# Semesteroppgave IN3210: Mobilsporing/ADINT

## Introduksjon – Hva er ADINT?

ADINT (Advertising-based Intelligence/intelligent markedsføring) er målrettet annonsering rettet mot brukere av nettsteder og apper. Data fra brukere spores på tvers av nettsteder og apper med hensikt om å samle inn data om interesser og preferanser. Informasjonen som samles inn blir igjen benyttet til å velge hvilke annonser brukeren presenteres for på nett, som gir annonsørene markedsføring direkte rettet mot interessegruppen.

Mengden av personlige data som samles inn er gjerne stor og kan inneholde informasjon om alt fra interesser til hvilke varer brukeren er interessert i, også informasjon om brukerens fysiske plassering. Denne sporingen på tvers av nettsteder kan være problematisk ettersom det også er mulig for aktører med onde hensikter å skaffe seg tilgang til informasjonen, på samme måte som de som kjøper den for reklameformål.

Derfor er det interessant å se på teknologien bak intelligent, målrettet markedsføring, den pågående debatten om hvor trygge personopplysningene våre er, og hvilke sikkerhetsrisikoer som eksisterer.

## Oversikt/Historie

Reklame og annonsering har tradisjonelt foregått via medier som TV, aviser, radio og reklameplakater, hvor den ofte treffer en stor gruppe mennesker, som ikke nødvendigvis er i målgruppen. Da internett kom og bruken økte rundt 1993-94 begynte mange også å reklamere på internett. Rundt slutten av 1990-tallet ble det vanlig å samle internett, telefoni og kringkastingen på et felles nettverk underlagt internett-protokollen, også kalt IP. Fra rundt 2010 ble sosiale medier mer og mer utbredt, og rundt denne tiden ble det også vanlig å ha mobiltelefoner med internett. Med denne utviklingen ble det også behov for måter å reklamere mer effektivt på. En viktig oppfinnelse i denne sammenhengen var cookies. (1)

**Cookies**

Cookies ble oppfunnet i 1994 av den da 23 år gamle amerikaneren Lou Montulli for nettleseren til selskapet Netscape. Netscape var selskapet som bygde en av de første nettleserne som ble brukt i utstrakt grad. Formålet med cookie-teknologien var å løse problemet med at nettsidene ikke gjenkjente brukeren, som gjorde at brukerne ble behandlet som fremmede ved hvert besøk på siden. Nettleserne manglet altså minne. Montulli vurderte en rekke andre løsninger først, blant annet å gi hver bruker en unik, permanent ID som nettleseren så deler ut til alle sidene brukeren besøker. Dette hadde vært en enklere løsning, men Montulli og Netscape valgte den bort i frykt for at den ville gjøre det mulig for tredjeparter å spore brukernes søkehistorikk. De valgte i stedet å gå for cookies.

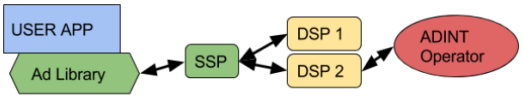
**Sikkerhetsutfordringer – tredjeparts cookies**

Da Montulli og Netscape skapte cookies, var sikkerhet og personvern et viktig fokus blant de store nettselskapene. De var derfor opptatt av at brukerne selv skulle kunne velge om de ville bli husket av en nettside eller ikke. Til tross for dette ble de i 1996 oppmerksomme på at annonsører hadde begynt å bruke cookies til å spore folk på nettet, og ble stilt overfor valget om å gjøre ingenting, og la annonsørene holde på, eller å blokkere tredjeparts cookies helt. De falt ned på å heller skape en mer nyansert løsning, der brukeren i større grad har kontroll over sine egne cookies. For å gjøre dette la de til funksjonalitet i nettleseren som gjorde det mulig for brukeren å se hvilke cookies som fantes på PCen og velge å slå av og på cookies for en nettside eller for alle nettsider.

