

UiO : **Det juridiske fakultet**

Samtykke som behandlings- grunnlag ved bruk av informasjonskapsler (cookies)

Særlig om hvorvidt vilkårene for et gyldig samtykke er sammenstilt med kravene til samtykke etter personvernforordningen- GDPR

Kandidatnummer:

Leveringsfrist: 25.11.19

Antall ord: 17700



Forord

Denne avhandlingen har vært krevende, men utrolig lærerikt. Oppgaven har gitt meg en god mulighet til å foreta en selvstendig vurdering av problemstillingen.

Jeg vil rette en stor takk til min venn, advokatfullmektig Fredrik Wiker, for hans forslag om en utrolig spennende problemstilling. Jeg vil også takke min veileder, Ingvild Schiøll Ericson, for gode råd og god oppfølging. Jeg vil også vise stor takknemlighet til Jan Morten Andresen, daglig lederen i Cookie Information AS, for bidraget av tekniske kunnskaper og animasjoner til denne avhandlingen.

En stor takk til min utrolig snille venn, Toqir Shaffi, og min gode kollega, Heidi Lunde, for gjennomlesning av oppgaven. Jeg vil også takke, Advokatfullmektig Christian Werner Skovly, for gode og relevante innspill gjennom hele prosessen.

Sist men ikke minst, vil jeg takke min gode og støttende familie som viste mye forståelse i denne perioden.

Oslo, November 2019

Lema N. Wahabzadah

1. Innholdsfortegnelse

1.	INNLEDNING	1
1.1.	Tema og aktualitet.....	1
1.2.	Problemstillingen.....	4
1.2.1.	Struktur og metode	5
1.2.2.	Avgrensninger	5
1.3.	Videre fremstilling.....	6
2.	INFORMASJONSKAPSLER (COOKIES)	6
2.1.	Tekniske bakgrunnen.....	6
2.1.1.	Hvordan foregår kommunikasjonen på internett?	7
2.1.2.	Hva gjør cookies?	7
3.	HVORDAN ER INFORMASJONSKAPSLER REGULERT?	10
3.1.	Rettskildebildet og metodiske utfordringer.....	10
3.2.	Oversikt over sentrale rettskilder.....	12
3.2.1.	Ekomloven	12
3.2.2.	E-privacy-direktivet/ ekomdirektivet	12
3.2.3.	Personopplysningsforordningen - GDPR	13
3.2.4.	Personopplysningsloven	13
3.2.5.	Forholdet mellom ekomloven og personopplysningsloven	14
3.2.5.1.	Nyansere sontringen i virkeområdene til ekomdirektivet og personvernforordningen vedrørende cookies.....	16
3.2.5.2.	Particularise.....	17
	Her reises det spørsmål om hvorvidt det gjelder kun personopplysning eller alle slags opplysninger.....	18
3.2.5.3.	Complement.....	19
3.2.5.4.	Artikkel 95 av GDPR.....	19
3.2.5.5.	Vil de samme forholdene gjelde i forhold til ekomloven?.....	19
3.3.	Hva krever den EU/EØS rettslige forpliktelsen av norsk rett når det gjelder krav til samtykke til cookies, og hvordan er disse implementert i norsk rett?.....	20
3.3.1.	Metodisk tilbakeblikk	20
3.3.2.	Innholdet av reglene i område	20
3.3.3.	Informert samtykke	23
3.3.4.	Samtykke etter GDPR	27

3.3.4.1.	Vilkårene	28
3.3.5.	Er samtykke gyldig under tilfeller hvor samtykke til cookies er en forutsetning for bruk av tjenesten på nettsiden? 29	
3.3.5.1.	Frivillig.....	29
3.3.6.	På hvilke måter kan samtykke innhentes? 33	
3.3.7.	Hva slags krav stilles det til informasjonsplikten? 36	
3.3.7.1.	Må det informeres om lengden av behandlingen?	38
3.3.8.	Hvilke krav stilles det til formidling av informasjonen om samtykke til cookies? 39	
3.3.9.	Utformingen 40	
3.3.10.	Dark Patterns 41	
3.3.11.	Hvem er ansvarlig for at vilkårene er oppfylt? 43	
3.3.11.1.	«social plug-ins»	44
3.3.12.	Tidspunktet for innhentes av samtykke46	
3.4.	Unntak fra kravet om samtykke.....	47
3.4.1.	Hvilke informasjonskapsler er unntatt fra kravet om samtykke? 49	
3.4.2.	Nødvendige cookies 50	
3.4.3.	Funksjonelle cookies 50	
3.4.4.	Statistisk cookies52	
3.4.5.	Markedsførende/targeting cookies 53	
3.5.	Rettsvirkning av brudd	55
4.	AVSLUTTENDE TANKER	55
	LITTERATURLISTE.....	57

1. Innledning

1.1. Tema og aktualitet

Temaet for denne avhandlingen er kravet om samtykke som behandlingsgrunnlag for innhenting av opplysninger ved bruk av informasjonskapsler på nettsider.

