke personopplysninger de samler inn og hvordan de behandles. Eksempel på selskap som benyttes av markedsførerne er Datalogix, Google Doubleclick, Media Math og Dataxu.

Tredjeparter på norske nettaviser

Vi har undersøkt hvilke tredjepartsaktører som er til stede på seks norske nettaviser, og hvor mange informasjonskapsler som blir plassert på nettleseren ved

31 Google har imidlertid utviklet en beacon-teknologi som ikke nødvendigvis krever installering av app. Googles Eddystone er et åpent beacon-format. Et Eddystone beacon-signal kan mottas direkte til apper eller som Eddystone-URL som kan bli brukt av smarttelefoner selv om den ikke har virksomhetens app installert.

32 http://unacast.com/welcome-to-unacast-prox-network/

33 The Economist, «Little Brother, Special Report on Advertising and Technology», 13.09.2014, http://www.ogilvydo.com/wp-content/uploads/2014/09/20140913_SR_MAILOUT.pdf

besøk på disse sidene. Avisene vi har undersøkt er Aftenposten, Dagbladet, Nettavisen, Adresseavisen, Dagsavisen og Drammens Tidende.[34]

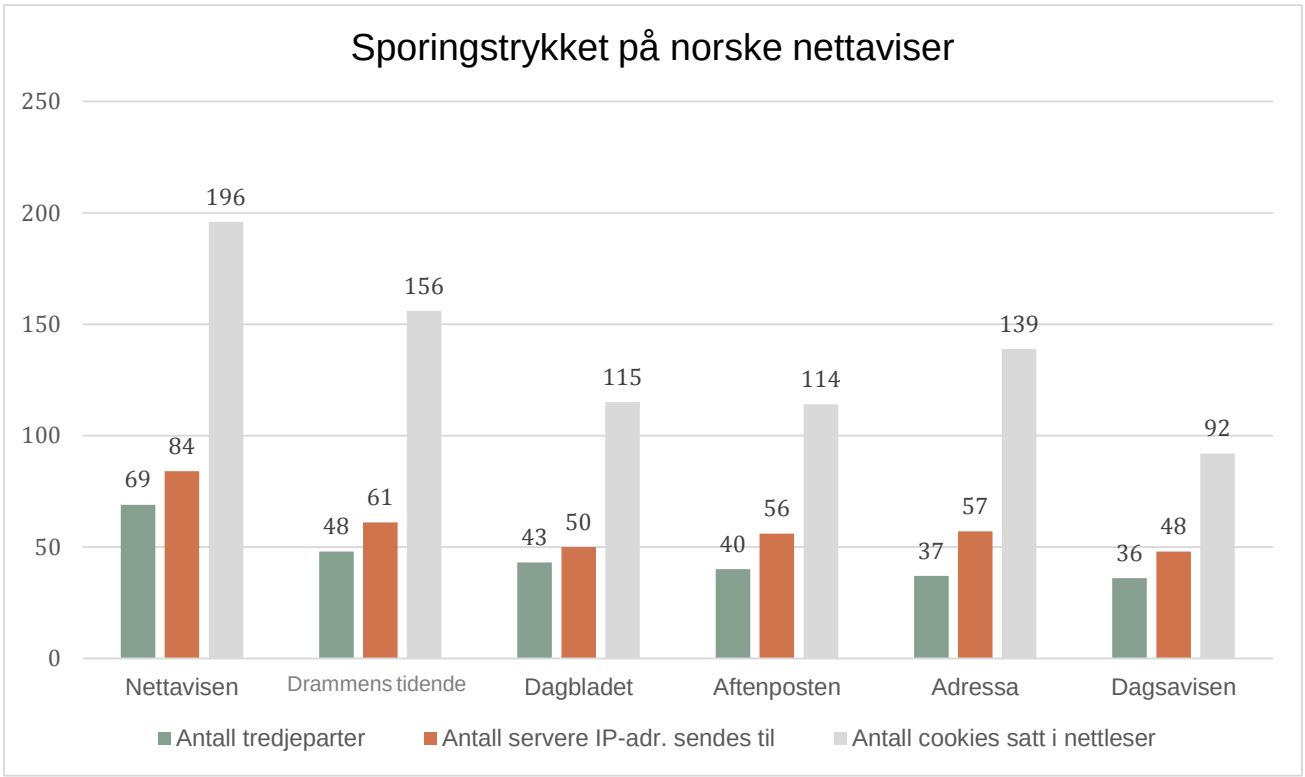
Konklusjonen på undersøkelsen er at tredjepartsaktørers tilstedeværelse er massiv. Det samme er antallet informasjonskapsler som plasseres ut. Mellom 100 og 200 informasjonskapsler ble plassert ut ved besøk på førstesiden til avisene. Eneste avis der det ble plassert ut under 100 informasjonskapsler var Dagsavisen.[35] I gjennomsnitt er 46 tredjepartsaktører til stede på hver av de seks nettavisene vi undersøkte. Til sammen elleve annonsebørser, tolv kjøper- og selgerplattformer, tolv datahåndteringsplattformer, åtte datameglere og tretten dataanalyseselskap samlet inn opplysninger om oss (se vedlegg 2). Opplysningene er i all hovedsak samlet inn av amerikanske selskap. Kun et fåtall er europeiske, for eksempel cXense (norsk), Internet Billboard (tsjekkisk), Semasio (tysk) og Adscale (tysk).

Avisen med flest tredjepartsaktører til stede er Nettavisen med minst 69 ulike selskap inne på siden. Ved hjelp av sporingsbilder (web beacons) sender disse selskapene vår IP-adresse til 84 ulike servere. De samme selskapene plasserer videre 198 informasjonskapsler på nettleseren vår. Drammens Tidende har også mange tredjepartsaktører til stede på siden. 48 selskaper sender vår IP-adresse til 61 servere og plasserer ut 156 informasjonskapsler.

Mangelfull informasjon

Ingen av de seks avisene gir informasjon til publikum om tilstedeværelsen av tredjepartsaktører på sidene sine. Personvernerklæringene gir kun generell og vag informasjon om cookie-bruken.

Nasjonal kommunikasjonsyndighet (Nkom) foretok et tilsyn med cookie-bestemmelsen i 2015.[36] Kontrollen avslørte at kun 19 prosent av de 500 nettstedene tilsynet undersøkte fulgte bestemmelsene.



34 4. og 7. september 2015 gikk vi inn på førstesiden til hver av de seks avisene. Vi benyttet analyseverktøyet Ghostery for å få informasjon om antallet tredjepartsaktører og antallet sporingselementer som ble satt på vår nettleser ved besøk på sidene. Vi har valgt aviser fra alle de tre store norske avishusene (Schibsted, Amedia og Polaris Media), en riksdekkende avis (Dagbladet), en regional avis (Aftenposten) og en lokalavis (Drammens Tidende). I tillegg har vi plukket ut en avis som utelukkende er en nettpublikasjon (Nettavisen).

35 Vi har i denne rapporten ikke foretatt en vurdering av hver enkelt informasjonskapsel og hvor invaderende den er. Informasjonskapslene kan omfatte både førstepartscookies og tredjepartscookies.

36 Nkom er underlagt Samferdselsdepartementet og driver tilsyn med dem som tilbyr post- og teletjenester.

Aller dårligst var mediehusene. Hele ni av ti nyhetssider oppfyller ikke informasjonskravene i loven.[37]

Hvorfor gir ikke nettstedeierne mer detaljert informasjon om tredjepartenes aktiviteter på siden? Er publisistene bekymret for at vi, hvis vi kjente til hva som foregikk i kulissene, ville stilt kritiske spørsmål eller vegret oss for å bruke tjenesten?

En forklaringer kan som nevnt være at de ikke full oversikt og kontroll over hvilke selskaper som er til stede i de delene av nettjenesten som er satt av til annonseflater. Enkelte publisister overlater derfor til brukeren å unngå å bli sporet, ved å informere om at brukere kan gjøre innstillinger på maskinen slik at ikke informasjonskapsler plasseres i nettleseren.

Men å bruke denne innstillingen hjelper bare mot noe av sporingen. Selv om brukerne har beskyttet seg mot informasjonskapsler i nettleseren, kan tredjepartsaktører følge med på dem ved å benytte andre sporingsverktøy, som for eksempel de tidligere nevnte digitale fingeravtrykk.

Å bli sporet på nett er ikke noe du velger. Default-løsningen er nesten alltid å bli sporet. Ønsker man å reservere seg fra sporing («opt-out»), er det sjelden godt tilrettelagt for dette. Internet Advertising Bureau (IAB) har opprettet siden Youronlinechoices.eu der brukere kan be selskap slutte å spore dem med informasjonskapsler. Her kan brukere klikke på de selskapene de vil eller ikke vil skal følge dem, eller klikke på den grønne knappen for å «slå på alle selskaper» eller den røde for å «slå av alle selskaper». Det er imidlertid kun de aller mest bevisste forbrukerne som vil oppsøke denne muligheten for å reservere seg. De fleste forbrukere aner ikke at de blir sporet og vil benytte løsningen som tilbys.

37 Nasjonal kommunikasjonsmyndighet, «Tilsynsrapport. Tilsyn etter Lov om elektronisk kommunikasjon § 2-7 b. Bruk av informasjonskapsler/cookies», 2015, http://www.nkom.no/aktuelt/nyheter/_attachment/18410?_ts=14dd7a6fc04

Bygging av profiler

Annonseindustrien og publisistene bruker opplysningene som samles inn ved hjelp av informasjonskapsler, innloggingsløsninger, nettvarder og digital fingeravtrykk til å utvikle profiler. Profilene danner grunnlag for å personalisere innhold og reklame. I dette kapittelet vil vi se på hvilke opplysninger profilene inneholder og hvor mye de er verdt.

Hva er en profil?

En profil er satt sammen av *antagelser* om et individs eller en gruppe av individers preferanser, evner eller behov. Antagelsene er utledet gjennom blant annet analyse av enkeltindividers surfehistorikk, oppdateringer i sosiale medier, leste nyhetsartikler, produkter kjøpt på nett og registrerte kundeopplysninger. Antagelser regnes også som personopplysninger, selv om det ikke er faktiske opplysninger. Profilering handler i dag i stor grad om å benytte Big Data-analyse for å se etter mønster og sammenhenger i store datasett som kan brukes til å forutsi forbrukeratferd.

> *«We now have a stalker economy where customers become products.»*
>
> *Al Gore*[38]

Googles globale dominans

Google er til stede på 87 prosent av alle norske nettaviser (kilde: trackography.org). Google er lengst fremme i å innhente kunnskap om den enkelte av oss. Google benytter mange ulike tjenester og teknologier for å innhente kunnskap om brukerne:

- DoubleClick
- Google Analytics
- Google tag manager
- Google search
- Google gmail
- Google maps
- Google streetview
- Adsense
- Adwords
- Youtube

Google henter inn opplysninger om den enkelte både direkte og indirekte. Selskapet samler inn opplysninger direkte fra brukerne gjennom tjenester som Gmail, søk, Youtube og kart, og indirekte som tredjepartsaktør (på millioner av nettsteder verden over) via tjenester som DoubleClick, Analytics, Adsence og Adwords.

Det er av sentral betydning at profiler benyttes som *grunnlag for å treffe beslutninger om den enkelte*. Det er et viktig personvernprinsipp at beslutninger om den enkelte skal fattes på grunnlag av korrekte data. Det er viktig at den enkelte derfor har mulighet til å få innsyn i opplysningene som samles inn, for å kunne kontrollere at opplysningene er korrekte slik at man ikke blir utsatt for feil avgjørelser. I dag bygges brukerprofiler opp om oss i det skjulte, av selskaper vi ikke vet eksisterer. Det gjør det utfordrende for den enkelte å praktisere sine personvernrettigheter. Dette vil vi diskutere ytterligere i kapittel syv.

Profilbygging er ikke en prosess som har en begynnelse og slutt, det er en kontinuerlig aktivitet. Alle aktørene i verdikjeden, annonsørene, mediebyråene, annonsebørsene, datatilbyderne og publisistene oppdaterer *hele tiden våre profiler med nye data* som samles inn fra våre analoge og digitale liv. Vi vet ikke hvor lenge de store internettaktørene som Google,

[38] Pando, «Al Gore says Silicon Valley is a «stalker economy», 11.06.2014, https://pando.com/2014/06/11/al-gore-says-silicon-valley-is-a-stalker-economy/

Yahoo! og Microsoft lagrer våre data og hvor omfattende våre personprofiler blir etter hvert. Volumet av opplysninger er antagelig enormt. En undersøkelse gjennomført av Dagens Næringsliv viste at Schibsted i løpet av et år hadde registrert 136 000 datapunkter om en unik bruker. [39]

Aktørene har ulike formål med profilbyggingen: Annonsører og markedsførere bygger profiler for å skille attraktive kunder fra mindre attraktive kunder, slik at reklamen blir mest mulig effektiv. Publisister lager profiler for å tiltrekke seg annonsører til sine annonseflater. Jo mer detaljerte og attraktive brukerprofiler de kan tilby, jo mer penger er annonsørene villig til å betale. Datatilbyderne høster inn opplysninger og lager profiler som de selger til både annonsører og publisister som ønsker å berike profilene sine med ytterligere opplysninger.

Mange markedsføringsselskap og publisister hevder at brukerprofilene de bygger opp kun inneholder anonyme opplysninger. Dette kan være riktig i møte med amerikansk lovgivning, der kun *direkte identifiserende* opplysninger regnes som personopplysninger. Amerikanske selskap kan for eksempel lagre IP-adresser i brukerprofilene uten at dette regnes som personopplysninger. Det holder å ha fjernet opplysninger som navn, adresse og e-post. Norsk og europeisk personvernlovgivning ser ikke slike profiler som anonyme på samme måte. I europeisk lovgivning er også *indirekte identifiserbare* opplysninger definert som personopplysninger, dette gjelder for eksempel IP-adresse eller data innhentet ved hjelp av informasjonskapsler (cookies).

Mange norske aktører hevder også at de bare benytter anonyme data til profilering og segmentering av brukere. Hvorvidt dette virkelig er tilfelle eller ikke, har det ikke vært mulig for Datatilsynet å bringe på det rene. Det er imidlertid vårt inntrykk at mange virksomheter tror at pseudonyme data er det samme som anonyme data.

Pseudonyme data inneholder fortsatt identifiserende opplysninger, selv om navn og adresse er fjernet, og er derfor å betrakte som personopplysninger. Dette vil bli ytterligere kommentert i kapittel 6.

Innholdet i profilene

En brukerprofil er satt sammen av data som forteller mest mulig om den enkelte. Jo mer data som finnes i en profil, jo høyere verdi har den i markedet. Verdien avhenger som vi skal se også av *hvilke* opplysninger som finnes i profilen.

Profilen inneholder som nevnt ikke nødvendigvis direkte identifiserende kjennetegn som navn, adresse og e-post, men opplysningene er knyttet til et unikt nummer som gjør det mulig å følge samme bruker over tid og slik berike profilene med nye opplysninger etter hvert som de strømmer inn.

Aktørene i bransjen bygger opp profilene på omtrent samme måte, med enkelte faste innholdskategorier. En brukerprofil er vanligvis bygget opp av følgende datakategorier:[40]

Demografiske data: Dette er bakgrunnsopplysninger om brukeren. Det kan være opplysninger om navn, adresse, kjønn, alder, sivilstatus, postnummer, utdanningsnivå, ansettelsesforhold (type bransje), inntekt, antall familiemedlemmer i husholdet, antall barn, alder på barn, om man er hytteeier, hvilken bil man eier, etnisitet, religiøs tilhørighet. Demografiske data samles gjerne inn i forbindelse med at brukere registrerer seg for å ta nye tjenester i bruk. Demografiske data kan også utledes gjennom analyse av cookie-data eller fra oppdateringer på sosiale medier. Det er dessuten vanlig å benytte statistiske data for å bygge opp et bredt sett med bakgrunnsvariabler om enkeltbrukere. For eksempel kan antatt partitilhørighet knyttes til en brukerprofil basert på postnummeret til vedkommende.

Lokasjonsdata: Dette er opplysninger som forteller hvor brukeren befinner seg, hentet inn via GPS, wifi og IP-adressen. Opplysninger om hvor brukeren befinner seg er svært nyttig for annonsørene i målrettingen av reklame. For eksempel er det nyttig å vite hvilke brukere som befinner seg et sted det regner når annonsører skal målrette reklame for paraplyer og regntøy.

39 Dagens Næringsliv, «Dette vet mediekjempene om oss», 19.10.2014, http://www.dn.no/etterBors/2014/10/19/2057/Kommentar/dette-vet-mediekjempen-om-oss

40 Rao, A., F. Schaub og N. Sadeh, «What do they know about me? Contents and concerns of Online Behavioral Profiles», Carnegie Mellon University, 2014, https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab14011.pdf og IAB Europe, «Programmatic Trading. An IAB Europe White Paper», 2014, http://www.iabeurope.eu/files/8614/0776/0957/IAB_Europe_Programmatic_Trading_White_Paper_July_2014_v2.pdf

Selskaper som opererer i Norge og bygger brukerprofiler

- **eXelate** – eid av Oracle og et av verdens største selskap for innsamling og analyse av tredjepartsdata. Selskapet sier de samler inn brukerdata om 200 millioner unike brukere i måneden gjennom å være til stede med cookies på hundrevis av nettsteder. eXalte sporer unike brukere for å se hvem som er på utkikk etter ny bil eller som er opptatt av sportsutstyr.
- **BlueKai**, konkurrent til eXelate, hevder de har profiler på 700 millioner unike brukere. Basert på opplysninger om nettatferd predikerer de hvilke type kjøp det er sannsynlig at brukerne vil foreta.
- **Schibsted:** Via sin innloggingsløsning som omfatter flere aviser og finn.no innhenter selskapet kunnskap om blant annet kundenes leservaner. Denne kunnskapen kan de bruke til å utlede ytterligere kunnskap om brukeren, for eksempel om interesser og hobbyer. I tillegg har avisene demografiske data om leseren, som for eksempel brukerens kjønn, alder og bosted. Alt dette er svært verdifulle data å tilby annonsører som vil nå helt spesifikke målgrupper.