Begrunnelsen for at tredjepart cookies ble bevart var at annonsering allerede hadde blitt den eneste inntektskilden for mange nettsteder, og at hele nettets fremtid var avhengig av reklame på nett. Cookies er fremdeles viktig for nettsteder og aktører på nett sin overlevelse, ettersom de bidrar til reklameinntekter og gjør det mulig å huske handlekurv i nettbutikkene. Et annet argument for cookies er at brukerne får gratis innhold og mer brukervennlighet mot at de deler informasjon om bruk. (2) (3)

## Definisjon/tekniske detaljer

Prosessen med å levere en annonse til en bruker av en nettside er kompleks. Den består av et publikum (brukeren) og en eier av en nettside eller app. Eieren av nettsiden inkluderer gjerne et reklame-bibliotek på siden tilbudt via en SSP (Supply-Side Provider), som kontrollerer kjøp og salg av reklame-plasser gjennom å auksjonere de ut til DPSer (Demand-Side Providers). Jo mer informasjon en SSP kan tilby, jo høyere bud kan de også få, og denne




**Figur 1: Prosessen der en annonse blir levert til brukeren. Pilene viser HTTP(S)-forespørsler (4)**

prosessen foregår gjerne automatisk. Den minste bestanddelen i informasjonen som sendes er cookies.(4)

## Hva er cookies/informasjonskaplser?

Cookies, eller informasjonskapsler, er mikroskopisk tekstfil som slippes fra nettleseren over på datamaskinens harddisk når man besøker en nettside. Cookies inneholder ingen personidentifiserende informasjon, men samler inn informasjon om interaksjoner på nettsiden, for eksempel hva man har klikket på, om man er logget inn, eller handlekurven i nettbutikken. Siden cookies kun inneholder data samlet inn av nettleseren, samles det heller ikke inn personlig informasjon fra harddisken.

Hver cookie har en medfølgende header bestående av et navn, en verdi, en utløpsdato og nettsiden den kommer fra. Headeren, med beskrivelser av hvordan innholdet skal tolkes og håndteres, blir fjernet fra dokumentet før det vises av nettleseren. Headeren er bare en del av en cookie idet den blir laget, og forsvinner når cookien lagres på harddisken. Eksempel på en header er:

Set-Cookie: NAME=VALUE;
expires=DATE; path=PATH;
domain=DOMAIN_NAME; secure (3)

## Hvordan fungerer cookies?

Cookies fungerer ved at når man skriver inn en nettadresse i nettleseren på mobilen eller datamaskinen, blir det automatisk søkt på harddisken til datamaskinen eller i nettleseren på telefonen etter allerede eksisterende cookies assosiert med nettsiden. Hvis siden tidligere er besøkt, gjenkjennes den unike identifikasjons-koden (UID) for datamaskinen, eller mobiltelefonen, som ligger lagret i en cookie-fil på harddisken eller i nettleser-appen, og nettleseren overfører innholdet i cookie-filen tilbake til siden. Hvis siden ikke tidligere er besøkt tilegnes brukeren en unik id, og det lagres en ny cookie-fil på maskinens harddisk eller mobiltelefonens nettleserapp. (3)

Cookies i nettlesere vil forsvinne dersom man lukker nettleseren eller skrur av telefonen, i motsetning til på PC. I apper eksisterer cookies kun innad i hver enkelt app, dersom appene har en innebygd nettleser eller viser reklame. Ettersom det er vanskelig å spore brukeraktivitet på tvers av apper, er det vanskelig for annonsørene å benytte seg av målrettet reklame i apper. På samme tid er 86% av tiden på mobiltelefoner brukt i apper, mens bare 14% av tiden brukes i nettleseren, og annonsører søker derfor å finne ny teknologi som gjør det mulig å spore på tvers av apper. (5)

## Ulike typer cookies

Det finnes mange ulike typer cookies, med ulike «arbeidsoppgaver». Noen, kalt «preferance cookies», husker hvilke innstillinger man ønsker på siden. Andre finner ut hvor man er i verden, om man vil fortsette å være innlogget på siden, eller hvilke annonser man har sett og

hvilke man har klikket på. Den vanligste informasjonskapselen kalles «visitor cookie», og holder oversikt over hvor ofte brukeren returnerer til siden. Denne gir informasjon til administratorer om hvilke sider som blir mest besøkt.
I tillegg skiller man mellom cookies tilhørende eierne av nettsiden og såkalte tredjeparts cookies, som plasseres på nettsiden av annonsører i et samarbeid med eierne av nettsiden. Data som samles inn kan derfor tilkomme både nettside-eierne og tredjepartsannonsørene.