Omtrent alle nettsider man besøker bruker informasjonskapsler. Det innhentes daglig et stort antall samtykker fra internettbrukere. Hittil, har det ikke vært en felles praksis om hvordan brukere skal samtykke og reglene rundt dette. Mange nettsider plasserer en liten boks med tekst enten under eller øverst i forsiden, hvor brukeren bes om å gi sitt samtykke. Andre innhenter samtykke gjennom innstillingene på brukerens nettleser.

Ettersom internettbrukerne ser anmodningen om samtykke hyppig, er det blitt en vane hos de fleste å trykke på et alternativ i teksten for å bli kvitt den. Mange er heller ikke klar over hvordan nettleser innstillingene deres er stilt. Det kan derfor bli stilt spørsmål ved hvorvidt et slikt samtykke anses for å være gyldig. Dette er viktig ettersom man gir samtykke til noe som i realiteten, er forbudt.¹

Personvern er et rettsområde som anses for å være meget spennende og dynamisk.² Den handler om retten til privatliv og retten til å bestemme over egne personopplysninger.³ Retten til privatliv er forankret både i Den europeiske menneskerettighetskonvensjonen art. 8 og i den norske Grunnloven § 102.

Personvern er ingen nytt fenomen. Den har eksistert lenge, men dens betydning endrer seg fra tid til annen.⁴ Opplysninger som folk ikke ville delt med sine venner eller naboer, er nå blitt helt normalt å dele på internett gjennom sosiale medier. Mange gjør dette uten å forstå betydningen og konsekvensene av det. Det er derfor både et behov for bevisstgjøring, men samtidig også sikring av individene gjennom rettsregler.

Personvernrettslige regler i Norge er i stor grad påvirket av og stammer fra rettsreglene i EU. Formålet med personvernrettslige regler er å sikre harmonisering av personvern i EU gjen-

¹ se punkt 3.3.2

² Bygrave, (2014), s.4

³ Datatilsynet, (2018)

⁴ Bygrave, (2014) s.8

nom regulering, og sørge for at brukerne får tillit til internett.⁵ Harmonisering av reglene fører til at individene har lik grad av beskyttelse i hele EU/EØS-område. Tilliten hos brukerne er essensielt for utvikling av økonomien i det indre markedet.⁶

Bakgrunnen for dette er at vi lever i en tid som kalles for «The era of big data»⁷. Utvikling av digitalisering har ført til at store mengder av opplysninger kan nå settes sammen på meget avanserte måter og finne opplysninger av betydning til ulike formål.⁸

Som Bill Gates sier «*if your buisness is not on the internet, then your buisness will be out of buisness*». Det er essensielt å ha en hjemmeside uansett hva slags virksomhet man driver med. Det kan f.eks. være detaljhandel i den private sektor helt til virksomheten i det offentlige. Det samles mye data av individer grunnet teknologi og organisatoriske endringer. ⁹

Teknologien fører til effektivitet, økning av næringslivets muligheter samt en mye bedre opplevelse for individer. Netthandel har økt globalt. EU borgernes personopplysninger er verdt 950 milliarder kroner.¹⁰ Norske forbrukere hittil i 2019 handlet for 163,4 milliarder kroner¹¹. I 2018 var tallene på ca 145 milliarder kroner. Det er klart det er økningen i norsk netthandel.

Opplysninger er derfor blitt en stor industri. En stor andel av opplysningene brukes til markedsføring. Den som samler opplysningene, kan enten selv bruke de eller selge disse til tredjeparter. Slik har mange t.o.m. bygget seg en forretningsmodell rundt kundeopplysninger. Ulempen for individer er at disse metodene kan misbrukes. Store økonomiske summer og mye opplysninger om brukere gjør at feltet må reguleres. Man må vite hvordan disse opplysningene samles, brukes og er regulert.

Opplysningene som samles, kan enten være adferdsdata eller demografiske opplysninger. Adferds opplysninger¹² er generert gjennom kundens oppførsel med nettsiden f.eks. hvilke

⁵ Ekomdirektivet art.1, GDPR art. 1, fortaler punkt 1-20, ekomloven § 1.

⁶ GDPR, fortale, punkt 7.

⁷ Kudyba, (2014) Introduction to the big data era, 8.7 Big Data.

⁸ Datatilsynet, (2017)

⁹ Bygrave, (2014) s. 9

¹⁰ Nyvold, (2018)

¹¹ Dibs, (2019)

¹² Cardinale

sider brukeren ser på, e-postadresse, konto osv. Demografiske opplysninger¹³ er opplysninger om karakteristikk av befolkningen som alder, kjønn, inntekt mv.

Det er tre måter opplysninger kan samles på.¹⁴ Den første måten, går ut på å spørre kunden direkte om opplysninger gjennom f.eks. kundeundersøkelser mv. Den andre måten, er å spore brukerne indirekte gjennom informasjonskapsler og andre sporeteknologier. Den siste måten, går ut på å samle opplysningene ved å kombinere andre kilder fra kunder til dine egne data.