Tekniske data: Dette er opplysninger knyttet til brukerens datamaskin, smarttelefon, nettbrett og eventuelt andre enheter som benyttes for koble seg opp til internett. Eksempel på tekniske opplysninger er IP-adresse, operativsystem (som Windows 7), nettleser (for eksempel Internet Explorer 10) og skjermoppløsning. [41]

Fra tekniske data, særlig IP-adressen, er det mulig å utlede mye annen informasjon om brukeren som navn, postadresse, mobilnummer og historikk over kjøp av varer på nett. Tekniske data blir også brukt til å vurdere kjøpekraften til brukere. Det er blant annet avdekket at Mac-brukere som handler på reisenettsteder må betale mer per natt for hotellrom enn det PC-brukere må.[42]

Interessedata[43]: Dette er opplysninger om interesser og holdninger til brukeren. Opplysningene er vanligvis utledet gjennom analyse av data innhentet ved hjelp av informasjonskapsler som viser hvilke nettsteder og annonser brukeren har besøkt, gjennom uker, måneder eller år. Analyse av søke- og surfehistorikken gir et rikt bilde av den enkelte. Den kan for eksempel avdekke interesse for helse- eller slankeprodukter (søk på søvnproblemer, smerter, slankekurer), interiør, reiser (bestilt hotell på Mallorca og langhelg til Paris) og politikk (klikket liker på Facebook-innlegget til Jonas Gahr Støre).

Prediktive data: Det gjøres analyser for å beregne seg frem til sannsynligheten for at brukeren vil kjøpe bestemte produkter med utgangspunkt i alle opplysningene som samles inn. Prediksjonene gjøres ved å analysere store mengder aggregerte data, men resultatet av analysen kobles til individuelle brukerprofiler. Eksempel på en teknikk som brukes til å bygge profiler er tvilling-analyse: Sannsynligheten for at et individ vil oppføre seg på en bestemt måte kan predikeres på bakgrunn av tidligere oppførsel. Denne prediksjonen kan overføres til andre individer som deler de samme karaktertrekkene. Eksempel på prediksjonsdata funnet i én og samme profil er: «personlig helse: 70-90 prosent» som indikerer sannsynligheten for at vedkommende vil foreta et kjøp av helserelaterte produkter i nær fremtid, «innenlands flyreiser – 70-90 prosent» indikerer sannsynligheten for at samme person vil kjøpe flybilletter og «bilforsikring på internett – 16-17 prosent» indikerer sannsynligheten for at brukeren vil kjøpe bilforsikring på nett innen kort tid.[44]

Atferd: Dette er opplysninger om brukerens livsstil og personlighet. Brukerne segmenteres i ulike kategorier på bakgrunn av på analyse av aggregerte data hentet ved å

41 Rao, A., F. Schaub og N. Sadeh, «What do they know about me? Contents and concerns of Online Behavioral Profiles», Carnegie Mellon University, 2014, https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab14011.pdf

42 Washington Post, «On Orbitz, Mac Users Steered to Pricier Hotels», 23.08.2012, http://www.wsj.com/articles/SB10001424052702304458604577488822667325882

43 På engelsk kalles denne gruppen data for psychographic data

44 Rao, A., F. Schaub og N. Sadeh, «What do they know about me? Contents and concerns of Online Behavioral Profiles», Carnegie Mellon University, 2014, https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab14011.pdf

bruke informasjonskapsler, sosiale medier, kunderegister, kjøpehistorikk og så videre. Brukerne tildeles merkelapper som indikerer deres forbruksmønster og kjøpekraft, eksempelvis «aktiv livsstil og SUV», «hjemmelaget mat», «barna først» og «urban, singel og lavt forbruk». [45] Det finnes også selskaper som bruker opplysninger hentet inn fra informasjonskapsler til å predikere folks personlighet basert på Myers-Briggs personlighetstypologisering (ekstrovert, introvert, leder, kommunikator og så videre). Selskapet V12 selger brukerprofiler til annonsører og hevder å ha tildelt en personlighetstype til 85 prosent av alle forbrukere i USA, basert på Myers-Briggs' forskjellige typer.[46]

Livshendelser: Dette er opplysninger om viktige hendelser som påvirker folks kjøpemønster, eksempelvis graviditet, nybakte foreldre, på flyttefot, nygift, og så videre. Slike opplysninger er ofte utledet gjennom analyse av nettatferd. Surfehistorikken viser at for eksempel at brukeren har lest tester av barnevogner og artikler om helse og svangerskap.

Hva er en profil verdt?

Tror du annonsørene vil betale 100 kroner eller 1 krone for surfehistorikken din? Systemet med auksjonering av profiler i sanntid gjør det mulig å finne ut hvor mye en profil er verdt. Forskere har avdekket at annonsører og mediebyrå betaler mer for brukere med kjent surfehistorikk, altså brukere som har informasjonskapsler installert i nettleseren og som selskapene derfor kjenner fra før, enn brukere som er nye for reklamekjøperne, for eksempel fordi de har slettet informasjonskapsler fra nettleseren.[47] Annonsører betaler aller mest for brukere der de kan drive gjentatt eksponering for reklame («re-targeting»), det vil mulighet til å plassere skoreklame til en bruker de vet har sett på sko eller blitt eksponert for skoreklame på et annet nettsted. Forskerne fant ut at prisen kan være så mye som to til tre ganger høyere for profiler som tillater gjentatt eksponering. Studien viste også at ikke bare surfehistorikken, men også hvilke *typer* sider brukeren besøker påvirker prisen. Annonsører betaler mer for brukere som besøker nyhetssider som Fox News enn nettsider om kampsport, for eksempel. Tilsvarende gir surfing på e-shoppingtjenester og biler høyere priser enn surfing på sportssider. Studien avdekket også at brukere geografisk plassert i USA hadde høyere verdi enn brukere i Europa. Dette skyldes trolig både at profilene til amerikanske brukere inneholder mer data, og/eller at det er flere annonsører som konkurrerer om å nå amerikanske brukere enn det er annonsører som vil ha fatt i europeere.

Prisen for en profil er ikke spesielt høy. Gjennomsnittsprisen for et bud på en bruker er 0.004 kroner, ifølge forskere bak studien referert til over. Prosjektet «How much is your data worth» i regi av Financial Times kom frem til den samme summen. I sistnevnte prosjekt kom det frem at også enkelte livshendelser bidrar til å øke prisen annonsører er villige til å betale for en bruker. Det ble lagt inn høyere bud på profiler som viste at brukeren nettopp hadde fått barn, flyttet eller skilt seg. Tilgang til opplysninger om at en kvinne er gravid i sjette måned øker prisen til nesten én krone (90 øre). Jo mer intime opplysninger annonsøren får tilgang til, for eksempel informasjon om helsetilstand eller inntak av bestemte legemidler, jo høyere pris er annonsører villige til å betale. Opplysninger om medisinbruk selges for to kroner per person, ifølge Financial Times.[48] Det er uheldig fra et personvernperspektiv hvis den høye betalingsvilligheten for sensitive opplysninger stimulerer til mer utstrakt innhenting og salg av slike opplysninger.

45 Turow, Joseph, «The Daily You. How the New Advertising Industry Is Defining Your Identity and Your Worth», Yale University Press, New Haven and London, 2011.

46 Bizreport, «Platform creates customer profiles using Myers Briggs types», 19.04.2012, http://www.bizreport.com/2012/04/platform-creates-customer-profiles-using-myers-briggs-types.html

47 Olejnik, Lukasz, Tran Minh-Dung og Claude Castelluccia, «Selling Off Privacy at Auction», 2013, HAL Id: hal-00915249, https://hal.inria.fr/hal-00915249

48 Financial Times, «How much is your personal data worth?», 12.06.2013.

Hva sier loven?

Vi har sett en eksplosjonsartet vekst i antall transaksjoner der det handles med personopplysninger for å gjøre markedsføring mer målrettet. I dette kapittelet skal vi se nærmere på det rettslige rammeverket for disse transaksjonene.

Personopplysnings-loven

Den norske personopplysningsloven regulerer behandling av personopplysninger. Dette er en generell lov som gjelder både overfor privat og offentlig sektor. Den ble til som følge av EUs personverndirektiv, som Norge er bundet av gjennom EØS-avtalen.

Personopplysningsloven har som formål «å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger». Loven er et rettslig rammeverk som den som behandler personopplysninger må holde seg innenfor.

Når gjelder loven?

Personopplysningsloven regulerer behandling av personopplysninger. For at loven skal gjelde i forbindelse med atferdsbasert eller tilpasset markedsføring på nett, kreves det altså at de dataene som blir behandlet helt eller delvis er personopplysninger. Loven definerer personopplysninger som «opplysninger og vurderinger som kan knyttes til en enkeltperson».[49]

I prinsippet omfattes all tenkelig informasjon som kan fortelle oss noe om en person av begrepet. I en nettverkstilkoblet verden vil dette omfatte mye av den informasjon som samles når vi bruker internett, slik som hvilke nettsteder vi besøker, hva vi søker etter, og hvordan vi bruker de ulike tjenestene.

For at informasjonen som samles inn i forbindelse med nettaktivitet skal kunne betraktes som personopplysninger, må den kunne knyttes til en enkeltperson. Dette er ofte det springende punktet. Med begrepet enkeltperson menes en person som er identifisert eller identifiserbar. Man må enten vite eller kunne få rede på hvem personen er.

I vurderingen av om personen lar seg identifisere, skal det tas i betraktning alle hjelpemidler som det er rimelig å tro at noen – det være seg det behandlingansvarlige selskapet eller andre aktører – kan komme til å bruke for å identifisere personen. I forarbeidene til den norske personopplysningsloven nevnes som eksempel at «den som registrerer besøk på sin hjemmeside på nettet, får tilgang til en anonym elektronisk identitet som bare kan knyttes til en identifiserbar enkeltperson dersom man har tilgang til opplysninger som vedkommendes internettleverandør sitter inne med. Men selv denne begrensede identifikasjonsmuligheten er tilstrekkelig til at de elektroniske sporene er «personopplysninger».»[50]

Det rådgivende organet Artikkel 29-gruppen har i en uttalelse fra 2010 lagt til grunn at data som samles inn og behandles i forbindelse med atferdsbasert eller tilpasset markedsføring på nett må betraktes som personopplysninger.[51],[52] Førende for dette synet er at atferdsbasert markedsføring normalt baserer seg på innhenting av IP-adresser eller unike identifikatorer gjennom bruk av informasjonskapsler eller andre teknikker. Dette gjør selskapene i stand til å følge en bruker over tid, og å skille brukerne fra hverandre. Informasjonen som samles forteller noe om personens karakteristika og atferd, og den brukes til å påvirke personen gjennom markedsføringen. Det må også tas i betraktning at dataene på et gitt tidspunkt kan kobles til direkte identifiserbar informasjon, for eksempel ved opprettelse av brukerkonto eller som følge av en stadig økende mengde data, som i seg selv kan avsløre identiteten.

Datatilsynet deler dette synet. Så lenge dataene som samles inn er egnet til å skille brukerne fra hverandre, må de sees på som personopplysninger. Atferdsbasert

49 For en bredere gjennomgang av personopplysningsbegrepet se Datatilsynets Big Data rapport: http://www.datatilsynet.no/Nyheter/2013/Big-Data-rapporten/

50 Ot. Prp. Nr. 92 (1998-1999) side 101

51 Artikkel 29-gruppen er et organ som er opprettet med hjemmel i personverndirektivets artikkel 29. Det avgir blant annet tolkningsuttalelser med sikte på harmonisering av direktivet i medlemslandene.

52 Opinion 2/2010.

markedsføring er innrettet slik at den enkelte bruker gjenkjennes når han eller hun besøker et nettsted, slik at markedsføringen kan tilpasses. Man må basere seg på at det kan la seg gjøre å identifisere den enkelte bruker. Dataene og personene bak dem er ikke anonyme.

Lovens geografiske virkeområde

Loven gjelder for behandlingsansvarlige som er etablert i Norge.[53] Med «behandlingsansvarlig» menes i lovens forstand den som bestemmer formålet med behandlingen av personopplysninger og hvilke virkemidler som skal brukes[54]. Den behandlingsansvarlige er pliktsubjektet etter loven – den som plikter å etterleve lovens krav. I denne rapporten vil vi gjerne bruke ordet selskap eller foretak istedenfor begrepet behandlingsansvarlig ettersom det stort sett er selskaper eller andre former for foretak som står bak innsamlingen og bruken av data til markedsføringsformål via internett.

Det avgjørende er hvilken tilknytning selskapet som står bak behandlingen av personopplysninger har til Norge. Selskapet må være etablert her for at loven skal gjelde. Med «etablert» menes at det ansvarlige selskapet må utøve en eller annen form for aktivitet i Norge innenfor en forholdsvis fast struktur. [55] Aktiviteten trenger ikke utøves gjennom et eget og selvstendig rettssubjekt i Norge. Det sentrale er om selskapet har tilstrekkelig tilknytning til Norge til å at det må sies å være etablert her ut fra en alminnelig språklig forståelse.

Etableringskriteriet må tolkes i lys av personverndirektivet

Etter direktivet er det ikke tilstrekkelig at den behandlingsansvarlige er etablert i Norge – altså bedriver aktivitet eller virksomhet i Norge. Det avgjørende er om den konkrete behandlingen av personopplysninger man står overfor skjer i kontekst av den aktivitet selskapet har i Norge. Det må altså være en naturlig sammenheng mellom etableringen i Norge og personopplysningsbehandlingen for at loven skal gjelde. Dette må innfortolkes også i den norske personopplysningsloven.

I praksis kan det være vanskelig å avgjøre om den behandlingsansvarlige er etablert i Norge. Et viktig eksempel fra rettspraksis er den såkalte Google-dommen, der EU-domstolen kom til Google Inc, som står bak og driver Googles søkemotor, måtte betraktes som etablert i Spania. [56] Det avgjørende for domstolen var at Google-konsernet har etablert et selskap i Spania – nemlig Google Spain. Dette selskapet står for salg og promotering av Googles kommersielle markedsføringsaktiviteter, herunder salg av annonseplass på nettsiden for søkemotoren. Domstolen mente at søkemotoren og markedsføringsaktiviteten måtte sees i sammenheng. Søkemotoren drives kommersielt med sikte på å tjene penger, blant annet som en plattform for annonser. Google Incs drift av søkemotoren har således en klar forbindelse til Google Spains aktivitet, og motsatt. Følgelig kom domstolen til at når Google Inc gjennom sin søkemotor behandler opplysninger om personer i Spania, så skjer det i kontekst av markedsføringsaktivitet Google har i dette landet. Selskapet var følgelig bundet av direktivet til å følge spansk personopplysningslov.

Datatilsynet har lagt til grunn at det samme gjelder for Google i Norge, ettersom selskapet også her har etablert et selskap – Google Norway AS – som har som vedtektsfestet formål å frembringe salg av og markedsføre internett-annonsering.

Hvis det behandlingsansvarlige selskapet ikke er etablert i Norge, men det er etablert i et annet EU/EØS-land, gjelder det landets lov ved behandlingen av personopplysninger.

Dersom det behandlingsansvarlige selskapet ikke er etablert i EØS-området, følger det av personopplysningsloven at loven likevel gjelder dersom selskapet benytter hjelpemidler i Norge til behandlingen av personopplysninger. Ifølge forarbeidene sikter begrepet «hjelpemiddel» her til all slags utstyr som kan brukes til å behandle personopplysninger. [57] Et viktig unntak er imidlertid hjelpemidler som brukes til å overføre opplysningene via Norge – det vil si ren transitt av opplysninger gjennom norske nett.

Det fleste av oss bruker i dag mobiltelefon, PC eller nettbrett til våre internettbaserte aktiviteter. Mye av denne aktiviteten blir registrert, lagret og videre behandlet blant annet med sikte på profilbygging og tilpasset markedsføring. Det er usikkert hvor langt hjelpemiddelkriteriet strekker seg her. Uttalelser i forarbeidene tilsier at slikt utstyr må regnes som

53 jf. § 4 første ledd første punktum.
54 Se § 2 nr. 4.
55 Ot.prp.nr. 92 (1998-1999) side 105-106.
56 Avsagt av EU-domstolen i sak C-131/12.
57 Ot.prp. nr. 92 (1998-1999) side 106.

hjelpemiddel. Artikkel 29-gruppen har også basert seg på at en persons PC er et hjelpemiddel («equipment») i direktivets forstand[58].

Det springende punktet for om loven gjelder, er imidlertid om selskapet som står bak innsamlingen av data, faktisk benytter personens PC, mobiltelefon eller liknende. Her må det antakelig kreves at utstyret på et eller annet vis utnyttes til innsamlingen. Et eksempel på et slikt tilfelle er hvis det plasseres en informasjonskapsel på PC-en. Her utnyttes utstyret mer aktivt som ledd i innsamlingen. Artikkel 29-gruppen har argumentert for at slik utnyttelse av utstyret utløser anvendelse av loven. Tilsvarende mener Artikkel 29-gruppen at bruk av JavaScript eller liknende programmer på brukerens PC kan medføre at hjelpemiddelkriteriet er oppfylt.

Det er ikke avklart gjennom rettspraksis hvor langt loven gjelder for virksomheter som ikke er etablert innenfor EØS.

Rettslig grunnlag for å behandle personopplysninger til markedsføringsformål

Personopplysningsloven angir ulike rettslige grunnlag for behandling av personopplysninger.[59] Dersom sensitive personopplysninger skal behandles, kreves det i tillegg at et av de rettslige grunnlagene i § 9 er til stede.[60]

Det sentrale spørsmålet er om behandlingen av opplysningene er betinget av at den enkelte (i loven kalt den registrerte) samtykker, eller om behandlingen kan gjøres uten samtykke. Som hovedregel må det kreves samtykke. Det vil imidlertid kunne være unntak hvor behandlingen må sees på som lovlig ut i fra øvrige rettsgrunnlag i loven.[61] Det er særlig to alternative rettsgrunnlag til samtykke som i denne sammenheng er av interesse, og som vi skal se litt nærmere på:

Behandlingen av personopplysninger som er nødvendig for å oppfylle en avtale med den registrerte

Det kan hevdes at bruk av ulike internettbaserte tjenester – for eksempel sosiale medier – representerer en slags gjensidig kontrakt der den enkelte får tilgang til og kan bruke tjenesten mot å bli eksponert for reklame (personopplysningsloven § 8 a). Og i forlengelsen av dette at behandlingen av personopplysninger for å tilpasse markedsføringen til den enkelte er en nødvendig del av denne kontrakten. Den enkelte betaler da indirekte for tjenesten ved hjelp av sine personopplysninger.