En type cookie kalt «tracking cookies» er mer kontroversiell, ettersom den samler inn informasjon om hvilke nettsider man har besøkt og hvilke shoppingvaner man har, for så å opprette en anonym profil av brukeren. Når det eksisterer visse cookies, eller en kombinasjon av cookies, på PCen eller telefonen, blir den anonyme profilen lagt inn i et segment basert på aktuelle annonser. Annonsører bruker deretter denne inndelingen til å levere annonser de tror vil være mest relevante for brukeren. Brukeren blir ikke personlig identifisert, og det benyttes ingen personlige data til å definere hva brukeren kan være interessert i. Men det benyttes en profil skapt av cookies, som igjen kan knyttes til en bestemt PC eller mobiltelefon.

### Web bug

I tillegg til cookies brukes ofte såkalte «web bugs». En web bug er grafisk fil som blir plassert på en nettside eller i en e-mail for å monitorere brukeraktiviten ved å levere informasjon om bruk fra brukerens datamaskin til en tredjepart. Web bug brukes ofte sammen med cookies, men i motsetning til en cookie kan ikke web bugs velges bort, men eksisterer på siden på lik linje med bildefiler og andre filobjekter.
Web bugs kan blant annet gi informasjon om IP-adressen til mottakeren av en e-mail eller hvor ofte en melding leses.

## Sikkerhetsutfordringer

Ved innsamling av data fra informasjonskapslene hender ofte at personopplysninger blir behandlet. Personopplysninger defineres ifølge datatilsynet som «alle opplysninger og vurderinger som kan knyttes til deg som enkeltperson». Vanlige personopplysninger er navn, adresse, telefonnummer, e-post og fødselsnummer. I tillegg regnes IP-adresse og opplysninger om adferdsmønstre, for eksempel hva man handler, hvor man beveger seg osv. som personopplysninger. (6)

### Mobilsporing - Lokasjon

Lokasjonssporing, eller sporing av brukerens plassering, ved bruk av annonser er en måte personopplysningene som innhentes av cookies kan misbrukes på. Lokasjonssporing går ut på å levere annonser med GPS-informasjon til en bestemt bruker og på den måten få oversikt over hvilke steder brukeren oppholder seg på.

Sporingen gjøres ved at brukerens MAID først blir innhentet. MAID, eller Mobile Advertising ID, er en identifikator som unikt identifiserer en bestemt PC eller mobiltelefon for reklameformål. MAID kan innhentes gjennom for eksempel bruk av sniffing mot brukerens nettverkstrafikk, som er den vanligste metoden. Sniffing, også kalt pakkesniffing, er en form for passivt angrep der flyten av datapakker over nettverket blir overvåket og

pakker hentes ut, for at dataene så blir dekryptert til en leselig form. MAID kan også innhentes ved at brukeren klikker på en reklame som tilhører de som skal ha MAIDen eller benytter seg av apper som tillater at JavaScript overfører MAID i en web-forespørsel, uten interaksjon fra brukeren.
I sporingen lages det annonser rettet mot den innhentede MAIDen og i tillegg mot forskjellige GPS-lokasjoner. På denne måten får man et geografisk nett med et mønster av annonser som viser hvor brukeren har befunnet seg.
I en case-studie av Paul Vines mfl. (4), der disse teknikkene ble forsøkt, fant de at sporingen forutsetter at brukeren tar i bruk apper på de ulike lokasjonene og at de befinner seg der i minst 5 minutter, og nøyaktigheten av plasseringen er på rundt 8 meter. De fant også ut at det eneste som trengs er 1000 $ og en web-side for å spore hvor noen befinner seg, og i tillegg få tilgang til andre personopplysninger.
For å begrense denne type sporing og annen innhenting av personopplysninger, og bedre ivareta personvernet har vi lover og regler for bruk av cookies. (4)