Det er sporing gjennom informasjonskapsler som er hovedfokuset i denne oppgaven. Ved å gi sitt samtykke til cookies på en nettside, gir man en type tillatelse for at denne nettsiden kan bruke de lagrede opplysningene på din mobil eller PC, og spore deg.

Formålene med sporingen kan være å bruke opplysningene til forbedring av kundeopplevelser f.eks. for å tilgjengeliggjøre visse funksjoner eller samle inn statistikk over feil i systemet.¹⁵ Raffinering av markedsføringsstrategi, selge kundeopplysninger videre til tredjeparter og bruk av data til sikkerhet av opplysninger er også vanlige formål til samling og bruk av data.

Derfor er det av stor betydning for forretninger å kunne innhente opplysninger, men rettsområde er nå ganske strengt regulert. Overtredelse av disse kan føre til store gebyrer i bot¹⁶, noe som er en utgift forretninger vil helst unngå. Dessuten er tilliten til brukerne også meget viktig for virksomheten av en forretning. Denne tilliten får forretninger når de har behandle opplysningene til brukere i henhold til sikre lovlige krav. Derfor utgjør det en stor interesse for forretninger å innhente opplysninger på en lovlig måte.

Det har vært klart at man trenger samtykke fra brukerne av en nettside for å bruke deres opplysninger.

Imidlertid, har det i Norge vært mye usikkerhet rundt hvordan dataansvarlige skal få gyldig samtykke, når de samler opplysninger fra besøkende gjennom cookies.

Det har ført til at mange aktører ikke har brukt cookies på en lovlig måte. Empirien viser at 97% av norske offentlige nettsider ikke tilfredsstillt krav til gyldig samtykke for lagring av

¹³ Big Wave Media

¹⁴ Uzialko, (2018)

¹⁵ Ibid.

¹⁶ GDPR art. 83

opplysninger om besøkere gjennom cookies.¹⁷ Dessuten deler de opplysninger av brukere med tredjeparter, uten at brukerne har samtykket til dette.¹⁸ De fleste tredjeparter bruker opplysningene i markedsføringssammenheng.¹⁹

Det foreligger også fare for at opplysningene om norske borgere blir delt med aktører i land som ikke er ansett å ha et system som beskytter opplysningene på en tilfredsstillende måte.²⁰

1.2. Problemstillingen

I tillegg til personvernaspektet er det også et aspekt om sikkerheten til opplysningene som settes på spill.²¹ Sikkerhetsaspektet er også meget interessant, men i denne oppgaven er hovedfokuset personvernaspektet.

Problemstillingen formuleres dermed slik: hvilke vilkår som må være oppfylt i henhold til gjeldende rett for å ta i bruk informasjonskapsler. Hensikten er imidlertid ikke å gi en fremstilling av alle vilkårene og underproblemstillingene som berører samtykke generelt. Se punkt 1.3.1 og 1.3.2 avgrensninger.

For å kunne besvare hovedproblemstillingen, må det blant annet drøftes hva slags krav stilles det til innholdet av informasjonen som gis til internettkbrukeren, før samtykke kan oppnås. Noen viktige underproblemstillinger er hvordan selve anmodningen om samtykke må bli presentert for brukeren og hvilke midler kan man anvende til dette formålet. Hvem som er ansvarlig for oppfyllelse av kravene, og under hvilke tilfeller er det ikke stilt krav til samtykke.

¹⁷ Cookie Information, (2018) s.1 og 15

¹⁸ Ibid.

¹⁹ Cookie Information undersøkte 131 tilfeldigvalgte offentlige nettstedene i perioden 22. til 23. mars 2019. Det ble identifisert hvilke tredjeparter som lagret cookies i brukerens nettleser, og hvilke som hadde tilgang til allerede lagrede cookies. Etter en grundig gjennomgåelse av personvernerklæringene til de fleste tredjeparter, ble det funnet at markedsføring er hovedformålet til lagring og anskaffelse av tilgang til cookies. Se vedlagt fullstendige rapporten.

²⁰ Ibid s.14

²¹ Årnes, (2018) s. 279-284

1.2.1. Struktur og metode

Formålet med oppgaven er å ta opp vanskelige og tvilsomme problemstillinger under vilkårene for samtykke til bruk av cookies. Disse er valgt etter relevans og praktisk betydning i rettsområdet.

Som tidligere nevnt, foreligger det en del uklarheter i rettsområde. Denne oppgaven har til hensikt å bidra med til klargjøring ved å foreta en rettsdogmatisk analyse av vilkårene for avgivelse av samtykke ved bruk av informasjonskapsler. Med rettsdogmatisk analyse menes at innholdet i et krav fastlegges ved å identifisere relevante rettskilder, tolke disses innhold, for så å avveie rettsreglene mot hverandre ved hjelp av rettskildeprinsipper.²²

Det skal dermed foretas en rettsdogmatisk analyse av hvilke vilkår som må være oppfylt for at en nettside skal kunne bruke informasjonskapsler.