Dette synspunktet kan ikke sies å ha fått nevneverdig gjennomslag. Artikkel 29-gruppen har for eksempel klart uttalt om den tilsvarende bestemmelsen i personverndirektivet artikkel 7 (b) at den ikke er anvendelig for profilbygging.[62] Det må også gjelde der formålet med profilbyggingen er å gi atferdsbasert reklame. Det sentrale her er at slik behandling av personopplysninger ikke kan betraktes som strengt nødvendig for leveransen av tjenesten. At atferdsbasert markedsføring er en nyttig og profitabelt, betyr ikke er at kravet til nødvendighet er oppfylt.

Balansetesten i § 8 f

Personopplysningsloven § 8 f er en bestemmelse som fastslår at en behandling av personopplysninger skal være nødvendig for at den behandlingsansvarlige skal kunne ivareta en berettiget interesse, med mindre hensynet til den registrertes personvern overstiger denne interessen.

Den omtales gjerne som en balansetest. Den kommersielle interessen som ligger i å bedrive tilpasset markedsføring er aktverdig og berettiget. Imidlertid må hensynet til privatlivet tillegges betydelig vekt i avveiningen mot kommersielle interesser.[63] I tillegg må behandlingen være nødvendig. I kravet til nødvendighet ligger at den aktuelle behandlingen er den minst inngripende fremgangsmåten for å ivareta interessen (subsidiaritet), og at behandlingen samlet sett er forholdsmessig.

---

[58] Working document on determining the international application of EU data protection law to personal data processing on the internett of NON-EU based websites.

[59] Jf. § 8.

[60] Se definisjon av sensitive personopplysninger i lovens § 2 nr. 8.

[61] For en bredere gjennomgang se Fredrik J. Zuiderveen Borgesius, Personal data processing for behavioral targeting: which legal basis?, International Data Privacy Law 2015 vol.5 no. 3.

[62] Opinion 6/2014 side 17.

[63] Se Ot.prp.nr. 92 (1998-1999) side 109.

Hvordan vurderingen vil slå ut, vil kunne variere fra et tilfelle til en annet. Generelt sett vil hovedregelen likevel være at innsamling og analyse av enkeltpersoners bruk av internettjenester for markedsføringsformål vil komme i konflikt med kravet til nødvendighet, og det vil overstiges av personvernhensyn. Særlig gjelder det der man står overfor sporing av enkeltpersoner på tvers av ulike tjenester.

Det kan imidlertid tenkes tilfeller hvor behandlingen av personopplysninger kanskje kan forankres i balansetesten: Hvis en nettbokhandel samler inn opplysninger om den enkeltes atferd kun på sitt nettsted – for eksempel hvilke bøker man klikker på eller kjøper – for å gi anbefalinger (som er en form for markedsføring av egne varer) neste gang personen kommer tilbake, vil dette kanskje kunne være legitimt ut fra personopplysningloven § 8 f. Virksomheten måtte antakelig likevel gi den enkelte mulighet til å reservere seg (opt out).[64]

Samtykke

Som vi har sett må den som samler inn og behandler personopplysninger for å drive atferdsbasert markedsføring overfor den enkelte basere seg på samtykke etter personopplysningsloven.

Et samtykke innebærer en *frivillig, uttrykkelig* og *informert* erklæring fra den registrerte om at han eller hun godtar behandlingen av opplysninger om seg selv.[65] Ved å la adgangen til å behandle personopplysninger bero på samtykke, utstyrer man den enkelte med makt og mulighet til å bestemme over seg selv. Samtykkekravet innkapsler slik sett kjernen i den enkeltes krav på respekt for sitt privatliv.

I kravet om frivillighet ligger at det ikke må ligge noen form for tvang eller press bak – det må være reell frivillighet. Dersom det å si nei medfører ulempe eller negative konsekvenser, kan dette utgjøre et slags press som ikke er forenlig med frivillighetskravet. Hvis for eksempel det reelle alternativet til samtykke, er å ikke bruke den aktuelle tjenesten, er det problematisk.[66] Slike «take it or leave it» løsninger er en stor utfordring.

I kravet om at samtykket skal være uttrykkelig ligger at det må være klart og utvetydig at personen samtykker. Det stilles ikke noe spesielt formkrav. Normalt krever dette en aktiv handling fra den enkelte. I en digital verden vil det kunne tilbys mange ulike teknologiske løsninger for at brukeren skal gi sitt samtykke. Det sentrale her er at løsning må være innrettet slik at brukeren gjør noe aktivt for å signalisere at vedkommende gir sitt samtykke. Det er for eksempel ikke tilstrekkelig at det gis informasjon om den behandlingen av personopplysninger som foregår på et nettsted, sammen med en setning om at man samtykker ved å bruke tjenesten.

I kravet om at samtykket skal være informert ligger at vedkommende skal få tilstrekkelig informasjon til å forstå hva det samtykkes til. Da må det blant annet gis informasjon om hva slags opplysninger som samles inn, hva opplysningene skal brukes til, hvem som er ansvarlig og all annen informasjon som er nødvendig for at den registrerte skal forstå hva han eller hun medvirker til. Det kan typisk være nødvendig å informere om når opplysningene slettes, om de deles med andre og i så fall med hvem. Informasjonen må presenteres på en enkel og forståelig måte. Gode og pedagogiske virkemidler bør tas i bruk. Samtykke må gis før behandlingen tar til. Et samtykke skal også kunne trekkes tilbake, med den virkning at det rettslige grunnlaget for behandlingen faller bort. Det må legges til rette for at samtykke kan trekkes tilbake.

Det å legge til rette for at den registrerte kan motsette seg behandling (opt out eller reservasjonsrett), er ikke ensbetydende med at behandlingen baserer seg på samtykke dersom personen ikke reserverer seg. Det å ikke motsette seg er ikke det samme som å samtykke.

Artikkel 29-gruppen har i flere uttalelser sagt at behandling av personopplysninger i forbindelse med atferdsbasert markedsføring på nett krever samtykke i samsvar med disse prinsippene.[67]

Andre viktige grunnkrav

Kravet om rettslig grunnlag er bare ett av flere grunnkrav. Personopplysningsloven inneholder flere grunnkrav som må være oppfylt ved enhver behandling av personopplysninger.[68] De øvrige kravene har selvstendig betydning og representerer selvstendig skranker. Vi skal se litt nærmere på noen av de viktigste grunnkravene.

---

[64] Eksempel er hentet fra Borgesius, op. cit.

[65] Se § 2 nr. 7.

[66] Artikkel 29-gruppen har for eksempel i working document 02/2013 side 5 og 6 lagt til grunn at internettbaserte tjenester ikke kan betinges av at bruker må akseptere informasjonskapsler. – det må være et reelt valg.

[67] Se opinion 2/2010, 16/2011 og working document 02/2013

[68] Jf. § 11

Formålsbegrensningsprinsippet

Personopplysninger skal kun behandles til uttrykkelig angitte og legitime formål. [69] Den behandlingsansvarlige plikter å gjøre det klart både for seg selv og for den registrerte (den det behandles opplysninger om) hva formålet er. Dette formålet må være klart når behandlingen tar til, altså når opplysningene samles inn eller registreres. Formålet er med på å sette en klar ramme for hva opplysningene kan og ikke kan brukes til.

For å understreke betydningen av å holde seg til formålet, forbyr loven behandling av opplysningene til nye formål som er uforenlig med det opprinnelige formålet.[70] Det eneste unntaket fra forbudet er hvis den registrerte samtykker til behandlingen til det nye formålet. Et nytt formål vil typisk være uforenlig hvis det skiller seg markert fra det opprinnelige og/eller går utover hva den registrerte berettiget kunne forvente. For eksempel vil det å registrere atferden til brukerne på et nettsted for å utvikle og drifte nettstedet effektivt være som noe markert forskjellig fra det å lage personprofiler på den enkelte bruker for individuelt tilpasset markedsføring.

Prinsippet om formålsbegrensning har betydning på to måter når det er snakk om bruk av personopplysninger til markedsføring. Før det første begrenser det adgangen til å ta i bruk opplysninger som opprinnelig er samlet inn til andre formål til markedsføringsformål. For det andre begrenser det muligheten til å ta i bruk opplysningene innhentet til markedsføringsformål, til andre og nye formål.

I praksis er det en utfordring at de opplysninger som samles inn med det formål å målrette markedsføring også brukes av den samme aktøren til andre uttalte formål. For eksempel sier Microsoft i sin personvernerklæring at «Fordi informasjonen for atferdsbaserte annonser også brukes til andre nødvendige formål (inkludert å tilby tjenestene våre, samt analysetjenester og avdekking av svindel), vil det å reservere seg mot atferdsbaserte annonser ikke føre til at informasjonen ikke blir samlet inn».[71]

Begrensninger i omfang og tid

Det følger av personopplysningsloven at den behandlings-ansvarlige må begrense sin behandling av opplysninger til det som er relevant og tilstrekkelig ut fra formålet, og at opplysningene skal slettes når lagring ikke lenger er nødvendig ut fra formålet.[72] I tillegg skal opplysningene være korrekte og oppdaterte.

I dette ligger at man må nøye seg med det som er relevant ut fra formålet og begrense seg til det som er tilstrekkelig. Det innebærer klare begrensninger på omfanget av opplysninger som kan behandles. Poenget er at omfanget av opplysninger som samles skal være så lite som mulig. Overdreven datainnsamling er ikke lov.[73]

Det er også en begrensning i tid. Det er ikke lov å lagre opplysninger videre når dette ikke er nødvendig ut fra formålet. Behandlingen av opplysningene skal ha en sluttdato.

I praksis kan disse begrensningene gli over i hverandre for eksempel ved at opplysningene mister sin relevans over tid og at det dermed også er unødvendig å lagre dem videre ut fra formålet. I tilknytning til atferdsstyrt markedsføring vil opplysninger om en brukers atferd fra noe tid tilbake fort måtte anses som utdatert, mindre relevant og unødvendige, og at behandlingen av disse opplysningene bør opphøre til dette formålet.

Rett til informasjon

Personopplysningsregelverket bygger på et grunnleggende prinsipp om at behandling av personopplysninger skal være gjennomsiktig. Det er derfor gitt egne regler om informasjon.[74]

Den enkelte har krav på å få informasjon når det behandles opplysninger om vedkommende. Informasjon skal gis uoppfordret. Det skal alltid gis informasjon om blant annet hva slags type opplysninger som behandles, hvilke formål opplysningene skal brukes til, hvem som er ansvarlig og hvem opplysningene eventuelt vil deles med.

---

69 For mer detaljer, gjennomgang se opinion 03/2013.

70 Jf. § 11 bokstav c.

71 http://www.microsoft.com/nb-no/privacystatement/default.aspx

72 Jf. § 11 bokstav d og e.

73 Se tilsvarende bestemmelse i personverndirektivet artikkel 6 c) som krever at behandlingen skal være «adequate, relevant and not excessive».

74 jf. lovens kapittel 3.

I tillegg er det særskilt informasjonskrav når noen, for eksempel som ledd i markedsføringsvirksomhet, henvender seg til en enkeltperson på grunnlag av en personprofil som er ment å beskrive atferd, preferanser, evner eller behov. I slike tilfeller skal det gis informasjon om hvem som er den behandlingsansvarlige, hvilke opplysningstyper som er anvendt og hvor opplysningene er hentet fra. Dette kravet må antas å komme inn ved den individuelt tilpassede markedsføringen som skjer via internett. Loven er her ment å sikre en ekstra gjennom-siktighet i en situasjon hvor det ikke er intuitivt for individet å forstå hva som skjer.

Den enkelte har videre rett til, på forespørsel, å få utdypende informasjon om den behandling av personopplysninger som angår han eller hun selv. Man har også rett til innsyn i de opplysninger som behandles. Når det gjelder atferdsstyrt markedsføring, vil det særlig kunne være av betydning å la folk få tilgang til den profilen de har.[75]

Cookie-bestemmelsen

Lagring av opplysninger i brukers kommunikasjonsutstyr, eller å skaffe seg adgang til slike, er ikke tillatt uten at brukeren er informert om hvilke opplysninger som behandles, formålet med behandlingen, hvem som behandler opplysningene, og har samtykket til dette. Første punktum er ikke til hinder for teknisk lagring av eller adgang til opplysninger:

1. utelukkende for det formål å overføre kommunikasjon i et elektronisk kommunikasjonsnett

2. som er nødvendig for å levere en informasjonssamfunnstjeneste etter brukerens uttrykkelige forespørsel.

Retting og sletting

Personopplysningsloven gir den enkelte på nærmere vilkår rett til å få opplysninger rettet og slettet.[76] Retting kan særlig være aktuelt der opplysninger er uriktige eller ufullstendige. Dette kan for eksempel være av betydning med hensyn til personprofiler. Profilen kan gi et feil bilde av personen, og det må være mulig for den enkelte å få korrigert bildet.

Sletting kan være aktuelt der den enkelte motsetter seg behandlingen, for eksempel ved å trekke sitt samtykke, og videre behandling av den grunn ikke lenger har et rettslig grunn. Sletting kan også være aktuelt fordi behandlingen ikke er i samsvar med grunnkravene – for eksempel at opplysningene er utdatert og irrelevant ut fra formålet, eller at videre lagring er unødvendig for formålet.

Ekomloven

I ekomlovens § 2-7 b (lov om elektronisk kommunikasjon) er det gitt en særregel om blant annet bruk av informasjonskapsler.[77] Lovens regel bygger på den tanke at brukers kommunikasjonsutstyr er en del av en enkeltes private sfære, og at det å lagre data på dette utstyret, eller hente ut data, representerer en form for inngrep. Dette gjelder helt uavhengig av om informasjon som lagres eller hentes ut er å anse som personopplysninger.

Bestemmelsen kalles gjerne *cookie-bestemmelsen*, og den har også fått overskriften «bruk av informasjonskapsler/cookies». Dette er noe misvisende ettersom bestemmelsen omfatter enhver situasjon hvor noen lagrer eller skaffer adgang til opplysninger i brukerens kommunikasjonsutstyr. Bestemmelsen kan for eksempel også komme til anvendelse på såkalte digitale fingeravtrykk[78] eller ved installasjoner av apper eller annen programvare.[79]

Loven gjennomfører artikkel 5 (3) i det såkalte kommunikasjonsverndirektivet fra EU (e-privacy-direktivet[80]). Bestemmelsen retter seg mot en spesiell handling, nemlig det å lagre eller skaffe seg adgang til opplysninger i brukerens kommunikasjonsutstyr – for

75 Selskaper som Google og Microsoft har begynt å legge til rette for dette.

76 Jf. § 27 og 28.

77 Jf. § 2-7 b.

78 Teknisk informasjon om enheten samles inn og brukes for å gjøre enheten unikt gjenkjennelig. Se Artikkel 29-gruppens opinion 09/2014 on the application of the Directive 2002/58/EC to device fingerprinting.

79 Se Artikkel 29-gruppens opinion 02/2013 on apps on smart devices.

80 Kommunikasjonsverndirektivet, e-privacy-direktivet (Direktiv 2002/58/EF)

eksempel sette en cookie i brukerens nettleser. Dette er forbudt med mindre brukeren er gitt tilstrekkelig informasjon og har samtykket[81].

Det følger av forarbeidene til ekomloven[82] at kravet til samtykke ikke er det samme som det kravet til samtykke som ligger i personopplysningsloven. Departementet viser til at det er praktiske hensyn bak dette: «En teknisk innstilling i nettleser vil kunne benyttes til å samtykke eller til å nekte samtykke, forutsatt at sluttbruker er tilstrekkelig informert om formålet med informasjonsinnsamlingen og lagringen. Også en forhåndsinnstilling i nettleser om at bruker aksepterer informasjonskapsler anses å utgjøre et samtykke.» Forarbeidene legger med andre ord opp til at det er tilstrekkelig å gi klar og tydelig informasjon om bruk av informasjonskapsler. Så lenge brukeren ikke har gjort noe med innstillingene i nettleseren for å motsette seg informasjonskapsler, er det fritt frem å sette slike på brukerens maskin.

Departementet begrunner sitt syn nærmere:

«Departementet legger til grunn at kommunikasjonsverndirektivet artikkel 5.3 ikke har til hensikt å vanskeliggjøre bruk av lovlig teknikker som informasjonskapsler, men å sikre brukernes personvern. Artikkel 5.3 retter seg i hovedsak mot personvernkrenkende teknikker som spionprogram og lignende. Departementet vil således presisere at endringen i regelverket ikke er ment å innebære noen endring når det gjelder å benytte lovlige teknikker, men skal forstås som en presisering av forpliktelsen til å gi brukere tilstrekkelig informasjon og valgmuligheter med hensyn til bruken av disse teknikkene. Dette vil gi brukerne mulighet til å ivareta sine rettigheter. Med «lovlige teknikker» menes informasjonskapsler eller lignende teknikker som har stor utbredelse, og som vanligvis benyttes som rene tekniske hjelpemiddel i utformingen av nettsteder.»

Vi mener samtykke etter ekomloven § 2-7 b må være forenlig med personopplysningslovens krav til samtykke.

Direktivforpliktelsen er en klar endring av tidligere regulering[83]. Den tidligere bestemmelsen i direktivets artikkel 5 (3) krevde at brukeren skulle ha anledning til å motsette seg handlingen. Dette ble endret til at det istedenfor skulle kreves samtykke fra brukeren.

Det følger av direktivets artikkel 2 (d) at begrepet samtykke skal samsvare med samtykke i personverndirektivets forstand, altså det direktiv personopplysningsloven gjennomfører.

Videre fremstår departementets henvisning til informasjonskapsler som en lovlig teknikk som vanskelig å forstå. Det er formålet med cookien og hvordan den brukes som avgjør hvor legitim den kan være. For de mest legitime formene for informasjonskapsler – de som er helt nødvendige for at tjenesten skal fungere – gjøres det uttrykkelige unntak fra kravet om samtykke. For andre typer informasjonskapsler, som for eksempel har som formål å samle inn opplysninger for atferdsbasert markedsføring, og som benyttes til å følge den enkelte på tvers av tjenester, stiller det seg annerledes. Her kreves det samtykke – og det er først hvis samtykke er gitt at denne teknikken for å samle informasjon er lovlig. Det blir derfor lite holdbart å si at informasjonskapsler er lovlig teknikk og bruke det som argument for at det vil være tilstrekkelig at brukeren ikke har motsatt seg informasjonskapsler i innstillingene til nettleseren.