## Lovverket

Bruken av cookies reguleres i dag av loven om elektronisk kommunikasjon (ekomloven), som tredde i kraft i 2003, kommunikasjonsdirektivet (ePrivacy-direktivet) fra 2002, og personopplysningsloven. Ekomloven reguleres igjen av Nasjonal kommunikasjonsmyndighet (NKOM) i samarbeid med Kommunal- og moderniseringsdepartementet.
NKOM må også forholde seg til bestemmelser i EU, og den 1. oktober i 2019 ble det avsagt en dom i EU som omhandlet artikkel 5 i kommunikasjonsdirektivet, hvor det slås fast at det kreves et *aktivt* samtykke for bruk av cookies. Det vil si at brukeren aktivt må krysse av for samtykke, fremfor at det er et ferdig avkrysset felt, og gjelder uavhengig av om det er snakk om personopplysninger eller ikke. Denne dommen fungerte som en presisesing av hvordan kommunikasjonsdirektivet skal forstås. (7)

## «Cookie law»

Kommunikasjonsdirektivet, også kalt ePrivacy-direktivet eller «cookie law», er en essensiell del av lovverket for datasikkerhet i EU, og har som hovedformål å sikre alle innbyggere i EU sitt privatliv på nett gjennom databeskyttelse. Direktivet ble først vedtatt av EU i 2002, og endret i 2009. Formålet med direktivet var å gi brukeren et forsvar mot sporing på nett, person-profilering, uønsket reklame og uønsket innhenting av data. I ePrivacy-direktivet heter det at «ingen informasjonskapsler eller sporere må plasseres før forhåndsgodkjenning fra brukeren, utenom de som er strengt nødvendige for grunnfunksjonen til nettstedet».
Europa er med en egen cookie-lov i tillegg til GDPR (General Data Protection Regulation) i front i verden når det gjelder databeskyttelse. (8)

## Fordeler og ulemper

Som tidligere nevnt ble det vurdert både positive og negative sider ved cookies da de først ble tatt i bruk. Et argument for cookies er at de gir brukeren gratis innhold i bytte mot reklame på

nett. Uten cookies hadde ikke internett vært like omfangsrikt som det er i dag, ettersom det hadde vært vanskeligere for innholdskapere å leve av internett. Samtidig bidrar de til økt brukervennlighet ved at de for eksempel husker handlekurv i nettbutikker, eller hvilke innstillinger man ønsker på siden. Uten cookies hadde man fortsatt å se reklame på nettet, men den ville vært mindre relevant for brukeren og hans eller hennes interesser.
I tillegg er det nå lettere for brukeren å velge om man vil skru cookies av eller på, noe som i de fleste tilfeller gjør brukeren i stand til å velge om han eller hun ønsker å dele cookies med nettside-tilbyder og eventuelle tredjeparter. Dette bidrar til å gi brukeren mer kontroll over sine egne personopplysninger.
For eieren av nettsteder og for annonsører har cookies flere fordeler. Annonsørene får vist frem produktet sitt direkte til målgruppen, og får med det mulighet til å øke salget og styrke merkevaren. Eieren av nettsidene tjener penger på at noen besøker siden deres, noe som gjør det mulig å tilby gratis innhold til brukere, og igjen skape mer interesse for nettsiden.

En ulempe med cookies er at de også kan benyttes av ondsinnede aktører til formål som krenker brukeres personvern. I og med at man legger igjen personopplysninger, som GPS-data, hva man interesserer seg for, informasjon om hva man gjør i hverdagen og helseopplysninger, kan en ved profilering etter hvert få et mer og mer komplett bilde av hver enkelt bruker.
En annen problemstilling er hvor mye internett-brukere egentlig vet om online adferds-annonsering og cookies, og om de er i stand til å gi et informert samtykke basert på denne kunnskapen. En studie av dette viste at kunnskapen om cookies i den generelle befolkningen sannsynligvis er for lav til at de er i stand til å gi et informert samtykke. De fleste sjekker heller anti-virus, blokkerer pop-ups og sletter søkehistorikken fremfor å lese personvernerklæringen. Det kan kanskje skyldes at mange ikke er så bekymret for at dataene skal bli misbrukt, og at mangel på kunnskap og det at det kan oppleves som tungvint gjør at mange nedprioriterer det. (9)