Opgaven har en teknisk side. Kunnskapen om den tekniske side ved cookies, er nødvendig for å kunne foreta den rettsdogmatiske analysen. Dette gjelder kunnskap om hva informasjonskapsler er, og hvordan disse fungerer. Denne delen er ikke-juridisk, og må forklares gjennom forklaringer fra informasjon -og kommunikasjonsteknologi, forkortet til IKT- eller IT.

Det utfordrende med denne delen av oppgaven var å finne faglig litteratur i form av bøker ettersom feltet er meget nytt, og er under stadig utvikling. Derfor er det vanskelig å kunne basere seg kun på litteraturbøker. Innhentede informasjon om de teknologiske forholdene i denne oppgaven stammer fra troverdige og oppdaterte artikler på internett og sakkyndige i selskapet Cookie Information AS.

1.2.2. Avgrensninger

Opgaven avgrenses mot de øvrige behandlingsgrunnlag i GDPR art. 6. Andre tekniske sporingsmekanismer enn cookies vil ikke bli behandlet. Det vil imidlertid påpekes i noen tilfeller hvorvidt de samme reglene vil også gjelde de.

Fornyelse av samtykke er et meget interessant tema, men behandling av disse går ut over drøftelse av kjerneproblemstillingene i oppgaven. Det avgrenses dermed mot drøftelse av disse i denne oppgaven. Kravet til eksplisitt samtykke og barnets samtykke vil heller ikke bli behandlet i oppgaven av samme årsak.

²² Eckhoff (2001), s.17-18.

1.3. Videre fremstilling

Detaljert tekniske informasjon blir presentert under de respektive rettslige tematikkene de er relevante for. Det er hensiktsmessig for en bedre forståelse av temaet. Innledningsvis, er det viktig å ha en grunnleggende forståelse av hvordan internettet fungerer, og hvordan informasjonskapsler brukes. Dette blir presentert under punkt 2. Drøftelsen om hvordan bruk av informasjonskapsler er regulert foretas under punkt 3.

Rettskildebildet og metodiske utfordringene blir presentert under punkt 3.1. En ryddig oversikt over sentrale rettskildene blir presentert under punkt 3.2, hvorav forholdene mellom ulike rettskilder også blir drøftet. Under punkt 3.3 ser vi nærmere på vilkårene til samtykke for cookies samt, de ulike underproblemstillingene. Under punkt 3.4 behandles tilfeller hvor man ikke har behov for å innhente samtykke fra brukerne for å anvende informasjonskapsler. Avslutningsvis, fremgår det en kort fremstilling av rettsvirkning av brudd på samtykkereglene.

2. Informasjonskapsler (cookies)

2.1. Tekniske bakgrunnen

En cookie er en informasjonskapsel som består av en «liten tekstfil som lastes ned og lagres på brukers datamaskin når brukeren åpner en nettside»²³. Disse kan være nyttig, både for brukerne og eier av en nettside.

På eiersiden kan tjenestene tilpasses ut fra informasjonen som lagres. Brukeren kan oppleve nettsiden mer brukervennlig og tilpasset.²⁴ For eksempel, å være innlogget hver gang man lukker og gjenåpner nettleseren eller at varene i handlekurver på nettbutikker blir lagret til neste besøk o.l. Samtidig kan disse også brukes i markedsføringsformål, dette blir behandlet nærmere under 2.1.2.

Forståelse av cookies og dens funksjoner, krever noen grunnleggende forkunnskaper om måten kommunikasjon foregår på internett.

²³ Datatilsynet, (2019)

²⁴ NKOM, (2019)

Det skal først redegjøres for hva en http er i punkt 2.1.1, funksjoner av cookies samt bruken illustreres under punkt 2.1.2. Deretter skal det redegjøres for ulike typer cookies og farene de kan utsette en internettbruker for.

2.1.1. Hvordan foregår kommunikasjonen på internett?

Hypertext transfer protocol (HTTP) danner grunnlaget for datakommunikasjon i World Wide Web (www).²⁵ Den er den mest anvendte protokollen for å overføre tekst på internett.²⁶ Måten den fungerer på er gjennom to-ende kommunikasjon. Det vil si at, man har nettleseren²⁷ på ene enden og internettserveren²⁸ på den andre.

Når en nettbruker klikker på en link, bruker klienter en URL/link, for å koble seg til nettserveren og sender en forespørsel. Nettserveren, etter å ha mottatt forespørselen, sender et passende svar²⁹ til brukeren. Brukeren blir deretter frakoblet fra nettserveren.

2.1.2. Hva gjør cookies?

I sin originale form er http protokollen uavhengig. Det betyr at ved hvert besøk, er man nødt til å logge inn og velge de samme preferansene. Handlekurven vil heller ikke automatisk huske varene. Etter at man lukker fanen, vil opplysninger om hvilke varer som var lagret i handlekurven forsvinne. Da må man huske alle varene man ville handle på en nettbutikk til neste besøk.