Endelig er det grunn til å fremheve at Artikkel 29-gruppen gjentatte ganger har vært avvisende til at innstillinger i nettleseren eller andre reservasjonsmekanismer («opt out») er forenlig med kravet til samtykke etter kommunikasjonsverndirektivet artikkel 5.3. Samtykkekravet må være forenlig med samtykke i personverndirektivets forstand, mener gruppen.[84]

Dersom ekomlovens krav til samtykke i § 2-7 skal tolkes i samsvar med uttalelsene i forarbeidene, er det altså risiko for motstrid mellom den norske regelen og det direktivet regelen er ment å gjennomføre. Norsk rett forutsettes å være i samsvar med våre folkerettslige forpliktelser (presumsjonsprinsippet), og det kan spørres om ikke ekomloven bør tolkes og anvendes slik at motstrid ikke oppstår.[85]

81 Unntaket i andre punktum går vi ikke nærmere inn på her.

82 Prop. 69 L (2012-2013) side 43.

83 I direktiv 2009/136/EF.

84 Se Artikkel 29-gruppen har for eksempel i working document 02/2013. side 5 og 6 lagt til grunn at internettbaserte tjenester ikke kan betinges av at bruker må akseptere informasjonskapsler. – det må være et reelt valg.

85 Se Rt. 2000 side 1811 (Finnanger I).

Hvem plikter å følge «cookie-bestemmelsen»?

Ekomloven § 2-7 b regulerer som nevnt en bestemt handling, nemlig det å lagre eller skaffe seg adgang til informasjon på brukerens kommunikasjonsutstyr. Det er den som står bak handlingen – og bestemmer formål og midler – som er ansvarlig for å følge loven[86]. Den ansvarlige etter ekomloven er ikke nødvendigvis behandlingsansvarlig i personopplysningsloven forstand. Dette henger sammen med at informasjon som lagres eller hentes ut ikke nødvendigvis er å anse som personopplysninger.

Når en bruker oppsøker et nettsted, som for eksempel en avis, vil vedkommende ofte komme i kontakt med flere aktører som bruker informasjonskapsler eller andre teknikker for å lagre eller skaffe seg adgang til informasjon på brukerens enhet. Det vil typisk være mediehuset som driver nettstedet, og andre aktører (ofte kalt tredjeparter) som for eksempel driver med markedsføringsvirksomhet eller analysevirksomhet.

I en slik situasjon vil i utgangspunktet hver aktør være ansvarlig for å gi informasjon og innhente samtykke der dette er påkrevd. Nasjonal kommunikasjonsmyndighet legger til grunn at den som tillater bruk av tredjeparts informasjonskapsler på eget nettsted må informere om dette i tillegg til informasjon om egne informasjonskapsler. [87] Samtidig sier Nasjonal kommunikasjonsmyndighet at tredjeparten er ansvarlig for å oppfylle informasjonsplikten på sitt eget nettsted.[88]

Datatilsynet mener brukeren bør få den nødvendige informasjonen på det nettstedet han eller hun besøker. Både eier av nettstedet (publisisten) og de ulike tredjepartene har et ansvar for å gi informasjon og innhente samtykke, og aktørene bør her samarbeide slik at informasjonen blir gitt ett sted. Publisister bør tilrettelegge for at tredjeparter kan gi opplysninger om sine informasjonskapsler og andre handlinger som omfattes av bestemmelsen, direkte på nettstedet til publisisten.

Geografisk virkeområde for «cookie-bestemmelsen»

Ekomloven § 2-7 b skal gi vern for dem som bruker elektronisk kommunikasjonsutstyr. Men hvor langt strekker dette vernet seg? Trenger utenlandske selskaper/aktører forholde seg til norsk rett når de benytter informasjonskapsler eller liknende på kommunikasjonsutstyret til norske brukere?

I forarbeidene til loven er ikke denne problemstillingen drøftet eller løst direkte. Ut fra de generelle bestemmelsene om virkeområde i ekomloven § 1-2 og § 1-3, synes loven å gjelde for den som driver virksomhet knyttet til elektronisk kommunikasjon på norsk territorium[89].

Artikkel 29-gruppen har i flere opinions lagt til grunn at kommunikasjonsverndirektivet artikkel 5 (3) retter seg mot alle som lagrer eller skaffer seg adgang til informasjon på brukerens utstyr, uavhengig av hvor i verden vedkommende befinner seg. [90] Artikkel 29-gruppen fremholder at artikkel 5 (3) skiller seg fra mange av de andre bestemmelsene i direktivet, som i hovedsak retter seg mot tilbydere av elektronisk kommunikasjonsnett- eller tjeneste i EØS: Den skal beskytte den enkelte mot en spesiell type handling, uavhengig av hvem som står bak handlingen eller hvor i verden vedkommende befinner seg. Artikkel 29-gruppen mener også at kommunikasjonsverndirektivet må forstås i lys av personverndirektivets bestemmelse om geografisk virkeområde (artikkel 4). Dette direktivet – eller mer presist, loven i det enkelte land som gjennomfører direktivet – vil nemlig gjelde for aktører som ikke er etablert i et EØS-land, men som bruker hjelpemidler i EØS-landet ved behandling av personopplysninger. Begrepet «hjelpemiddel» vil som nevnt tidligere kunne omfatte elektronisk kommunikasjonsutstyr når den behandlingsansvarlige tar dette utstyret i bruk som ledd i sin behandlingen av personopplysninger, for eksempel ved å sette en informasjonskapsel som registrerer personopplysninger.

Det er dessverre uklart hvor stor rekkevidde den norske loven er ment å ha. Det er imidlertid rimelig å forvente at utenlandske aktører som retter sin tjenester mot det norske markedet, for eksempel ved å tilby markedsføringstjenester, må følge norsk lov i møtet med norske brukere.

Forholdet mellom ekomloven og personopplysningsloven

---

[86] Se forarbeidene Prop. 69 L (2012-2013) side 102.

[87] Nasjonal kommunikasjonsmyndighet (Nkom), tilsynsmyndighet etter ekomloven.

[88] http://www.nkom.no/teknisk/internett/cookies/informasjonskapsler-cookies.

[89] Ekomloven § 1-3 utvider det geografiske virkeområde til å gjelde blant annet norske skip og fly.

[90] Se opinion 01/2008, 02/2010 og 03/2013.

Ekomloven § 2-7 b og personopplysningsloven virker side om side. Ekomloven § 2-7 b regulerer kun den handling å lagre eller å skaffe seg adgang til informasjon på brukerens kommunikasjonsutstyr, helt uavhengig av om informasjonen er personopplysninger eller ikke. Dersom det blir behandlet personopplysninger, kommer personopplysningslovens bestemmelser fullt ut til anvendelse i tillegg. Dette betyr at den som gjennom handlinger som omfattes av ekomloven § 2-7 b samler inn personopplysninger, vil måtte opptre i samsvar med begge regelsettene.

Et springende punkt er imidlertid om ekomloven § 2-7 b er et selvstendig rettslig grunnlag for behandling av personopplysninger (lex specialis), eller om behandlingen av personopplysninger må ha rettslig grunnlag i henhold til personopplysningslovens alminnelige bestemmelser. Som nevnt over tilfredsstiller ikke samtykkekravet i ekomloven, slik det fremstår i forarbeidene, det tilsvarende kravet etter personopplysningsloven. Vil samtykke etter ekomloven gi nødvendig rettslig grunnlag for å behandle personopplysninger?

Etter personopplysningsloven § 8 og § 9 er det tillatt med en gitt behandling av personopplysninger hvis det er fastsatt i lov at det er adgang til slik behandling. Med lov menes her en annen lov enn personopplysningsloven.

Er ekomloven § 2-7 b en særbestemmelse om en type personopplysningsbehandling?

Datatilsynet vil mene at ekomloven § 2-7 b *ikke* er en særregel om behandling av personopplysninger – den regulerer ikke behandling av personopplysninger som sådan. Selv om det underliggende motiv for regelen er personvernhensyn, dreier ikke bestemmelsen i sin natur om beskyttelse av personopplysninger.

Regelen bygger tvert imot på den enkeltes kommunikasjonsutstyr tilhører vedkommende privatsfære, og reglen skal gi beskyttelse mot inngrep i denne sfæren ved slike handlinger som regelen beskriver – helt uavhengig av hva slags informasjon som lagres eller hentes ut. Om handlingen medfører at opplysninger om personen blir behandlet, kommer personopplysningsvernet inn i tillegg[91].

Verken ordlyden i bestemmelsen eller forarbeidene sier noe konkret om at bestemmelsen er særregulering av en bestemt type personopplysningsbehandling. Forholdet til personopplysningsloven er ikke berørt, utover at det sies at samtykkekravet er annerledes enn det som gjelder etter personopplysningsloven.

Datatilsynet mener derfor at samtykkekravet etter personopplysningsloven vil kunne stå seg i situasjoner hvor det blir behandlet personopplysninger.

Det vil i så fall bety at den som samler inn og behandler personopplysninger ved hjelp av handlinger som omfattes av ekomloven § 2-7 b, faktisk må ha et samtykke som er forenlig med samtykkekravet i personopplysningsloven – det er ikke tilstrekkelig å bare opptre i samsvar med samtykkekravet i ekomloven.

[91] Tilsvarende argumentasjon finnes i juridisk teori, se Zuiderveen Borgesius op. cit. Artikkel 29-gruppen kan imidlertid forstås i den retning at e-privacy direktivet artikkel 5 (3), som ekomloven gjennomfører, er lex specialis i relasjon til personverndirektivet når det kommer til kravet om rettslig grunnlag. Men som nevnt er gruppen av den oppfatning at samtykkekravene i de to regelsettene skal være forenlige, slik at den som får et samtykke etter artikkel 5 (3), samtidig får samtykke i personverndirektivets forstand til eventuell behandling av personopplysninger som samles inn.

Nye regler i vente

I EU arbeides det nå med en ny forordning som skal erstatte dagens personverndirektiv. Det er forventet at EU vil komme i mål med de nye reglene i nær fremtid. Forordningen vil tas direkte inn i norsk rett. Forslaget slik det nå lyder bygger på eksisterende direktiv, men det vil etter alle solemerker bli vesentlige endringer. [92] Vi vil her nevne noen:

I utgangspunktet bygger forslaget på kjent stoff når det gjelder det geografiske virkeområdet. Forordningen skal gjelde der den behandlingsansvarlige er etablert i EU, og når det er sammenheng mellom behandlingen av personopplysninger og den aktivitet den behandlingsansvarlige har i EU. Men det er én viktig endring. Forslaget inkluderer databehandlere slik at forordningen skal gjelde også der det bare er databehandleren[93] som er etablert i EU. Dette er en klar utvidelse.

I tilfeller hvor etableringskriteriet ikke er oppfylt, er det foreslått endringer som klart bærer preg av et ønske om å utvide forordningens virkeområde. Reglene skal gjelde der det behandles opplysninger om enkeltpersoner som oppholder seg i EU, så lenge behandlingen er knyttet til tilbud om varer eller tjenester til disse enkeltpersonene i EU, eller til monitorering av deres atferd.

I lys av dette må vi gå ut fra at reglene får et betydelig virkeområde når det gjelder den individuelt tilpassede markedsføringen som skjer på nett.

Prinsippet om formålsbegrensning er i utgangspunktet foreslått videreført i forslagene til forordning. Samtidig foreligger det forslag om at personopplysninger kan behandles til nye og uforenlige formål så lenge behandlingen har rettslig grunnlag i forordningen. Det vil si at man ikke er avhengig av samtykke for å bruke opplysningene til helt andre formål.

Forslaget har her møtt stor motstand, med rette. Parlamentet har i sitt utkast ikke innskrenket formålsbegrensningsprinsippet, slik at her er det veldig uklart hva man ender opp med.

Dersom Kommisjonens eller Rådets forslag blir gjeldende rett, er det grunn til å frykte at forutsigbarheten (kun behandle opplysninger til opplyst formål) blir vesentlig dårligere.

Prinsippene for samtykke er foreslått videreført – det skal være frivillig, informert og uttrykkelig. Det er samtidig foreslått flere regler som presiserer betydningen av samtykke. Det er foreslått at den behandlingsansvarlige skal ha bevisbyrden for at samtykke foreligger. Dette vil skjerpe kravet til at det må kunne dokumenteres at den registrerte har gitt sin aksept til behandlingen.

Det er videre foreslått at dersom samtykke skal gis i sammenheng med en skriftlig erklæring som også tar for seg andre forhold, må samtykke til å behandle personopplysninger skilles ut på en tydelig måte. Dette vil kunne ramme bruk av brukeravtaler (terms and agreement) som inkluderer hvordan personopplysninger blir behandlet. Dette er en viktig tydeliggjøring av at samtykke til å behandle personopplysninger er noe annet en generell avtaleinngåelse, og at det skal holdes fra hverandre. Parlamentet har også foreslått at gjennomføringen av en kontrakt eller en tjeneste ikke kan gjøres betinget av at det gis samtykke til å behandle personopplysninger, dersom personopplysningene ikke er nødvendige for å gjennomføre kontrakten eller levere tjenesten. En slik regel vil i stor grad styrke frivillighetselementet i samtykket. Det er nemlig i praksis en stor utfordring at den enkelte ikke har en reell mulighet til å si nei hvis de ønsker å nyttiggjøre seg av en nettjeneste.

Det er foreslått egne regler for profilering som skal styrke den enkeltes rett til ikke å bli profilert. Reglene tar særlig sikte på handlinger som baserer seg på automatiserte prosesser, inkludert profilering, og hvor handlingen har rettslig betydning for enkeltindividet eller på annen måte klart berører personen. Reglene må antas å ha betydning for tilpasset markedsføring i en digital, nettverkstilknyttet verden.

I forslaget styrkes samtykkets betydning, og det legges begrensninger på adgangen til å behandle sensitiv informasjon som ledd i profileringen.

[92] Kommisjonen, Rådet og Parlamentet har alle utarbeidet forslag til lovtekster. Disse har noe varierende utforming. Det forhandles nå om en enighet.

[93] En databehandler er en som behandler personopplysninger på vegne av den behandlingsansvarlige.

Personvernutfordringer

Annonseinntektene fra målrettet markedsføring bidrar til å finansiere en kolossal mengde gratis internettjenester. Uten å betale kan vi glede oss over tilgang til aviser, oversettingstjenester, e-post, musikk og videoer. Men personalisert og målrettet reklame utfordrer også personvernet.

Den største utfordringen sett fra et personvernperspektiv er at enorme mengder personopplysninger blir samlet inn om oss i det skjulte. Den alminnelige internettbruker har ikke innsikt i hvilke data som samles inn om ham eller henne, hvordan dette gjøres, hvem som behandler opplysningene, rekkevidden av hvordan de brukes og hvilke konsekvenser bruken av dataene har for dem. Skal vi sørge for et godt personvern, krever det åpenhet, etterrettelighet og etterprøvbarhet. Dagens globale annonsemarked er lukket, komplekst og tilbaketrukket.

Informasjonsasymmetri

Svært få internettbrukere er klar over at flere titalls selskaper er til stede i kulissene og samler inn personopplysninger når de leser aviser på nett. En massiv innsamling av personopplysninger foregår i det skjulte uten at den alminnelige nettbruker har mulighet til å motsette seg at dette skjer. Vi har fått et samfunn som ligner på et enveisspeil, der tusentalls selskaper vet svært mye om oss, mens vi ikke engang vet at de vet.

Personvernet svekkes når vår personlige autonomi og råderett over egen skjebne utfordres av at vi mangler informasjon. Retten til informasjon er en sentral rettighet for personvernet. Den reguleres gjennom personopplysningsloven, for eksempel gjennom retten til innsyn. Uten informasjon og kjennskap til hva som foregår er vi heller ikke i stand til å være bevisste og kritiske forbrukere.

> *«Når folk forstår hva som skjer, kan jeg ikke forestille meg noe annet enn at de vil protestere.»*[94]
>
> *Britisk medieleder*

Markedet kjennetegnes av såkalt informasjonsasymmetri. Økonomer har siden 1970-tallet vært opptatt av dette fenomenet og har blant annet studert hvordan mangelfull informasjon fører til at forbrukeren ikke er i stand til å vurdere *kvaliteten* på det produktet eller tjenesten han eller hun kjøper.[95] En konsekvens av at forbrukeren ikke er i stand til å gjenkjenne kvalitet, er at selgere ikke vil konkurrere på kvalitet. Informasjonsasymmetri kan føre til at forbrukerne tilbys produkter og tjenester av stadig lavere kvalitet: et stormløp mot bunn. Informasjonsasymmetri betegnes derfor som en form for *markedssvikt* og rettferdiggjør, fra et økonomisk perspektiv, regulatoriske inngrep fra myndighetene.[96]

Når vi besøker en nettside, er det nesten umulig å vite hvor mye informasjon som blir samlet inn om oss, og hvordan denne informasjonen blir brukt. Denne mangelen på kunnskap hos forbrukeren fører til at selskapene ikke har insentiver til å konkurrere om å levere personvernvennlige tjenester. Forbrukerne er ikke i stand til å gjenkjenne kvalitet, her forstått som tjenester som ikke lar tredjeparter samle inn personopplysninger i det skjulte, og er dermed ikke villig til å betale for dette.

Hvis folk ikke vet at det blir samlet inn opplysninger om dem, kan de heller ikke etterspørre eller verdsette tjenester som lar dem være i fred. Den ujevne fordelingen av informasjon resulterer i en konkurransesituasjon som oppmuntrer markedsaktørene til å ta i bruk mer og mer personverninngripende virkemidler.[97]

94 Sitat fra leder av britisk mediebyrå, sitert i The Economist, «Little Brother, Special Report on Advertising and Technology», 13.09.2014, http://www.ogilvydo.com/wp-content/uploads/2014/09/20140913_SR_MAILOUT.pdf

95 Sørgard, Lars, «Informasjonsasymmetri og konkurransepolitikk», publisert i: Stortingsmelding nr. 15 (2004-2005): Om konkurransepolitikken, Vedl. 1, s 95-109., Institutt for samfunnsøkonomi, Norges Handelshøyskole, Bergen, 2005

96 Zuiderveen Borgesius, Frederik J., «Behavioural Sciences and the Regulation of Privacy on the Internet», draft chapter to the book «Nudging and the Law - What can EU Law learn from Behavioural Sciences?», red. A-L Sibony & A. Alemanno (Hart Publishing), Institute for Information Law Research Paper No. 2014-02, Amsterdam Law School Research Paper No. 2014-54, 2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2513771

97 Ibid.

I en slik situasjon vil ikke konkurransen i markedet bringe balanse i regnskapet. Det kommer ikke tjenester og produkter som baserer seg på at brukerne skal få være i fred og som kan representere et reelt alternativ for folk flest.