## Forbedringer

Til tross for at mange er hverken bevisst på eller bekymret for personopplysningene sine, vil det snart bli enklere, i alle fall for Apple-brukere, å få oversikt over hvilke apper man blir sporet av. Under Apples utviklerkonferanse Worldwide Developers Conference 2021 varslet de at de vil bygge inn en «sladrefunksjon» for apper i iOS 15.2 beta. Denne funksjonen finnes allerede i nettleseren deres, Safari, og fungerer som en slags «personvernsrapport», som forteller brukere hvilke nettsteder som følger mest med på aktiviteten deres og hvilke sporingstjenester som benyttes. Disse nye funksjonene kan kanskje, om ikke forbedre sikkerheten, gjøre brukere bedre i stand til å ta kontroll over sine egne personopplysninger og bidra til å rette fokus mot personvern på internett. (10)

## Oppsummering/konklusjon

ADINT/ målrettet annonsering har vært essensielt for internett sånn vi kjenner det i dag. Det brukes både som et reklameverktøy og inntektskilde, og teknologien bak gjør det mulig å tilpasse brukeropplevelsen på nettsider. Samtidig finnes det sikkerhetsrisikoer ved at personopplysninger samles inn, og selv om det legges til rette for at man skal kunne ta informerte valg, hemmes dette av at bevisstheten og kunnskapen rundt bruken av cookies og målrettet reklame er lav. Dette er imidlertid noe som står høyt på agendaen hos store teknologiselskaper, som lanserer løsninger som gjør det enklere for brukere å se hvilken informasjon de deler med tredjeparter og nettside-tilbydere. Likevel kan det hende det rett og slett er for komplisert for hver enkelt å avgjøre hvilke personopplysninger man ønsker å dele, og at det kan bli utfordrende å finne løsninger som imøtekommer alle sikkerhetsutfordringene ved bruk av cookies.

# Kilder:


1. Rossen, Eirik; Liseter, Ivar M.; Nordal, Ola: "*Internetts historie*" i *Store norske leksikon* på snl.no. Hentet 25. november 2021 fra https://snl.no/Internetts_historie
2. Rivero, Nicolas: "*The inventor of the digital cookie has some regrets*", 26. Mai 2021. Hentet 25. November 2021 fra The inventor of the digital cookie has some regrets — Quartz (qz.com)
3. William T. Harding, Anita J. Reed & Robert L. Gray (2001) *"Cookies and Web Bugs: What They are and How They Work Together"*, Information Systems Management, 18:3, 17-24, DOI: 10.1201/1078/43196.18.3.20010601/31286.3. Hentet 25. November 2021 fra Cookies and Web Bugs: What They are and How They Work Together (uio.no)
4. Paul Vines, Tadayoshi Kohno, Franziska Roesner, *"ADINT: Using Targeted Advertising for Personal Surveillance"*, 2017. Hentet 25. November 2021 fra https://adint.cs.washington.edu/. 0.3in Exploring ADINT: Using Ad Targeting for Surveillance on a Budget —or —How Alice Can Buy Ads to Track Bob
5. Lele, Shruti: *"Cookies in Mobile: Do They Exist?"*, 18. Desember 2014. Hentet 25. November 2021 fra Cookies in Mobile: Do They Exist? | Social Media Today
6. Personopplysninger | Datatilsynet, sist endret: 17.07.2019.
7. Bruk av informasjonskapsler (cookies) | Datatilsynet, sist endret: 10.10.2019.
8. EU cookie law vs GDPR | Differences & Requirements | Cookiebot CMP , sist endret: 15. Februar 2020.
9. Edith G. Smit, Guda Van Noort, Hilde A.M. Voorveld, *"Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe"*, Computers in Human Behavior, Volume 32, 2014, Pages 15-22, ISSN 0747-5632. Hentet 25. November 2021 fra https://www.sciencedirect.com/science/article/pii/S0747563213004299
10. Jansen, Vegar: "*Snart forteller Apple hvilke apper som sporer deg"*, 28. Oktober 2021. Hentet 25. November 2021 fra Snart forteller Apple hvilke apper som sporer deg - Tek.no