For å kunne hjelpe nettsserveren i å opprettholde avhengigheten, slik at man slipper å gjøre samme handlingene om igjen, er man nødt til å opprette en slags «minne» for nettsserveren. Da kan den huske hvor den slapp³⁰.

Cookies brukes for å oppnå slike funksjoner på nettsider. Når serveren svarer på en forespørsel, setter den samtidig informasjon på nettbrukeren, slik at den kan bli gjenkjent ved neste besøk³¹.

²⁵ Årnes, (2018) s. 284

²⁶ Difi, (2015)

²⁷ F.eks. Chrome, Internet Explorer osv.

²⁸ Brukerens side

²⁹ Innholdet av den siden som klienten har bedt om gjennom URL

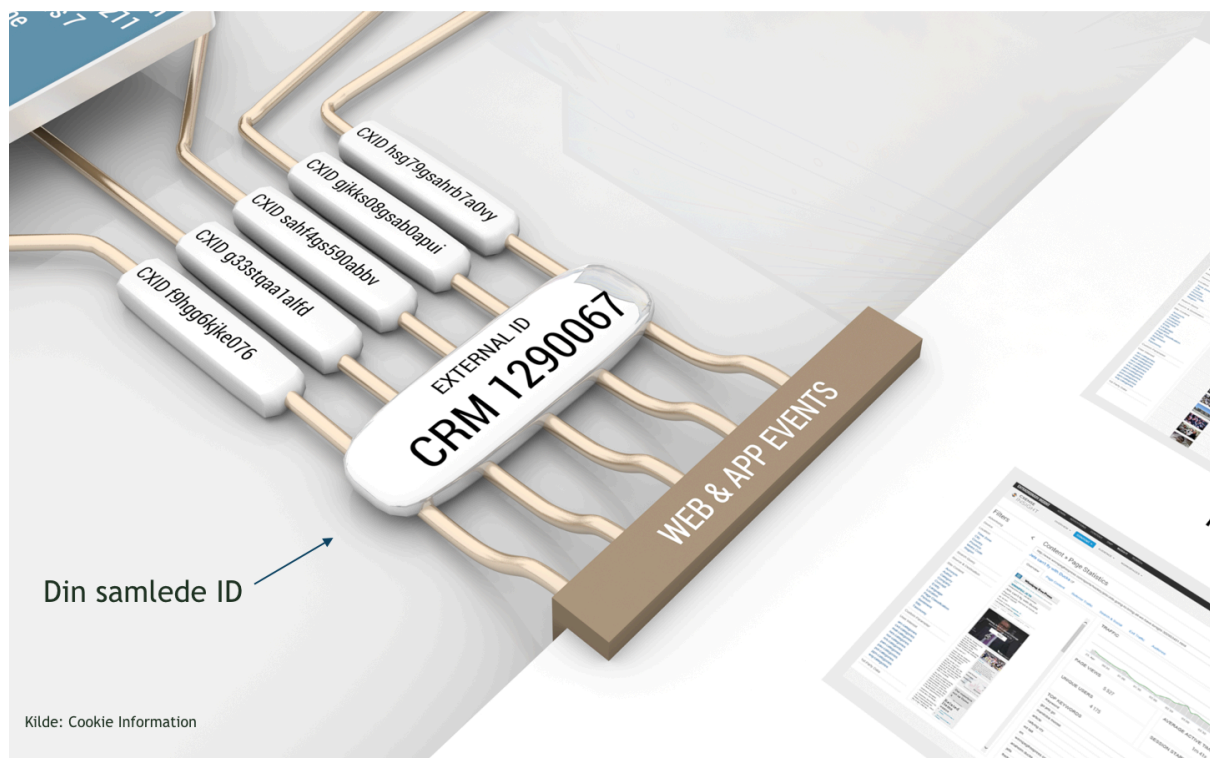
³⁰ Kristol, (2001) s.3-5

³¹ Kristol, (2001) s.5

Cookies er ikke den eneste måten man kan oppnå avhengighet mellom ulike besøk på nettsider, men det er en av de enkleste og mest anvendte måter. I tillegg til å lagre innloggingsdetaljer og nettbrukers preferanser, kan den også spore nettbrukerens online oppførsel og vaner.³²

Det finnes flere måter å spore brukere på, men denne måten gjøres på tvers av ulike enheter f.eks. telefon, pc, lpad, smartklokker osv. Denne måten heter scripting. Hver av enhetene har sin egen cookie-ID, og ulike plattformer f.eks. Cxense³³, som kobler sammen de ulike cookie-IDene på tvers av enhetene og knytter de opp til en person.

Det gjør brukeren identifiserbar, se figuren under for en grafisk fremstilling av operasjonen nevnt ovenfor.