Svakheter ved samtykke

Et krav om samtykke innebærer at man utstyrer den enkelte med makt og mulighet til selv å bestemme hva man vil være med på. Det er imidlertid grunn til å spørre hvor reell makt og innflytelse den enkelte har i en digital verden[98].

Som nevnt er det veldig vanskelig for folk flest å sette seg inn i hva som skjer. Den enkelte har i praksis dårlige muligheter til å treffe informerte beslutninger. Dette henger delvis sammen med at det som foregår er lite gjennomsiktig, og delvis henger det sammen med at det blir for mye informasjon for den enkelte å sette seg inn i.

Utfordringer med samtykke kan også forklares med menneskelige egenskaper. Vi er ofte mindre rasjonelle enn vi liker å tro, og vi har ofte tendenser til å velge status quo-løsninger eller de løsninger som gir umiddelbart positivt utbytte. Hvis for eksempel en kunde går inn i et nettbutikk for å kjøpe en vare, så vil dette være det primære fokuset for kunden. Reelt sett representerer det en kostnad for kunden å skulle sette seg inn i hvordan personopplysninger blir behandlet i tillegg til alt det andre kunden blir presentert, slik som de alminnelige avtalevilkårene. Kunden vil gjerne være opptatt av det kortsiktige, nemlig å få kjøpe varen, og vil nærmest på automatikk akseptere alt det vedkommende blir bedt om akseptere. Reservasjonsløsninger («opt out») blir ofte ikke benyttet fordi vi tenderer til å forholde oss til standardvalget løsningen leveres med.

Slik menneskelige egenskaper — eller svakheter, om man vil — kan utnyttes. Dette gjøres antagelig også.

I realismens navn kan vi innrømme at det å la behandling av personopplysninger være betinget av samtykke i mange tilfeller ikke fungerer etter sin hensikt. Ved å la den enkelte bestemme selv, lar man også den enkelte stå alene overfor store og mektige aktører som i realiteten kan diktere hva han eller hun må samtykke til.

Resignasjonen råder

En spørreundersøkelse gjennomført i USA viser at folk oppgir resignasjon som hovedårsak til at de gir fra seg sine personopplysninger i bytte mot gratis tjenester. Det er ikke fordi de synes det er en grei byttehandel, slik det ofte blir fremholdt av bransjen selv. Folk sier at de føler seg maktesløse og at ikke mener at de har noe annet valg. Studien viser også at jo mer innsikt og forståelse folk har om hvordan internettjenester samler inn og utnytter personopplysninger kommersielt, jo mer negative er de til å akseptere rabatter i bytte mot sine personopplysninger.

Kilde: Turow, Joseph, Michael Hennessy og Nora Draper, «The Tradeoff Fallacy, How Marketers Are Misrepresenting American Consumers And Opening Them Up to Exploitation», Annenberg School for Communication. University of Pennsylvania. 2015

Risiko for manipulering

Maktubalansen mellom de som profilerer og de som blir profilert øker. Dette utfordrer vår personlige autonomi fordi den store informasjonsasymmetrien øker risikoen for manipulering.[99]

Før i tiden foretok vi våre innkjøp ansikt-til-ansikt i butikken. I dag foregår kjøp av produkter og tjenester i stor grad via en datamaskin, smarttelefon eller nettbrett. Dagens forbruker er blitt en «mediert» forbruker.[100] Dette har ulike konsekvenser. For det første samler tjenestene og produktene vi samhandler med inn og lagrer enorme mengder data om oss. For det andre ønsker selskapene som leverer tjenestene og produktene våre i stadig større grad selv å velge når de vil komme i

98 For en bredere gjennomgang se Zuiderveen Borgesius, Frederik J., «Behavioural Sciences and the Regulation of Privacy on the Internet», op. cit

99 Europarådet mener den økende bruken av profilering utgjør en trussel mot enkeltindividets mulighet til selvbestemmelse, se Europarådet, «Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling», 2010, https://wcd.coe.int/ViewDoc.jsp?id=1710949

100 Calo, Ryan, «Digital Market Manipulation», 82 George Washington Law Review 995 (2014); University of Washington School of Law Research Paper No. 2013-27, 2013, http://dx.doi.org/10.2139/ssrn.2309703

kontakt med oss, i stedet for å vente på at vi skal ta kontakt med dem. Det at virksomheter tar kontakt med brukeren, og ikke omvendt, har konsekvenser. Vi har ikke på samme måte mulighet til innta rollen som kritisk konsument før vi entrer en kjøpssituasjon. I en tid med konstant skjermtid er vi hele tiden i en konstant kjøpssituasjon. Disse to tingene, selskapers enorme kunnskap kombinert med deres konstante tilgang til oss, gjør oss sårbare for å bli manipulert.

I dag er markedsførere opptatt av relevans. Markedsførerne serverer brukere annonser for produkter de tror de vil ha, basert på sporene de har lagt igjen. Utviklingen går imidlertid i retning av at data også brukes til å analysere seg frem til folks *sårbarheter* og personlighetstrekk. Reklamen skal ikke bare være relevant i forhold til brukerens interesser, den skal også ha en form som er tilpasset den enkeltes personlighet. Dataanalyse kan for eksempel avsløre om folk er impulsive eller forsiktige, om de responderer best på visuelle budskap eller reklame med mye tekst, om de liker å være først ute med det siste eller om de reagerer best på å høre at en vare nesten er utsolgt. Denne typen dataanalyse er foreløpig i startgropen. Illustrerende for utviklingen er at Dean Eckles, forfatter av flere forskningsartikler om denne typen profilering («persuasive profiling»), i ble hentet av Facebook for å jobbe i deres Data Science Team. [101]

Personalisert markedsføring kan fremover bli så effektiv at annonsørene får et *urettmessig overtak* over forbrukerne. Dette vil utfordrer enkeltindividets autonomi og rett til selvbestemmelse. Selskaper som samler inn data om oss kjenner oss så godt at de kan dytte oss i akkurat den retningen de vil. Fordi vi ikke har tilstrekkelig kjennskap til hvordan annonsemarkedet fungerer, vil dette skje uten av vi selv er klar over det.

Risiko for gale slutninger

Det er et grunnkrav i personopplysningsloven at virksomheter som behandler personopplysninger skal sørge for at opplysningene som behandles er korrekte. Profilene som benyttes til målrettet markedsføring består ofte av opplysninger som virksomhetene har samlet inn selv, som kombineres med data hentet fra eksterne kilder. Det er særlig kvaliteten på sistnevnte, såkalte tredjepartsdata, som kan være av variabel kvalitet. Cookie-data gir for eksempel ikke faktakunnskap om et enkeltindivid, men analyse av cookie-data danner grunnlag for å gjøre antagelser om et individs kjønn, alder, bosted, interesser, vaner, og så videre. Opplysninger hentet fra sosiale medier gir heller ikke verifiserbar kunnskap om enkeltindivider. Det er reell risiko for at gale karaktertrekk blir tildelt identifiserte eller identifiserbare enkeltindivider når denne typen data brukes i bygging av brukerprofiler. Når gale beslutninger fattes fordi man blir vurdert på grunnlag av gale data, representerer det en trussel mot den enkeltes rett til rettferdig behandling.

Rett til innsyn i data er i denne sammenheng svært sentralt. Retten til innsyn gjør det mulig for den enkelte å kreve at uriktige opplysninger, vurderinger og påstander blir korrigert eller slettet. Forbrukeren står i en svak posisjon her. Det er nærmest umulig å avdekke hvorvidt man er gjenstand for feilaktige slutninger, og hvis man avdekker dette er det vanskelig å vite hvilke selskap man skal ta kontakt med. Det er ikke usannsynlig at selskapet er utenlandsk, og at de ikke utgir data til utenlandske borgere, eller at de ikke forholder seg til europeisk regelverk som gir rett til innsyn.

Skjult diskriminering

Profilering øker risikoen for uberettiget og usynlig diskriminering. Selv om dataene som legges til grunn for beslutningen er korrekte, kan de gi et urettferdig og diskriminerende resultat for den enkelte. Det er en voksende bevisbyrde for at automatisert, algoritmestyrt markedsføring kan befeste eksisterende fordommer og stereotypier. Det er en utbredt oppfatning at programvare og algoritmer som er avhengige av data er objektive. Men algoritmer er ikke fri for menneskelig påvirkning. Algoritmer er skrevet og vedlikeholdt av mennesker, og maskinlæringsalgoritmer justerer hva de gjør basert på data innsamlet om folks atferd. Som et resultat kan algoritmer forsterke menneskelige fordommer. [102]

Googles nettbaserte annonsesystem, for eksempel, viste en annonse for høyinntektsjobber til menn mye oftere enn det viste annonsen til kvinner, og forskere har avdekket at reklame for kredittlån kun har blitt vist til

101 Ibid.

102 The New York Times, «When Algorithms Discriminate», 9.7.2015, http://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html

folk bosatt i nabolag med lav inntekt.[103] Det er også avslørt at profilering kan fungere prisdiskriminerende. The Wall Street Journal fant ut at en nettbutikk endret prisene etter hvor brukeren oppholdt seg.[104]

Det er svært vanskelig for forbrukerne å oppdage denne typen diskriminering. Den alminnelige forbruker har liten innsikt i dette markedet og har ikke mulighet til å kontrollere om algoritmer er satt sammen på en måte som fungerer diskriminerende. Ikke engang selskapene som har utviklet algoritmene er nødvendigvis klar over at algoritmene har diskriminerende effekt. At selskaper har revisjon og tilsyn med sine algoritmer, er derfor av stor betydning.

Når markedsførere etter hvert kan beregne seg frem til svært detaljert kunnskap om enkeltpersoner, eller grupper av personer, er det en utfordring å benytte denne kunnskapen uten at det får diskriminerende utfall.

Det er viktig at utviklere av algoritmer for tilpasset markedsføring er bevisst denne problematikken. De må ha et bevisst forhold til at enkelte datakategorier i noen tilfeller ikke fungerer diskriminerende, mens de i andre tilfeller vil gjøre det. Kjønn og adresse er eksempler på slike kategorier. I enkelte tilfeller vil det være uproblematisk å benytte disse kategoriene, men det i andre tilfeller kan virke diskriminerende, som vi så i eksemplet om Googles annonsesystem. Gjelder markedsføringen kjoler, er kjønn uproblematisk. Gjelder det tilbud på gressklippere, vil det være relevant å vite om vedkommende bor i blokk eller villa.

Risikoen for at bruk av data kan få diskriminerende utfall for enkeltpersoner var en av årsakene til at det i sin tid ble stilt krav til kredittopplysningsbransjen om større åpenhet. Ettersom konsekvensene av å få en dårlig kredittscore er så store, er det satt strenge krav til bransjen om gjennomsiktighet og åpenhet om deres virksomhet. Kredittopplysningsselskap opererer på konsesjon fra Datatilsynet, der det blant annet er spesifisert hvilke data som kan brukes i vurderingen når selskapene skal foreta beslutninger om folks kredittverdighet.

Vide formål

En milepel for innhenting og utnyttelse av data om den enkelte av oss ble nådd 1. februar 2012. Den datoen foretok Google en omfattende endring av sin personvernerklæring. Google lanserte det som en *forenkling* av policyen. Forenklingen lå i at det ble innført én felles personvernpolicy for alle Googles tjenester. Forenklingen medførte at opplysninger samlet inn fra én tjeneste, for eksempel YouTube, kunne utnyttes på tvers av alle selskapets tjenester, for eksempel overfor annonsører for å selge målrettet reklame.[105] Ikke lang tid etter at Google gjennomførte denne avgjørende endringen, fulgte andre store internettaktører etter. Facebook, Microsoft og Yahoo foretok tilsvarende endringer i sine personvernpolicyer i løpet av 2012.

Det er et viktig personvernprinsipp at personopplysninger kun skal samles inn og brukes til klart angitte formål. [106] Muligheten som ligger i stordataanalyse (Big Data) til å sammenstille og analysere data fra mange kilder utfordrer prinsippet om formålsbegrensning. For å stå friere til å dele og utnytte data på tvers av tjenester, har vi fått en utvikling der nesten alle store internettaktører bruker den samme vide formålsbegrunnelsen av typen:

> *«Opplysningene blir samlet inn for å utvikle tjenesten og å gi deg bedre service».*

Et slikt formål gir selskapene ekstremt fritt spillerom til å utnytte opplysningene de samler inn fra brukerne. Dette er uheldig fra et personvernperspektiv fordi enkeltindividet da mister kontrollen over hvordan opplysningene deres blir brukt. Bruken av opplysningene blir lite forutsigbar.

Hvis folk føler at de mister kontrollen over sine egne personopplysninger og ikke vet til hvilke formål de kan bli brukt, kan det føre til at folk begynner å legge bånd på seg selv. For eksempel kan det føre til at folk unngår å lese bestemte artikler i avisen fordi de er usikker på hvilke konsekvenser analysen av leservanene deres gir.

103 Ibid.

104 The Wall Street Journal, «Websites Vary Prices, Deals Based on Users' Information», 21.12.2012, http://www.wsj.com/articles/SB10001424127887323777204578189391813881534

105 I oktober 2012 sendte de europeiske personvernmyndighetene et brev til Google med et krav om at selskapet skulle implementere en rekke endringer for å tilfredsstille det europeiske personverndirektivet, 95/46/EC: http://www.cnil.fr/fileadmin/documents/en/20121016-letter_google-article_29-FINAL.pdf

106 Jf. Personopplysningsloven § 11 første ledd bokstav c)

Dette fenomenet kalles nedkjølingseffekt og er en direkte konsekvens av dårlig ivaretatt personvern.

Nærgående kartlegging

Mange føler et ubehag ved å bli kartlagt i detalj.[107] Retten til privatliv innebærer at vi skal få ha ulike sfærer av privatliv som må respekteres av alle virksomheter som samler inn og behandler data. Bygging av profiler innebærer å blande sammen opplysninger fra mange ulike sfærer av en persons liv. Slik deling av data på tvers av livsområder kan skape en følelse av å bli overvåket.[108]

«Google's privacy policy is to get right up to the creepy line and not cross it».

Erick Schmidt, Executive Chairman, former CEO, Google[109]

Ved å innføre innloggingsløsninger der brukerne er kontinuerlig logget på, kan virksomheter bygge opp svært omfattende profiler som over tid kan gi et komplett og nøyaktig bilde av en persons private identitet. Datatilsynsmyndighetene i Europa vil trolig bli konfrontert med at aktørene i bransjen ønsker å lagre kundedata over lang tid for ikke å tape i konkurranse med amerikanske internettaktører. Ved å følge brukere over flere år, kan publisister og markedsførere se hvordan forbruksmønstre endrer seg gjennom ulike livsfaser. De vil kunne se når viktige livshendelser inntreffer, som for eksempel at en bruker flytter hjemmefra, gifter seg eller får barn. Dette er data som vi har sett at det er høy betalingsvilje for i markedet.

Jo lengre data blir lagret jo flere sider av en persons liv og identitet vil bli kartlagt. Lang lagringstid av data for å bygge opp omfattende profiler av enkeltbrukere, kan derfor komme i konflikt med proporsjonalitetsprinsippet, det vil si at tiltaket utgjør et for stort inngrep i den enkeltes rett til privatliv. [110]

Dataanalyse kan også avdekke opplysninger den enkelte *ikke* har samtykket til å dele. Gjennom analyse av innsamlede personopplysninger kan det genereres nye personopplysninger, opplysninger som kan være sensitive. Dette var for eksempel tilfelle i det mye brukte Target-eksempelet der en amerikansk butikkjede fikk utviklet en algoritme som avslørte hvorvidt kunder var gravide på bakgrunn av hvilke varer de kjøpte. Ved innsamling og analyse av enkelte typer av data, for eksempel lokasjonsdata og sensordata fra kroppsnær teknologi, er risikoen for å avsløre sensitiv informasjon om brukeren ekstra høy.

De store internettselskapene og annonsørene er påpasselige på at de ikke utnytter de innsamlede opplysningene på en slik måte at brukeren oppfatter det som påtrengende eller ubehagelig. Allikevel vil aktørene hele tiden prøve så langt som mulig å innhente informasjon og målrette reklame uten å tråkke over grensen for hva den enkelte forbruker anser for å være «creepy». Aktørene tar tiden til hjelp dersom ønskede løsninger er for påtrengende. Over tid vil forbrukerne mykne og endre oppfatning. Datatilsynet skrev i 2011 om hvordan Facebook har endret personvernpolicy og vilkår kontinuerlig siden starten i 2008.[111] Ved å ta ett skritt av gangen innarbeides ny policy uten at kundene forsvinner. Et eksempel på dette var Facebooks forsøk på innføring av ansiktsgjenkjenning. Løsningen ble sterkt kritisert av myndigheter og forbrukere i Europa noe som medførte at implementeringen ble stoppet. Motstanden var imidlertid ikke like stor andre steder i verden i verden og her ble løsningen implementert.

[107] Datatilsynet mottar jevnlig henvendelser fra publikum som reagerer på hvordan markedsførere samler inn opplysninger og at de ikke føler at de har kontroll på hvordan opplysningene blir brukt.

[108] Polakiewicz, Jörg, «Profiling – the Council of Europe's Contribution» i artikkelsamligen «European Data Protection: Coming of Age», Red: Gutwirth, Serge, Ronald Leenes, Paul de Hert og Yves Poullet, Springer, Dardrecht, 2013

[109] Business Insider, «Eric Schmidt: Google's Policy Is To "Get Right Up To The Creepy Line And Not Cross It», 01.10.2010, www.businessinsider.com/eric-schmidt-googles-policy-is-to-get-right-up-to-the-creepy-line-and-not-cross-it-2010-10

[110] Datalagringsdirektivet ble i 2013 kjent ugyldig av EU-domstolen fordi direktivet ble vurdert til å utgjøre et alvorlig inngrep i den enkeltes privatliv og kunne avsløre detaljerte opplysninger om vårt privatliv ved å tillate lagring av trafikkdata i opptil to år. Pressemelding fra EU-domstolen: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

[111] Datatilsynet, «Social Network Services and Privacy A case study of Facebook», 2011, http://www.datatilsynet.no/Global/english/11_00643_5_PartI_Rapport_Facebook_2011.pdf

Lagring av enorme datamengder om enkeltindivider utgjør også i seg selv en risiko. Konsekvensene ved datainnbrudd og datalekkasjer blir enda større når datamengdene er store og kan gi et rikt og avslørende bilde av enkeltpersoner.

Fare for reidentifisering

Markedsførere hevder at de ikke benytter identifiserbare opplysninger når de bygger profiler, men at profilene består av aggregerte og anonymiserte opplysninger som ikke kan knyttes tilbake til et unikt individ. Etter hvert som en anonym brukerprofil inneholder mer og mer data, vil den likevel etter hvert antyde et relativt beskrivende bilde av en person. Profil xyx tilhører mann, 44 år, skilt, bosatt på postnummer 0655, eier av fuglehund, jaktinteressert, trolig på utkikk etter ny bil. Sannsynligvis er dette en beskrivelse som ikke vil passe på mer enn en liten håndfull mennesker, kanskje bare én person. Jo mer data som inngår i byggingen av en profil, jo mer utfordrende er det å ivareta anonymiteten til den eller de som inngår i profilen.

Ved å sammenstille data fra flere kilder er det mulig å identifisere enkeltindivider fra i utgangspunktet anonyme datasett. [112] Big Data-teknologi har ført til at skillet mellom anonyme opplysninger og personopplysninger har blitt mer uklart. Undersøkelser har vist at det er tilstrekkelig å kun kjenne til postnummer og fødselsdato til et individ for å kunne avsløre en persons identitet. Enkelte opplysninger er også mer utfordrende å anonymisere enn andre. Ett eksempel på slike opplysninger er lokasjonsdata. Dette er data som er så unikt knyttet til det enkelte individ at de er vanskelige å anonymisere fullstendig. En gruppe forskere studerte anonymiserte lokasjonsdata til en og en halv million mennesker, og lykkes ved kun å sammenstille fire tids- og stedsangivelser og identifisere 95 prosent av individene i datasettet.[113]

Med økt risiko for reidentifisering blir det viktig at selskaper som bygger profiler foretar grundige risikovurderinger i forbindelse med anonymisering av innsamlede opplysninger. Det er også viktig at virksomheter engasjert i profilbygging er bevisst forskjellen mellom pseudonyme data og anonyme data. Førstnevnte data er fortsatt å anse som personopplysninger, selv om direkte identifiserende kjennetegn er fjernet fra datasettet.

Strøm av opplysninger ut av EU

Majoriteten av tredjepartsselskapene som er til stede på norske nettsider er amerikanske. Det betyr at store mengder personopplysninger om norske borgere strømmer ut av landet og behandles under et annet regelverk enn det norske og europeiske. Dette utfordrer nordmenns personvern.

Etter den såkalte Safe Harbor-avtalen skulle USA anses som et land med adekvat beskyttelse av personopplysninger så lenge man overførte opplysninger til amerikanske selskaper som hadde sluttet seg til ordningen. I lys av blant annet Snowden-avsløringene ble det stilt spørsmål ved om Safe Harbor-avtalen egentlig ga god nok sikkerhet for personopplysningene overført til USA. Avtalen ble kjent ugyldig av EU-domstolen i oktober 2015, og det er foreløpig uavklart hvordan overføring av personopplysninger til USA kan løses best mulig for fremtiden. [114]

Datatilbydere i USA, slik som Axciom og Experian, har etter påtrykk fra myndighetene laget løsninger som gjør det mulig for brukerne å få innsyn i opplysningene som ligger lagret om dem. Løsningene er imidlertid kun mulig å benytte for brukere med bostedsadresse i USA. Selv om Axcioms datasiloer med stor sannsynlighet inneholder opplysninger om norske brukere, er det ikke mulig for norske borgere å få innsyn i disse dataene.

112 Les mer om risikoen knyttet til reidentifisering og bruk av Big Data i Datatilsynets rapport «Big Data, Personvernprinsipper under press», 2013, http://www.datatilsynet.no/Global/04_planer_rapporter/Big%20Data_web.pdf

113 de Montjoye, Yves-Alexandre, César A. Hidalgo, Michel Verleysen og Vincent D. Blondel, «Unique in the Crowd: The privacy bounds of human mobility», Scientific Reports 3, Article number: 1376, 2013, http://www.nature.com/articles/srep01376

114 http://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=553887

Oppsummering og anbefalinger

I en ideell verden, der den enkeltes rett til personvern ble respektert av alle:

- ville vi kunne lese avisen og bruke andre nettbaserte tjenester uten at et mylder av ukjente selskap tittet oss over skulderen
- ville vi enkelt kunne velge hvilke opplysninger om oss som samles inn og hva de kan brukes til
- ville opplysninger vi la igjen i én tjeneste ikke bli brukt til andre formål av en annen tjeneste
- ville det finnes sporingsfrie alternativer enkelt tilgjengelig for alle
- ville vi enkelt kunne få vite hvordan profilene våre så ut.

I arbeidet med rapporten har vi erfart særlig én ting: Det er krevende å få innsikt i hvordan markedet for automatisert annonsehandel fungerer. Det er nesten umulig å få klarhet i hvilke opplysninger som samles inn, hvordan de samles inn, hvordan brukerprofiler bygges, hvor lenge de lagres og hvordan opplysninger utveksles mellom selskap. Ingen av aktørene i verdikjeden gir informasjon til nettbrukerne om de blir solgt til høystbydende på børs hver gang de går inn på en nettside.

Markedsføring handler i sin natur om å påvirke mennesker. Innledningsvis reiste vi spørsmålet om hvor langt annonseindustrien kan gå i å påvirke andre før det ikke lenger er greit. Hvilke virkemidler er det greit å ta i bruk for å få et menneske til å handle, tenke eller mene på en bestemt måte? Som vi har vist i rapporten er det i dag teknisk mulig å kartlegge det enkelte menneske ned i den minste detalj. Selskaper kan spore hvor vi befinner oss i alle døgnets timer, registrere alt vi leser og søker etter på nett og basert på dette lage historier om våre liv. Er dette greit? Slik annonseindustrien fungerer i dag, der kartleggingen i stor grad foregår i det skjulte og er vanskelig å unnslippe, er det ikke greit, mener vi.

Personvern handler om vår rett til selv å kunne bestemme over hvilke opplysninger om oss selv vi vil dele med andre. Det handler om vår rett til å utvikle oss og leve våre liv uten at noen hele tiden følger med på hva vi gjør. Hvis vi mister kontrollen over våre egne personopplysninger, mister vi også kontrollen over selv å kunne definere hvem vi er – vi mister kontrollen over historien om oss selv.

Ingen bransje i verden vet mer om oss enn annonseindustrien. Samtidig har vi svært lite innsyn i hvordan disse selskapene behandler opplysningene de samler inn om oss. Dette påvirker maktbalansen i samfunnet. Personvernet skal ikke bare gi enkeltindividet beskyttelse mot myndighetenes konstante blikk, det skal også beskytte oss mot at private virksomheter kan følge med på alt vi gjør. Enkeltindividet er lite i møte med store konsern. Personvernlovgivningen skal bøte på noe av denne maktubalansen, ved å gi individet rettigheter slik at det kan kontrollere at det ikke blir utsatt for urettmessig eller diskriminerende behandling. Fordi annonseindustrien er så lukket, har enkeltindividet begrensede muligheter til å utøve sine grunnleggende personvernrettigheter.

Markedet preges av informasjonsasymmetri. Informasjonsasymmetri er en form for markedssvikt. Når forbrukeren ikke har kjennskap til, eller forstår hva som foregår, kan de heller ikke etterspørre tjenester som gir bedre personvern. Dette fører til at bransjen ikke har insentiver til å lage mer personvernvennlige tjenester. Vinneren i markedet er den som har mest data, og utviklingen fremover vil derfor preges av en stadig mer intens innhøsting av personopplysninger.

Datatilsynet vil jobbe for å øke gjennomsiktigheten og åpenheten i det norske annonsemarkedet. Vi vil også jobbe for å skape reell valgfrihet for brukerne, samt enkle måter å utøve bestemmelsesretten på.

Ettersom markedet ikke stopper ved Norges grenser, er internasjonalt samarbeid avgjørende for å utvikle regler som virker i en global verden. Europeiske datatilsyn må jobbe sammen for å utveksle erfaringer, koordinere tiltak overfor de ulike aktørene i verdikjeden og harmonere kravene som settes til aktørene.

Den nye personvernforordningen vil forhåpentligvis styrke personvernet til europeiske borgere. Alle virksomheter innad i EU-området må følge identisk lovgivning, og dette gjelder også utenlandske selskap som retter seg mot europeiske borgere.

Datatilsynene i Europa må også jobbe tettere sammen med forbruker- og konkurransemyndighetene for å ivareta enkeltindividets interesser.[115] Individet er ikke sterkt nok alene, og kan ikke alene påvirke selskap til å tilby mer personvernvennlige alternativ. Sammen med andre myndigheter må vi se på hva som kan gjøres for å sikre

115 European Data Protection Supervisor, «Privacy and competitiveness in the age of Big Data: The interplay between data protection, competition law and consumer protection in the Digital Economy», 2014, https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf

brukerne mer kontroll, bedre informasjon og tilgang til alternative, sporingsfrie tjenester.

Vi har listet opp anbefalinger og tiltak. Den enkelte er i dag utsatt for massiv sporing på nett. Målet er at tiltakene sammen vil bidra til å redusere sporingstrykket. Målsetningen er videre at tiltakene vil bidra til å skape større åpenhet og gjennomsiktighet i markedet for målrettet reklame, og gi brukeren mer kontroll over egne personopplysninger og bedre valgmuligheter. Listen over tiltak og anbefalinger er ikke uttømmende.

Alle aktører i verdikjeden må ansvarliggjøres for sin behandling av personopplysninger: annonsørene, mediebyråene, kjøper- og selgerplattformene, annonsebørsene og datatilbyderne. Datatilsynet vil fremover gjennomføre kontroller for å påse at aktørene samler inn og behandler personopplysninger i tråd med personopplysningsloven.

Anbefalinger i forbindelse med innsamling av opplysninger

- **Publisistene må ta ansvar for tredjepartsaktørene de slipper til på sidene sine**. De må gi informasjon om hvilke tredjepartsaktører som er til stede, hvorfor de er der, hvilke opplysninger tredjepartene samler inn og hva opplysningene brukes til. Dette krever mer samarbeid mellom publisisten og tredjepartene for å finne gode løsninger på hvordan informasjonen kan gis ett sted. Publisistene må forsikre seg om, og kunne gi tilstrekkelige garantier overfor de besøkende, om at alle aktørene som er inne på siden opptrer i samsvar med norsk og europeisk personvernlovgivning.

- **Innsamling av personopplysninger til profilerings- og markedsføringsformål må hvile på aktivt samtykke**. Den enkelte skal få en enkel mulighet til frivillig å si ja eller nei. Alle virksomheter som benytter informasjonskapsler eller andre sporingsverktøy til å samle inn opplysninger om brukerne må innhente samtykke til dette. Ved bruk av informasjonskapsler skal ikke virksomhetene kun forholde seg til om den enkelte har beskyttet seg gjennom innstillinger i nettleser eller på annen måte.

- **«Take-it-or-leave-it»-løsninger må unngås**. Publisistene må gi alle brukere tilgang til tjenestene sine, også de som *ikke* samtykker til at deres opplysninger samles inn og brukes til persontilpasset innhold og annonsering.

  Visse former for behandling av personopplysninger kan finne sted uten en persons samtykke. For eksempel kan det være opplysninger som er strengt nødvendig å behandle for at tjenesten skal fungere eller for å oppfylle en kontrakt. I slike tilfeller at det rimelig at personen må finne seg i behandlingen av opplysningene. Personen må tåle det hvis han eller hun skal benytte seg av tjenesten.

  Dersom behandlingen hviler på samtykke, *må samtykket være basert på et reelt valg*. Datatilsynet mener at tilgang til internettjenester ikke kan gjøres betinget av at brukeren gir sitt samtykke til at deres opplysninger samles og behandles for markedsføringsformål. Det er ikke rettferdig å møte enkeltmennesker med holdningen: «Du er ikke velkommen hvis du ikke samtykker». En slik praksis undergraver kjernen i samtykket og respekten for den enkeltes privatliv.

  Brukerne av internettjenester må få reelle valgmuligheter når de blir spurt om de vil gi sitt samtykke. De må kunne si ja eller nei. Her må publisister og andre leverandører av internettbaserte tjenester gå foran i utviklingen, samtidig som datatilsynsmyndighetene i EØS-området bør praktisere kravene til samtykke strengt og gripe inn ved behov.
  Antakelig bør det også vurderes tiltak fra lovgivers side. Datatilsynet er i den forbindelse positive til forslaget fra EU-parlamentet om at gjennomføringen av en kontrakt eller tjeneste ikke kan være betinget av at det gis samtykke.

- **Samtykkeerklæringene må bli bedre**. Erklæringene må skrives i et klart og tydelig språk. De må være korte og oversiktlige, men samtidig inneholde tydelig informasjon om hvilke opplysninger som samles inn, hvordan de behandles og om andre aktører får tilgang til opplysningene. Samtykkeerklæringen må gi informasjon om hvordan profilene bygges opp og hvilke datakategorier profilene består av (for eksempel at profilen består av opplysninger om hvor brukeren befinner seg, demografiske data og data om interesser utledet fra surfehistorikk). Selskap som samler inn personopplysninger må slutte å bruke vide formålsformuleringer av typen «vi vil bruke dine data til å forbedre våre tjenester». Slike formuleringer gir ikke brukerne tilstrekkelig forståelse for hva opplysningene deres blir brukt til eller forutsigbarhet knyttet til den videre bruken av opplysningene. I EUs nye personvernforordning vil det trolig stilles sterkere krav enn i dag til hvordan samtykkeerklæringene skal utformes for å sikre at brukerne forstår hva de samtykker til.

- **Gi informasjon på alternative måter**. For at brukere av digitale tjenester lettere skal forstå hvilke opplysninger tjenesten samler inn og hva opplysningene brukes til, kan det for eksempel være nyttig å bruke ikoner. Annonseindustrien bør se på

hvordan de kan merke sidene sine med ikoner som forteller brukeren at opplysninger samles inn til profileringsformål, for eksempel. [116]

- **Markedsførere må gi informasjon til den enkelte** når vedkommende blir eksponert for individuelt tilpasset reklame ved hjelp av en eller annen form for personprofil. Åpenhet er ikke bare er krav i lovgivning, men dreier seg dypest sett om å respektere de menneskene man så gjerne vil nå. Respekter dem ved å si fra hvorfor de fikk akkurat den reklamen.

Anbefalinger til bruken av opplysningene

- **Formål og relevans** må være styrende prinsipper for all behandling av data. Datahåndteringsplattformer er bygget opp med det formål å sammenstille og sammenkoble data fra mange ulike kilder, førstepartsdata og tredjepartsdata innhentet fra andre aktører. Slike analyseløsninger må ikke benyttes på en måte som kommer i konflikt med personopplysningslovens bestemmelser om blant annet formålsbestemthet.

- **Data må slettes**. Lang lagringstid av innsamlede personopplysninger vil føre til at virksomheter kan bygge opp svært omfattende og nærgående profiler av den enkelte. Selv om innsamlingen av opplysningene oppfyller kravet til formålsbestemthet og relevans, kan lagring av opplysningene over lengre tid komme i konflikt med hensynet til proporsjonalitet, det vil si at virkemiddelet vil være for inngripende i den enkeltes rett til privatliv. Omfattende databaser med personopplysninger utgjør også en sikkerhetsrisiko. Personvernkonsekvensene i forbindelse med datainnbrudd blir mer alvorlige hvis utenforstående klarer å få tilgang til personprofiler som inneholder informasjon samlet over flere år.

- **Ikke lov å profilere på sensitive data.** Det er ikke lov å samle inn sensitive data og bruke disse til profileringsformål. Det bør heller ikke være lov å lage algoritmer som resulterer i opplysninger som er sensitive, eksempelvis en analyse som gir antagelser om hvorvidt folk har et vektproblem. Den nye personvernforordningen vil trolig gjøre dette ulovlig.

- **Ikke tillatt å bygge profiler ved hjelp av cookie-matching**. Datatilsynet vil se nærmere på praksisen med cookie-matching i forbindelse med kjøp og salg av brukere på annonsebørsene. Tilsynet vil undersøke hvorvidt det er tilfelle at selskaper som byr på brukere på annonsebørser, benytter opplysningene de får om brukere i forbindelse med budgivningsprosessen til å berike egne profiler. En slik praksis bør ikke finne sted.

- **Jevnlig revisjon av algoritmene.** Det er viktig at virksomheter som utvikler algoritmer til profileringsformål er bevisst at algoritmene kan gi utilsiktede og diskriminerende resultater. Det må gjennomføres jevnlig revisjon av algoritmene og resultatene de gir for å sikre at algoritmene fungerer etter hensikten.

- **Risikovurderinger i forbindelse med anonymisering av personopplysninger.** Anonymisering er et viktig virkemiddel for å kunne hente ut verdifull innsikt ved dataanalyse, samtidig som risikoen reduseres for berørte personer. Anonyme opplysninger er ikke definert som personopplysninger, og behandlingen av slike opplysninger faller derfor utenfor personopplysningsloven. Å anonymisere data er imidlertid utfordrende, og det er mer utfordrende i dag enn det var tidligere. Det enorme tilfanget av offentlig tilgjengelige data, kombinert med tilgang til stadig billigere og mer kraftfull analyseteknologi, har bidratt til å øke faren for reidentifisering. Skillet mellom anonyme opplysninger og personopplysninger er blitt mindre tydelig. Det gjør det viktig å foreta grundige risikovurderinger i forbindelse med anonymisering av data, og å bruke solide anonymiseringsteknikker.

  Datatilsynet vil vurdere hvorvidt det bør reageres med sanksjoner overfor selskap som bevisst forsøker å reidentifisere opplysninger i anonyme datasett som de har kjøpt eller på annen måte erverver seg fra andre selskap. Selskaper som selger anonymiserte datasett bør skrive inn et forbud mot at kjøperne forsøker å reidentifisere opplysningene i kontraktsvilkårene.

  Det er også viktig at selskap som bygger profiler som inneholder pseudonyme opplysninger er klar over at pseudonyme opplysninger er definert som personopplysninger og derfor må behandles i tråd med personopplysningslovens bestemmelser.