På den ene siden, fører dette til bedre brukeropplevelse f.eks. ved at brukeren slipper å logge inn all informasjonen på tvers av enhetene. På den annen side, kan disse opplysningene manipuleres og misbrukes mot brukeren. Det kan føre til at vedkommende må betale mer for en vare eller tjeneste basert på interesse og kjøpekraft.³⁴

³² Barth, (2011) s.3-6

³³ Cxense ASA er et teknologiselskap grunnlagt i Oslo i februar 2010. Ved hjelp av brukerdata og sanntidsanalyse skaper Cxense innholdsanbefalinger og annonsering basert på interesse og intensjoner, såkalt personalisering av innholdstjenester.

³⁴ Nyvold (2018)

Disse opplysningene om brukeren, som tidligere nevnt, kan enten brukes av netteieren selv eller videreselges til tredjeparter gjennom såkalt «real time bidding».

RTB – Real Time Bidding



Kilde: Cookie Information

Din profildata med dine opplysninger blir presentert i nettverket for markedsføring. Deretter settes det en budgivning, hvor annonsører gir tilbud for å vise deres annonser til deg. Annonsøren som gir høyeste bud vinner, og annonsen til vinneren vil vises til deg på ulike nettsider mens du surfer.³⁵ Annonsenettverket kan gjennom opplysninger fra cookies se om en annonse fører til kjøp, og dermed måle effekten av annonsen.³⁶

Misbruk av informasjon tatt fra cookies, kan også føre til noe som heter session hijacking. Under hvilket en angriper kan enkeltvis utgi seg for å være nettbrukeren for å få tilgang til serveren³⁷. Angriperen plasserer seg mellom din datamaskin og nettserveren din f.eks. Facebook, Amazon, Instagram mens du er aktiv på siden. Vedkommende kan se alt du gjør på din konto, og dette gjøres uten å måtte hacke kontoen. Angriperen kan t.o.m. kaste deg ut og ta kontroll over din konto³⁸. Det kan t.o.m. føre til økonomisk tap hos internettbrukeren dersom det er f.eks. snakk om en online investeringskonto.

Dette viser hvor inngripende dette er i individers private sfære. Dessuten, viser det også behovet for at individet må ha mer påvirkningen over hele prosessen med behandlingen av opplysningene om seg selv og fra seg selv.

³⁵ Doyle, (2016)

³⁶ Tønseth, (2016), 8.8.2 Hva slags teknologi er omfattet av bestemmelsen

³⁷ LaCroix, Loo, Choi, (2017) s.21-23

³⁸ Cucu, (2017)

3. Hvordan er informasjonskapsler regulert?

3.1. Rettskildebildet og metodiske utfordringer

Bruk av cookies reguleres på den ene siden av ekomloven og ekomdirektivet, og på den annen side av personopplysningsloven og personvernforordningen.³⁹ Dette har skapt store misforståelser om hvordan samtykke skal innhentes for informasjonskapsler som lagres på brukerens maskin⁴⁰, noe som har ført til ulik praksis for nettsider generelt.

Mye av grunnen er at rettsområdet er kompleks og fragmentarisk med uklare regler. Nasjonale regler på område er internasjonalt inspirert, spesielt av EU/EØS lovgivningen. Mange av reglene kommer direkte fra EU-lovgivningen, som gir metodiske utfordringer på rettsområdet.

Norge opererer med et dualistisk rettssystem. Internasjonale konvensjoner må derfor gjennomføres i norsk rett for å være gjeldende.⁴¹ Som tidligere nevnt, kommer mye av lovgivningen på område fra EU/EØS. Disse må derfor gjennomføres i norsk rett enten i form av inkorporasjon eller transformasjon.⁴²

Norge er ikke medlem av EU, og reglene som blir vedtatt i EU kan derfor ikke ha direkte virkning for Norge. Norge er imidlertid medlem av EFTA-samarbeidet, og har gjennom EØS-avtalen bundet seg til gjennomføring av EØS-regler som har sitt opphav fra EU-regler. I realiteten, innebærer EØS-avtalen at reglenes homogenitet skal gjelde i hele EU/EØS-område og slik styrke det europeiske indre markedet.

Oppgaven handler selvsagt om samtykkereglene i norsk rett, og det er norske regler som drøftes. Norske regler i området stammer imidlertid fra EU-retten i form av forordning og direktiv. For en forståelse av reglene, må det derfor også henvises til disse. Innholdet av de EØS-rettslige bestemmelsene fastsettes gjennom deres respektive rettskildeprinsipper.

Rettskildeprinsippene i EU/EØS er mer formålsrettet og dynamisk i motsetning til norsk rett, hvor det er ordlydsdominans. Rettspraksis er veldig viktig, men er i større grad

³⁹ Datatilsynet, (2019)

⁴⁰ PC, mobil, Ipad osv.

⁴¹ Smith, (2012) s. 158

⁴² *ibid.*

rettsutviklende enn i norsk rett. Norsk Høyesterett kan av og til også virke rettsutviklende, men neppe i like stor grad som i EU-domstolen.