[116] Artikkel 29-gruppen tar til orde for bruk av ikoner i Opinion 02/2013 On apps on smart devices.

Anbefalinger for å fremme bedre innsynsmuligheter og valgfrihet

- **Automatiserte innsyns- og utleveringsløsninger.** Virksomheter bør utvikle automatiserte løsninger som gir brukeren tilgang til og mulighet til å få utlevert alle data som ligger lagret om vedkommende. Opplysningene må utleveres i et brukervennlig format.

- **Gi innsyn i profilen.** For å sikre størst mulig åpenhet rundt bygging av profiler, bør brukeren gis innsyn i sin profil. I dette ligger at den enkelte bør gis innsyn i hvordan profilen er bygd opp, for eksempel hvilke segmenter og kategorier brukeren er plassert i. Den enkelte bør også få informasjon om fra hvilke kilder de ulike personopplysningene er hentet.

- **Det må gjøres lettere å velge sporfrie alternativer**. Transaksjonskostnadene forbundet med å unnslippe sporing er i dag for høy. Folk velger det alternativet som er lettest tilgjengelig, og det er som oftest det alternativet der man blir sporet. Muligheten til å si nei til sporing må være godt synlig og enkelt tilgjengelig for brukeren.

- **Lag valgpaneler for personvern («privacy dashboards»).** Brukeren bør få mulighet til selv å velge i hvor stor grad hun ønsker å bli sporet for å få brukertilpasset innhold og annonser. Publisister og andre relevante aktører bør utvikle løsninger der brukeren selv kan stille inn hvilke opplysninger som kan samles inn, hva opplysningene kan brukes til, hvem som kan få tilgang til opplysningene og så videre. Google, Microsoft og Facebook har utviklet løsninger der brukeren til en viss grad kan styre grad av personvernbeskyttelse.

Bransje- og myndighetssamarbeid, innebygd personvern og personvern på timeplanen

- **Godt personvern er godt forbrukervern.** Datatilsynsmyndigheter og forbrukermyndigheter bør jobbe tettere sammen for å sikre større åpenhet og bedre valgfrihet for den enkelte. Den målrettede markedsføringen som skjer via internett reiser spørsmål både etter personopplysningsloven og markedsføringsloven. For eksempel har den individuelt tilpassede markedsføringen mer karakter av å være direktemarkedsføring enn generisk markedsføring. Annonsørene kan nå rette markedsføringen sin mot utvalgte individer på nett. Som bruker av internettjenester blir du ikke gjenstand for oppmerksomhet fra annonsørene som sådan. Du blir gjenstand for oppmerksomhet fra enkelte annonsører som er særlig interessert i akkurat deg. Annonsørene kan forfølge deg på tvers av tjenester og sørge for at du blir eksponert for den samme markedsføringen igjen og igjen. Utfordringene knyttet til innsamling av personopplysninger på den ene siden og selve markedsføringen på den andre, glir over i hverandre. Det gjelder blant annet spørsmålet om den enkeltes mulighet til selv å bestemme hva han eller hun skal bli gjenstand for.

- **Bransjenorm.** Publisister, mediebyråer og annonsører bør komme sammen og lage retningslinjer som bidrar til å skape større åpenhet om hvordan markedet for målrettet markedsføring fungerer. Retningslinjene bør ivareta hensynet til personvernet på en bedre måte enn i dag. Aktørene i markedsføringskjeden bør dokumentere etterlevelse av felles retningslinjer overfor hverandre, og dette bør være grunnlaget når aktørene ber om forbrukerens tillit.

  Bransjeorganisasjonene bør opprette etiske komiteer der utnyttelse av personopplysninger til markedsføringsformål diskuteres opp imot hensynet til forbrukernes personvern. Nye forretningsideer og teknikker for målretting bør diskuteres i den etiske komiteen før de settes ut i livet. Bransjeorganisasjonene bør videre oppfordre sine medlemmer til å utvikle nye systemer etter prinsippene om innebygd personvern. Innebygd personvern innebærer at det tas hensyn til personvern i alle fasene av et systems utvikling, i rutiner og i forretningspraksisen.

- **Utvikling av personvernvennlige målrettingssystemer.** Datatilsynet vil fremme forskning på utvikling av mer personvernvennlige målrettingssystemer. Det finnes allerede forskere som hevder å ha utviklet målrettingssystemer som er like effektive som de som er i bruk i dag, men som ivaretar personvernet til brukerne ved å blant annet beskytte deres identitet ved bruk av anonymiseringsteknikker. [117]

- **Personvernvennlig bruk av data i markedsføring på pensum**. Etisk bruk av personopplysninger og kunnskap om personvern og personvernlovgivningen må inn på pensum ved universiteter og høgskoler som underviser i markedsføring, journalistikk og informasjonsteknologi.

[117] Tran, Minh-Dung, Gergely Acs and Claude Castelluccia, «Retargeting Without Tracking», INRIA, 2015, Frankrike, http://arxiv.org/pdf/1404.4533.pdf

Litteraturliste

Aftenposten, «Liten dings skaper store endringer», 16.03.2015, http://www.aftenposten.no/kultur/Liten-dings-skaper-store-endringer-7939980.html

Analysen, «Vil markedsførerne ha behov for markedsanalyse i fremtiden?», Analysen nr. 3, 2013, http://www.tns-gallup.no/tns-innsikt/vil-markedsforerne-ha-behov-for-markedsanalyse-i-framtida

Acxiom, «Casestudy: The Guardian, Boosting audience engagement across the globe», 2014, http://dq2qu0j6xxb34.cloudfront.net/wp-content/uploads/2014/02/The-Guardian.pdf

Adweek, «Google's Latest Role: The Cookie Monster. Ad tech firms are on alert», 11.11.2013, http://www.adweek.com/news/technology/google-s-latest-role-cookie-monster-153712

Article 29 Data Protecion Working Party – uttalelser og arbeidsdokumenter:

- Opinion 2/2010 on online behavioural advertising (WP 171)
- Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising (WP 188)
- Opinion 02/2013 on apps on smart devices (WP29)
- Opinion 03/2013 on purpose limitation(WP29)

Bizreport, «Platform creates customer profiles using Myers Briggs types», 19.04.2012, http://www.bizreport.com/2012/04/platform-creates-customer-profiles-using-myers-briggs-types.htmlSmith

Business Insider, «Eric Schmidt: Google's Policy Is To «Get Right Up To The Creepy Line And Not Cross It», 01.10.2010, http://www.businessinsider.com/eric-schmidt-googles-policy-is-to-get-right-up-to-the-creepy-line-and-not-cross-it-2010-10

Business Insider, «Google Is Now Bigger Than Both The Magazine And Newspaper Industries», 12.11.2013, http://www.businessinsider.com/google-is-bigger-than-all-magazines-and-newspapers-combined-2013-11

Calo, Ryan, «Digital Market Manipulation», 82 George Washington Law Review 995 (2014); University of Washington School of Law Research Paper No. 2013-27, 2013, http://dx.doi.org/10.2139/ssrn.2309703

Dagens Næringsliv, «Dette vet mediekjempene om oss», 19.10.2014, http://www.dn.no/etterBors/2014/10/19/2057/Kommentar/dette-vet-mediekjempen-om-oss

Dagens Næringsliv, «Kjemper om reklamebørs», 01.05.2015, http://www.dn.no/etterBors/2015/05/01/2052/Reklame/kjemper-om-reklamebrs

Dagens Næringsliv, «Vil bevise reklameeffekt», 31.07.2015

Datatilsynet, «Anonymisering av personopplysninger. Veileder, 2015», 2015, http://www.datatilsynet.no/Global/04_veiledere/anonymisering-veileder-240815.pdf

Datatilsynet, «Big Data, Personvernprinsipper under press», 2013, http://www.datatilsynet.no/Global/04_planer_rapporter/Big%20Data_web.pdf

Delta Projects, «Nåværende Programmatic status i Norge», 2014 http://www.deltaprojects.com/assets/programmaticstatusnorway.pdf

The Economist, «Little Brother, Special Report on Advertising and Technology», 13.09.2014, http://www.ogilvydo.com/wp-content/uploads/2014/09/20140913_SR_MAILOUT.pdf

Europarådet, «Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling», 2010, https://wcd.coe.int/ViewDoc.jsp?id=1710949

European Data Protection Supervisor, «Privacy and competitiveness in the age of Big Data: The interplay between data protection, competition law and consumer protection in the Digital Economy», 2014, https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf

Federal Trade Commission, «Data Brokers. A Call for Transparency and Accountability», 2014, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

Financial Times, «How much is your personal data worth?», 12.06.2013, http://www.ft.com/intl/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html#axzz3lAaLdwax

Gutwirth, Serge og Mireille Hildebrandt, «Some Caveats on Profiling», in Gutwirth, Serge, Yves Poullet og Paul De Hert (eds), *Data Protection in a Profiled World*, s 31 – 41, Springer, Dordrecht, 2010

IAB Europe, «An Introduction to Programmatic Trading Webinar», 2014 http://www.iabeurope.eu/files/8914/2789/7694/IAB_Europe_Introduction_to_Programmatic_Webinar_slides.pdf

IAB Europe, «Programmatic Trading. An IAB Europe White Paper», 2014, http://www.iabeurope.eu/files/8614/0776/0957/IAB_Europe_Programmatic_Trading_White_Paper_July_2014_v2.pdf

Le Monde Diplomatique, «Reklamerevolusjonen», november 2013, http://www.lmd.no/?p=13010

McCafferty&co, «European Media Conglomerate RTL Group Purchases SpotXchange, Paving the Way for Broadcasters to Keep Traditional Ad Dollars without the Traditional Ad Model», 01.03.2015, http://mccaffertyco.com/european-media-conglomerate-rtl-group-purchases-spotxchange-paving-the-way-for-broadcasters-to-keep-traditional-ad-dollars-without-the-traditional-ad-model/

de Montjoye, Yves-Alexandre, César A. Hidalgo, Michel Verleysen og Vincent D. Blondel, «Unique in the Crowd: The privacy bounds of human mobility», Scientific Reports 3, Article number: 1376, 2013, http://www.nature.com/articles/srep01376

The New York Times, «When Algorithms Discriminate», 9.7.2015, http://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html

Olejnik, Lukasz, Tran Minh-Dung og Claude Castelluccia, «Selling Off Privacy at Auction», 2013, HAL Id: hal-00915249, https://hal.inria.fr/hal-00915249

Ot.prp. nr 92 (1998 – 1999) om lov om behandling av personopplysninger

Pando, «Al Gore says Silicon Valley is a 'stalker economy'», 11.06.2014, https://pando.com/2014/06/11/al-gore-says-silicon-valley-is-a-stalker-economy/

Pasquale, Frank, «The Black Box Society. The Secret Algorithms That Control Money and Information», Harvard University Press, Cambridge, MA, 2015

Polakiewicz, Jörg, «Profiling – the Council of Europe's Contribution» i artikkelsamligen «European Data Protection: Coming of Age», Red: Gutwirth, Serge, Ronald Leenes, Paul de Hert og Yves Poullet, Springer, Dordrecht, 2013

Rao, A., F. Schaub og N. Sadeh, «What do they know about me? Contents and concerns of Online Behavioral Profiles», Carnegie Mellon University, 2014, https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab14011.pdf

Smith, Mike, «Targeted. How Technology Is Revolutionizing Advertising and the Way Comnpanies Reach Consumers», Amacom, 2015

Sørgard, Lars, «Informasjonsasymmetri og konkurransepolitikk», publisert i: Stortingsmelding nr. 15 (2004-2005): Om konkurransepolitikken, Vedl. 1, s 95-109., Institutt for samfunnsøkonomi, Norges Handelshøyskole, Bergen, 2005

TechRepublic, «Windows 10 violates your privacy by default, here's how you can protect yourself», 4.8.2015, http://www.techrepublic.com/article/windows-10-violates-your-privacy-by-default-heres-how-you-can-protect-yourself/

Tran, Minh-Dung, Gergely Acs and Claude Castelluccia, «Retargeting Without Tracking», INRIA, 2015, Frankrike, http://arxiv.org/pdf/1404.4533.pdf

Turow, Joseph, Michael Hennessy og Nora Draper, «The Tradeoff Fallacy, How Marketers Are Misrepresenting American Consumers And Opening Them Up to Exploitation», Annenberg School for Communication, University of Pennsylvania, 2015, https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf

Turow, Joseph, «The Daily You. How the New Advertising Industry Is Defining Your Identity and Your Worth», Yale University Press, New Haven and London, 2011

USA Today, «Google may ditch 'cookies' as online ad tracker», 17.09.2013, http://www.usatoday.com/story/tech/2013/09/17/google-cookies-advertising/2823183/

The Wall Street Journal, «What they know. The Web's New Gold Mine: Your Secrets», 30.07.2010, http://www.wsj.com/articles/SB10001424052748703940904575395073512989404

The Wall Street Journal, «Websites Vary Prices, Deals Based on Users' Information», 21.12.2012, http://www.wsj.com/articles/SB10001424127887323777204578189391813881534

World Federation of Advertisers, «WFA guide to Programmatic Media. What Every Advertiser Should Know about Media Markets», 2014, http://www.wfanet.org/media/programmatic.pdf

Zuiderveen Borgesius, Frederik J.,»Behavioural Sciences and the Regulation of Privacy on the Internet», draft chapter to the book «Nudging and the Law - What can EU Law learn from Behavioural Sciences?», red. A-L Sibony & A. Alemanno (Hart Publishing), Institute for Information Law Research Paper No. 2014-02, Amsterdam Law School Research Paper No. 2014-54, 2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2513771

Zuiderveen Borgesius, Frederik J., «Personal data processing for behavioural targeting: which legal basis?», International Data Privacy Law, s. 1 – 14, 2015, http://idpl.oxfordjournals.org/content/early/2015/06/23/idpl.ipv011.full.pdf+html

Vedlegg 1: Oversikt over tredjeparter på norske nettaviser

Undersøkelsen gjennomført 4. september og 7. september 2015.

	Aftenposten	Dagbladet	Nettavisen	Adresse-avisen			Dagsavisen		Drammens tidende
Omtrent antall tredjeparter	40	43	69	37			36		48
Omtrent antall servere brukerens IP-adr sendes til	56	50	84	57			48		61
Omtrent antall cookies satt	114	115	196	139			92		156
Analyse	AT Internet Burt Google analytics MixPanel New Relic Rich TNS	Google analytics Hotjar Integral Adsciense TNS	Google analytics Net Ratings SiteCensus TNS	Burt Google analytics Media innovation group Rich TNS			TNS		Google analytics Net Ratings SiteCensus TNS

Markeds-føring	Adform Admeta AdScale ADTECH AppNexus BidSwitch Criteo Datalogix DoubleClick Emediate Facebook exchange Improve Digital Internet Billboard LiveRail MediaMath Pubmatic Right Media Rubicon Smart Adserver Trade Desk Turn Inc Videoplaza Yieldlab	Adform Admeta AdScale ADTECH Advertising.com AooNexur Bid Swch Casale Media Criteo Datalogix DoubleClick Facebook exchange Google Adsense Improve Digital Internet Bilboard LiveRail MediaMath Pubmatic Quantcast Right Media Rubicon Smart Adserver Trade Desk Turn Inc Yieldlab	[x+1] Acuity Ads AdAction Adap.tv Adform AdGear Adition Admeta AdScale Adscience ADTECH Advertising.com AppNexus BidSwitch BrightRoll Casale Media Connexity Criteo cXense Datalogix DataXu Digilant DoubleClick Dstillery EQ Advertising eyeReturn Facebook exchange	Adform Admeta AdScale ADTECH AppNexus BidSwitch Criteo cXense Datalogix DoubleClick Facebook Exchange Google Adsence Improve Digital Internet Billboard LiveRail MaxPoint Interactie PubMatic Right media Rubicon SMART Adserver Turn Inc. Videoplaza Yieldlab			Adform Admeta AdScale ADTECH AppNexus BidSwitch Criteo cXense Datalogix DoubleClick Emediate Facebook exchange Google Adsense Improve Digital Internet Billboard LiveRail MediaMath Pubmatic Right Media Rubicon Smart Adserver Trade Desk Turn Inc Yieldlab		[x+1] Adap.tv Adform Adition Adnologies ADTECH Advertising.com AppNexus Brandscreen BrightRoll Casale Media cXense Datalogix DoubleClick Emediate eyeview LiveRail MediaMath Moat Netseer Nexage OpenX Platform161 PubMatic Right Media Rubicion Smato spotXchange

			Google Adsense Improve Digital Internet Billboard LiveRail MediaMath Nexage Nugg.Ad OpenX Platform161 PubMatic Quantcast Right Media Rubicion Smato SMART Adserver spotXchange Tapad The ADEX Trade Desk Turn Inc Yieldlab						Tapad Trade Desk Turn Inc
Personvern							TRUSTe Notice		
Sporings-bilder **(for innhenting av informasjon)**	Aggregate knowledge Audience Science	eXelate Eyeota Linkpulse	Aggregate knowledge BidTheatre BlueKai	eXelate Eyeota LiveRamp			BidTheatre EXelate Eyeota		Aggregate knowledge Audience Science

	EXelate Eyeota LiveRamp Media optimizer Neustar Adadviser Optimizely Semasio	LiveRamp Media optimizer Neustar Adadviser Optimizely Rhytmxchange Rocket fuel Veruta	eXelate Eyeota Linkpulse LiveRamp Magnetic Media Optimizer Netmining Neustar Adadviser Rocket fuel ScoreCard Research beacon Semasio Videology	Media Optimizer Neustar Adadviser			LiveRamp Media optimizer Neustar Adadviser Videology		BlueKai Chango Linkpulse LiveRamp Media Optimizer Neustar Adadviser Rocket fuel ScoreCard Research beacon Videology
Widgets Social **(Verktøy for å legge til innhold)**	AddThis	Facebook coneckt Facebook Social plugins Google tagmanager Twitter Button	AddThis Facebook connect Twitter button	AddThis Facebook coneckt			Facebook coneckt Facebook social graph Facebook Social plugins Twiiter Badge		AddThis Facebook social graph
Er det oppgitt informasjon om hvordan tredjeparter behandler besøkendes person-opplysninger?	Generell overordnet informasjon. Ikke noe konkret om 3.-parters bruk.	Generell overordnet informasjon. Ikke noe konkret om 3.-parters bruk.	Generell overordnet informasjon. Ikke noe konkret om 3.-parters bruk.	Generell overordnet informasjon. Ikke noe konkret om 3.-parters bruk.			Ingen		Generell overordnet informasjon. Ikke noe konkret om 3.-parters bruk.