EU-domstolen har siste ordet ved fastsettelse av innholdet i reglene. Dette er særlig viktig for forståelse av reglene i GDPR og om forholdene mellom de ulike rettsaktene som stammer fra EU. EU-domstolen gjør lite bruk av forarbeider, men det henvises oftere til forarbeider nå enn det ble gjort før. Det tillegges likevel ikke like mye vekt på forarbeidene, slik det gjøres i norsk rett. Vekten av forarbeidene varierer også i norsk rett, noe vi skal drøfte under tolkning av bestemmelsene i ekomloven og personopplysningsloven.

En annen sontring fra norsk rett er at teori/juridisk litteratur tillegges ingen vekt. EU-domstolen innhenter ideer fra litteraturen til tider, men disse blir ikke nevnt i selve resonnementet. Når det gjelder rettspraksis i personvernområde, er det lite å finne om samtykkekravet etter det opphevede direktivet. Det er avsagt kun én avgjørelse⁴³ etter reglene i GDPR hittil. Tidligere rettspraksis viser at EU-domstolen pleier å være dynamisk i tolkning av reglene på dette rettsområdet. Selv om rettsområde var preget av stor grad uforbindende regler, ble de likevel tillagt mye vekt. Det er fremdeles mange uforpliktende uttalelser og retningslinjer i område, spesielt fra arbeidsgruppen-art.29. EU-domstolens praksis viser dermed at disse tillegges mye vekt der reglene er uklare.

Personvernforordningen er gjennomført i norsk rett som et vedlegg i siste kapittelet av personopplysningsloven. Ved tolkning av forordningen, må man anvende EU-metoden og må derfor gå til EU/EØS-rettslige rettskildedefaktorer. Den tolkningen som vil gjelde i EU/EØS-rett, vil dermed være den riktige, og vil gjelde som norsk rett.

Når det gjelder ekomdirektivet, er den blitt gjennomført i norsk rett gjennom ekomloven. Et direktiv er imidlertid ikke en regulering, og inkorporeres ikke ordrett til norsk rett. Direktivet har visse rettslige rammer som lovgiveren i det landet, må respektere. Ekomdirektivet vil derfor ikke ha særlig betydning ved tolkning av bestemmelsene i ekomloven.

Derimot, der det oppstår innholdsmessig tvil under tolkning av bestemmelsene i norsk rett som har til formål å gjennomføre konkrete bestemmelser i direktivet, vil det være grunn til å se hvordan direktivets bestemmelser er å forstå i sin originale form.

Presumpsjonsprinsippet går ut på at norsk lov skal tolkes slik at den på best mulig måte samsvarer med Norges internasjonale forpliktelser.⁴⁴ Dette vil da føre til at man må tolke

⁴³ Planet49, EU Domstolen, C- 17/46

⁴⁴ Rt.2000 s.1811, Finanger I

norske regler i samsvar med det tolkningsalternativet som er i overensstemmelse med tolkningen av bestemmelsen i direktivet.

Dette er ikke til hinder for at det likevel velges et tolkningsalternativ som ikke er i samsvar med forpliktelsene våre. Det må imidlertid foreligge en klar intensjon fra lovgiverens side om dette. Begrunnelsen er at Stortinget har ikke gitt fra seg den lovgivende makten til EU/EØS-myndighetene, og kan dermed gi regler som er i strid med direktivet. En annen sak er at det kan bli ansett som et konvensjonsbrudd, og Norge kan bli møtt med konsekvensene for det.

3.2. Oversikt over sentrale rettskilder

3.2.1. Ekomloven

Loven gjelder virksomhet knyttet til elektronisk kommunikasjon (e-kommunikasjon) og tilhørende utstyr jf, e-kompl, jf. § 1-2. Den gjennomfører ekomdirektivet⁴⁵. Med elektronisk kommunikasjon menes kommunikasjon ved bruk av et "elektronisk kommunikasjonsnett".⁴⁶ Begrepet er definert som "*system for signaltransport som muliggjør overføring av lyd, tekst, bilder eller andre data ved hjelp av elektromagnetiske signaler i fritt rom eller kabel der radioutstyr, svitsjer (...) tilhørende utstyr eller funksjoner inngår herunder nettverkselementer som ikke er aktive*" (min utheving).

Den relevante bestemmelsen er § 2-7b om bruk av informasjonskapsler.

3.2.2. E-privacy-direktivet/ ekomdirektivet

Direktivet er et sektordirektiv med fokus på telekommunikasjon. Det opphevet direktivet EU 97/66/EC, og var ment som en supplering til direktivet om data beskyttelse.⁴⁷

Formålet med direktivet er å beskytte legitime interesser av brukere, både fysiske og juridiske personer, i forhold til «tjenester av elektronisk kommunikasjon». Definisjonen av terminologien er ikke å finne i selve direktivet. Imidlertid, i direktiv 2002/21/EC er definisjonen som følger "a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on Electronic communications networks".