Vi benyttet analyseverktøyet Ghostery for å få frem hvilke tredjeparter som var til stede på sidene.

Avisenes personvernerklæringer

Aftenpostens: https://kundeportal.aftenposten.no/personvern/

Dagbladet: http://www.dagbladet.no/2009/08/18/nyheter/avtale/brukeravtale/plikter/7706966/

Nettavisen: http://www.nettavisen.no/vilkaar.html og http://www.nettavisen.no/datapolicy.html

Adresseavisen: http://www.polarismedia.no/datapolicy.jsp

Drammens Tidende: http://www.dt.no/tilgang/personvernpolicy/

Dagsavisen: Kunne ikke finne opplysninger på åpningssiden om behandling av personopplysninger.

Vedlegg 2: Beskrivelse av tredjepartsaktører på norske nettsider

Beskrivelsene er hentet fra hjemmesiden til de enkelte selskapene i september 2015.

Addthis
«The AddThis Audience Intelligence (Ai) platform transforms the real-time activity of 1.9 billion web visitors across 15 million sites into actionable tools to help you optimize your marketing and develop authentic audience relationships.»

Adform
«Adform is a cloud technology built for agencies and advertisers, who want to make display advertising the best performance channel by use of personalized targeting, real time bidding and rich media.»

Admeta
«Admeta is a company focused on delivering full service technology solutions for large online publishers helping them increase yield on online ad inventory. We are one of Europe's leading suppliers of online ad exchange solutions and are working with some of Europe's largest premium publishers.»

Adscale
«adscale is Germany's leading marketplace for digital advertising, bringing advertisers and website operators together to buy and sell video, display and text advertising.»

Adsniper
«AdSniper is an automatic ad placement system, modifying costs in real-time according to the changes in the campaign results.» Translated by AdSniper LLC

Adtech
«The company's flagship product is an integrated ad serving platform - amended by features for mobile devices and video ads. These enable web publishers to manage, serve and evaluate virtually any kind of online advertising campaigns. ADTECH allows its customers to enhance efficiency, reliability and ROI in their online advertising businesses.»

Appnexus
«AppNexus is the world leader in real-time advertising technology, serving the largest and most innovative companies in the ecosystem on both the buy and sell side. AppNexus offers the industry's most advanced display advertising platform to empower companies to build, manage and optimize their entire display advertising businesses.»

At Internet
«AT Internet is an independent and trustworthy company that enables an integral analysis of websites, intranet and mobile sites.»

Audience Science
«Manage all of your data and digital media in one advertiser-owned SaaS based system with complete control, transparency and efficiency across your entire ad spend. The AudienceScience® Helios technology combines control and ownership of data with 100% media spend transparency. This enables advertisers to store and analyze BIG data, build proprietary audiences, target those audiences across display, video and mobile—in real time—and all within a single, fluid system. Advertisers can now fully and seamlessly manage both their data and buying in one system, enabling safe and effective targeted advertising.»

BidSwitch
«IPONWEB has a vision for RTB and Media Trading that is open, transparent and allows many different kinds of businesses to trade and sell media in real-time... Operating as an infrastructure-level «Switch», the BidSwitch facilitates both Supply and Demand technology partners to efficiently and transparently connect, trade and manage multiple RTB partners.»

Burt
«Burt creates software to help advertisers and agencies improve the efficiency and effect of their online campaigns.»

Criteo
«Criteo's advanced technology enables online e-commerce sites to re-engage with potential customers who have left their website via dynamic banners containing the most relevant product specific recommendations that are generated in real-time for each individual.»

Datalogix
«Even as consumers spend more and more time online, over 85% of purchasing still occurs offline. DLX is the first company to connect the online and offline silos. The result is a first-time, precise digital ROI metric. Now, DLX partners in CPG, Automotive, and Retail verticals have the ability to measure the impact online advertising campaigns have on sales across channels.»

Doubleclick
«Google's DoubleClick products provide ad management and ad serving solutions to companies that buy, create or sell online advertising.»

Emediate
«Emediate is the leading provider of ad serving technology in the Nordic region.»

Exelate
«We make the process of accessing online audiences simple, safe, and scalable by arming data buyers and data owners with proprietary technology that automates data connections and centralizes audience management. Through our DataLinX data management platform, we enable transparent, secure, private data connections for publishers, data owners and marketers.»

Eyeota
«Eyeota is an audience-targeting data technology company and the leading source for 3rd party audience targeting data for advertisers across Asia-Pacific, Europe and Australia… Eyeota's solutions are driven by strong, proprietary, data management platform (DMP) and marketplace technologies. Eyeota supplies 3rd party data to all major global and regional ad buying platforms, DSPs and ad networks.»

Facebook connect
«Build with the Open Graph. Integrate deeply into the Facebook experience. Grow lasting connections with your users.»

Facebook exchange
«Through Facebook Exchange, advertisers and agencies have been able to use cookie-based targeting through Demand-Side Platforms (DSPs) to reach their audience on Facebook with more timely and relevant messages. For brands and agencies, the result is a powerful tool for driving direct response goals on Facebook.»

Facebook social plugins
«Social plugins are tools that other websites can use to provide people with personalized and social experiences. When you interact with social plugins, you share your experiences off Facebook with your friends and others on Facebook.»

Google Adsence
«Many websites, such as news sites and blogs, join the Google Display Network, which enables Google to show ads on their sites. Based on your visits to these websites, Google uses an advertising cookie (from DoubleClick) to associate your browser with interest and demographic categories. Google then uses these categories to show interest-based ads on these websites. Google's Ads Preferences Manager lets you edit these categories associated with your browser. Using the Ads Preferences Manager, you can edit the list of inferred interest and demographic categories that Google has associated with your cookie or opt-out of the cookie entirely. All information Google gathers is used in accordance with Google's privacy policy and helps Google improve your online experience. It is not used to identify you personally and Google will not show interest-based ads based on personal information without your permission. We also will not show interest-based ads based on sensitive information or interest categories, such as those based on, race, religion, sexual orientation, health, or sensitive financial categories, without your opt-in consent.»

Google Analytics
«Google Analytics gives you insights into your website traffic and marketing effectiveness. We help you buy the right keywords, target your best markets, and engage and convert more customers.»

Google tag Manager
«Google Tag Manager is free and easy, leaving more time and money to spend on your marketing campaigns. You manage your tags yourself, with an easy-to-use web interface, rather than forcing you or your IT department to write or rewrite site code.»

Improve digital
«The company provides real time advertising technology to owners of premium digital media that want to build their own Private Ad Ecosystem. Improve Digital enables them to build, grow, manage, control, and optimise their own environment driving revenues from direct campaigns, RTB, ad networks, exchanges, trading desks and any other 3rd party media buyer.»

Internet Billboard
«The Internet BillBoard company develops and runs software solutions for a complex internet advertising management and runs the biggest internet advertising network in the Czech Republic and Slovakia. We develop and run the advertising management system BBelements AdServer, BBelements IntextServer and other products.»

Linkpulse
«Linkpulse is an analytics tool tailor made for high traffic news sites. Optimize and prioritize your front page backed by live data.»

Liverail
«LiveRail delivers technology solutions that enable and enhance the monetization of internet-distributed video.»

Liveramp
«LiveRamp helps marketers with CRM Retargeting and helps data companies onboard their offline data into anonymous cookies.» (Liveramp, formerly Rapleaf)

Media Innovation group
We provide marketing communicators with a single access point to every digital audience, and the technology platform to engage them in startling new ways.

Media Optimizer
«Adobe Media Optimizer provides customers the ability to deliver relevant ads to targeted audiences. Our technology provides both data management functionality and a unified campaign management platform that optimizes advertising campaigns across search, display and social.»

Mixpanel
«Mixpanel's mission is to help the world learn from their data. We offer the most sophisticated analytics platform companies online can use to understand how users behave. We do all of our data analysis in real-time.»

New relic
«New Relic is the all-in-one web application performance tool that lets you see performance from the end user experience, through servers, and down to the line of application code.»

Neustar Adadviser
«Our core mission is to provide the most comprehensive, accurate and up-to-date IP geolocation service. If your business is looking to improve your marketing and website's performance, enhance your customers' experience, ensure your customers' online safety or confidently comply with your industry's regulations, Neustar's IP geolocation services are right for you.»

Optimizely
«Optimizely, Inc. offers a range of website analytics services for A/B and multivariate testing purposes. Optimizely partners implement Optimizely as a way to better understand how their website is used.»

PubMatic
«PubMatic's ad monetization and management solution combines impression-level ad auction technology, the most comprehensive brand protection tools, and enterprise ad operations support to give the Web's premium publishers the most control over their revenue and brand.»

Rich
«Rich is the campaign analytics tool used by the world's leading digital agencies and advertisers.»

Right Media
«Right Media launched the first global digital advertising exchange in 2005, evolving to support the needs of businesses in today's digital media world. From sellers maximizing yield to buyers optimizing their ROI, businesses choose Right Media as the premium, trusted destination where they can build invaluable relationships.»

Rubicon
«Powered by the REVV Yield Optimization Platform, the REVV Marketplace is the world's largest premium display advertising marketplace, providing a single point of access for the over-whelming volume of opportunity that exists for publishers today. From international networks to DSPs to highly niche demand sources, publlshers can access it all via the REVV Marketplace, enabling publishers and their sales channels to transact efficiently, effectively and safely.»

Semasio
«The User Intelligence Platform enables you to turn all of the potentially hundreds of contacts you have with digital media users into data points from which a qualitatively new level of information is derived – information which belongs to you and only you.»

Smart AdServer
«Smart AdServer develops and markets premium ad serving solutions for media agencies and publishers to manage display campaigns for Web, mobile and iPad/tablets.»

TNS
«TNS is the world's largest Custom Market Research specialists. We provide quality marketing information delivered by Global Industry Sector expert consultants, innovative Market Research Expertise across the product life-cycle, in 80 countries.»

Tradedesk
«We power the most sophisticated buyers in advertising technology.»

Turn Inc.
«Turn has developed the digital advertising industry's only integrated, end-to-end platforms for data and media management. The Turn Audience Platform and Turn Media Platform are currently utilized to manage digital advertising campaigns for Global 2,000 brands. Turn's global infrastructure, intuitive software and analytics, and open ecosystem for partners – all available in a real-time integrated environment – represent the future of digital advertising.»

Twitter button
«Twitter is a real-time information network that connects you to the latest information about what you find interesting...At the heart of Twitter are small bursts of information called Tweets. Each Tweet is 140 characters in length.»

UserVoice
«UserVoice helps companies listen to their customers to build better products and improve customer satisfaction. We've built a platform that helps companies, from startups to Fortune 500's, collect feedback from thousands, and sometimes millions, of customers.»

Videoplaza
«Videoplaza empowers broadcasters, publishers and ad networks to maximise their advertising revenues from the New IP-delivered TV. Videoplaza's sell side ad management platform, Karbon, is used to monetise video experiences across PCs, mobile devices, tablets, game consoles, IPTV and Smart TVs.»

Yieldlab
«Our focus is on the development of software systems for the real-time trading and delivery of advertisements via digital channels. We enable web sites, marketers, media houses and publishers, to strengthen and optimize their business relations with agencies and advertising clients.»

Vedlegg 3: Ordliste

Ad call (annonsevarsel)
En ad call er et varsel som sendes fra avisens server til annonsebørsen for å varsle om at en bruker er i ferd med å laste ned en side der annonseflater må fylles med innhold.

Ad tag (annonsekode)
En ad tag eller annonsekode er knyttet til annonsene på siden som brukeren laster. Når denne koden når brukerens datamaskinen, sender den umiddelbart videre et varsel til annonsebørsen som avisen har en avtale med. Varselet som sendes fra avisens server via brukerens nettleser til annonsebørsen kalles en *ad call* (se over).

Aggregerte data
Statistiske data om flere individer som har blitt kombinert for å vise generelle trender eller verdier uten å identifisere enkeltindivider i datasettet. Aggregerte data er ikke nødvendigvis anonyme data.

Annonsebørs (ad exchange)
En annonsebørs er en markedsplass for kjøp og salg av annonseplasser, bygget opp etter samme prinsipper som finansbørsene. Annonsebørsene er en plattform for å drive med sanntidskjøp (real time bidding) der kjøpere av annonseplasser kan by på brukere lagt ut av publisistene. På de åpne annonsebørsene (i motsetning til de private børsene, se under) er det fri tilgang for alle aktører til å selge og kjøpe brukere side om side (begrenset tilgang for enkelte kategorier av nettsteder, eks. pornografiske nettsteder).

Anonyme data
Data som det ikke er mulig, ved hjelp av alle rimelige tekniske hjelpemidler, å knytte tilbake til en enkeltperson.

Anonymisering
Anonymisering er å gjøre personopplysninger anonyme. Datasett som kan knyttes til en identifiserbar person bearbeides med tanke på å gjøre tilknytningen mellom informasjon og individ umulig. Flere teknikker kan brukes for å nå målet om å gjøre opplysningene anonyme.

Artikkel 29-gruppen
Artikkel 29-gruppen er et uavhengig rådgivende organ i personvernspørsmål. I gruppen sitter representanter for de europeiske lands datatilsyn, fra EUs personvernmyndighet og fra EU-kommisjonen. Norge har observatørstatus i gruppen.

Beacon
Beacons eller nettvarder er en liten sensor som benytter blåtann-teknologi for å sende informasjon som kan mottas når en person kommer i nærheten av dem. Bruk av teknologien krever at brukeren har utstyr som kan lese den utsendte informasjonen.

Cookies
Se informasjonskapsler.

Cookie-matching (kapselkobling)
Cookie-matching er en avgjørende funksjonalitet i forbindelse med sanntidskjøp av unike brukere på børs. For at kjøpersiden skal kunne avgjøre hvorvidt de vil legge inn et bud, og ikke minst *hvor mye* de vil by, må de vite hvem brukeren er. Cookie-matching gjør det mulig å koble sammen data som befinner seg i databasen til selgeren og til kjøperen av brukeren.

Datahåndteringsplattform (Data Management Platform)
Data Management Platforms (DMP) er datavarehusteknologi som brukes for å organisere, sammenstille og analysere data fra mange ulike kilder. Formålet med en DMP er å sette sammen data på en slik måte at det gir et mest mulig rikt

bilde av den enkelte forbruker.[118] Målsettingen er å hjelpe markedsførere og publisister til å forstå sine kunder bedre. Den blir brukt til å segmentere og profilere kundebasen.

Dobbeltannonsering (re-targeting)
Re-targeting eller dobbeltannonsering er en betegnelse på når annonsører viser reklame for et produkt de allerede vet kunden har sett på. For eksempel kan de ønske å vise skoreklamer til en bruker de vet har sett på sko eller som tidligere har blitt eksponert for skoreklame.

Informasjonskapsel (cookie)
En informasjonskapsel er en liten fil som blir lagret i brukerens utstyr når brukeren besøker et nettsted. Hver gang brukeren besøker nettstedet, sender nettleseren informasjon tilbake til nettstedets server for å varsle nettsiden om brukerens aktivitet på siden. Selskap kan plassere ut informasjonskapsler som ligger lagret på folks utstyr over flere år, også mer enn ti år, eller bruke informasjonskapsler som slettes umiddelbart når nettsesjonen avsluttes.

IP-adresse
En IP-adresse er en unik identifikator som viser til en enhet, som en pc eller et nettbrett, i et nettverk som Internett.

Kjøperplattform (Demand Side Platform)
En kjøperplattform er programvare spesielt utviklet for å kjøpe brukere på annonsebørsene. En kjøperplattform kjøper brukere basert på målrettingskriterier (en algoritme) utviklet i samarbeid med annonsøren. Algoritmen er basert på sammenstilling av førstepartsdata og data hentet fra andre kilder.

Nettvarde
Se beacon.

Personopplysning
Er en opplysning eller vurdering som kan knyttes til deg som enkeltperson

Privat børs (Private Market Place)
En privat børs er en annonsebørs kontrollert av publisister der de legger ut brukere for salg til inviterte kjøperplattformer.

Profil
En profil er satt sammen av antagelser om et individs eller en gruppe av individers preferanser, evner eller behov. Antagelsene er utledet gjennom blant annet analyse av enkeltindividers surfehistorikk, oppdateringer i sosiale medier, leste nyhetsartikler, produkter kjøpt på nett og registrerte kundeopplysninger. Antagelser regnes også som personopplysninger, selv om det ikke er faktiske opplysninger.

Pseudonymisering
En prosess der direkte identifiserende parametere erstattes med unike indikatorer for ikke å direkte avsløre den virkelige identiteten til de registrerte.

Sanntidskjøp (real time bidding)
System for kjøp og salg av brukere i sanntid på annonsebørser. Systemet gjør det mulig for kjøpere av annonseplasser å estimere verdien av, og å legge inn bud på, unike brukere lagt ut av publisister. Annonsekjøperen som legger inn høyest bud på brukeren, vinner rettigheten til å vise vedkommende en annonse i det nettsiden lastes opp..

Selgerplattform (Supply Side Platform)
En selgerplattform er programvare utviklet for å legge ut ledig annonseflate og brukere for salg på annonsebørser.

Sensitive personopplysninger
Opplysninger om rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning, at en person har

[118] IAB Europe, «Programmatic Trading. An IAB Europe White Paper», 2014, http://www.iabeurope.eu/files/8614/0776/0957/IAB_Europe_Programmatic_Trading_White_Paper_July_2014_v2.pdf

vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, helseforhold, seksuelle forhold eller medlemskap i fagforeninger.

Sporingsbilde (web beacon)
Sporingsbilde (web beacon) brukes alene eller i kombinasjon med cookies for å skaffe mer informasjon om de besøkende til nettsiden. Et web beacon er vanligvis et usynlig grafisk bilde (vanligvis 1 pixel x 1 piksel) som er plassert på nettsiden. Web beacons brukes også av tredjeparter til å samle inn opplysninger om brukerne og som en mekanisme for å plassere ut cookies. Sporingsbilder kan brukes til å samle inn opplysninger om blant annet brukerens IP-adresse, tidspunktet for når nettstedet ble besøkt, hvilken nettleser brukeren har med mer.

Web beacon
Se billedsporing.

Besøksadresse:
Tollbugata 3, 0152 Oslo

Postadresse:
Postboks 8177 Dep., 0034
Oslo

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no