⁴⁵ Prop.69 L (2012-2013)

⁴⁶ ekomloven § 1-5 nr.2

⁴⁷ Fortaler til ekomdirektivet, punkt 4

Det generelle materielle virkeområde av direktivet gjelder bare for offentlig elektronisk kommunikasjons tjenester.⁴⁸ Det er imidlertid utvidet til å gjelde cookies etter endring av 2009 art. 5(3).

Det er stor enighet om at fortolkninger⁴⁹ av direktivet tilsier at det gjelder kun for telekommunikasjonsoperatører. Topp-tjenester så kalte “over- the- top services” er dermed unntatt. Disse kan være mobilapplikasjoner, netjtjenester osv. For å nevne noen eksempler direktivet vil ikke gjelde for WhatsApp, Viber og abonnementstjenesten Netflix. Disse søkes å reguleres i den nye ekomforordningen, som for øyeblikket er under forhandlinger.

Derimot er topp-tjenester innenfor virkeområdet til ekomloven. Slik sett, gir den norske lovgivningen innen telekommunikasjon individer bedre vern enn det direktivet krever.

Det er varierende hvordan ulike land har transportert direktivet. Når det gjelder cookies er det irrelevant hvordan direktivet er transformert i landets rett. Det vil si at, Art. 5 (3) utgjør en generell norm som får anvendelse på alle tjenester, inkludert e-handel.⁵⁰

Direktivet fra 2009 anvendes på alle nettsider som bruker cookies uavhengig av om virksomheten er inn eller utenfor EU/EØS område.⁵¹ For eksempel, en amerikansk nettside som kan anses å være også rettet mot europeiske nettbrukere og som bruker cookies eller lignende teknologi, må forholde seg til direktivet.

3.2.3. Personopplysningsforordningen - GDPR

Forordningen opphever personverndirektivet, og er den generelle lovgivningen om beskyttelse av personlig data av privatpersoner. Den dekker mye mer enn kun online kommunikasjon. Det er kun EU- domstolen som kan tolke forordningen i sisteinstans og alle EU/ EØS-medlemslandene vil være bundet av den tolkningen.

3.2.4. Personopplysningsloven

Loven gjennomfører personopplysningsforordningen, og gjør den om til norsk rett. Reglene er blitt inkorporert i norsk rettssystem uten videre endringer i selve forordningen. Som nevnt i

⁴⁸ European Data Protection Board, Opinion 5/2019 s. 10

⁴⁹ Gutwirth, Leenes and De Hert, (2016) s.214-215

⁵⁰ Artikkel 29-gruppen A29WP, 00737/EN WP148 4. April 2008 s. 12

⁵¹ Bond, (2012) s. 217

forrige avsnitt er det EU-domstolen som har rett og plikt til å tolke bestemmelsene i forordningen. Imidlertid, er det ikke mye rettspraksis på området grunnet lovgivningens alder.

I fravær av klargjørende rettsavgjørelser, må bestemmelsene som er nye i GDPR tolkes i lys av de generelle personvernrettslige prinsipper som er nevnt i GDPR art. 5 og eldre avgjørelser fra EU-domstoler i saker avgjort basert på direktivets bestemmelser. Fortalene i forordninger er detaljerte og gir god veiledning til forståelse av bestemmelsene ellers.

I de siste månedene, er det blitt avsagt en del avgjørelser som er av avgjørende betydning for denne oppgaven. Disse klargjør rettstilstanden, og bidrar til forståelse av hvordan bestemmelsene i GDPR og ekomdirektivet er å forstå.

Cookies er regulert i ekomdirektivet art. 5 (3) og definisjonen for samtykke er gitt i art. 2(f). Imidlertid, er det regler i GDPR som er generelle. Disse vil derfor også gjelde for cookies. Hver av disse rettsaktene har visse regler som berører samtykkevilkårene ved bruk av cookies. Det er derfor viktig å fastsette forholdet mellom lovgivningene for å kunne fastsette hvilke regler som gjelder under ulike tilfeller og omstendigheter. Dette er imidlertid et spørsmål som er omtvistet.

For å kunne finne ut av hva slags krav stilles til et gyldig samtykke for å innhente cookies, er det viktig å vurdere hvorvidt reglen ekomloven § 2-7b er i samsvar med våre folkerettslige forpliktelser, altså personvernforordningen⁵² og ekomdirektivet⁵³. Dersom avvik finnes, blir spørsmålet om dette har vært ønskelig fra lovgivers side eller om det kan løses gjennom norske rettsprinsipper.

3.2.5. Forholdet mellom ekomloven og personopplysningsloven

Personopplysningsloven og forordningen gjelder i hovedsak helt eller delvis automatisert behandling av «personopplysninger»⁵⁴ mens ekomloven gjelder virksomhet knyttet til elektronisk kommunikasjon (...) ⁵⁵, hvorav internett.⁵⁶

⁵² FOR 2016/679 EU

⁵³ Dir 2002/58/EC og Dir 2009/136

⁵⁴ Personopplysningsloven § 2

⁵⁵ Ekomloven § 1-2

⁵⁶ Ot.Prp.nr.58 (2002-2003) til § 1-2 saklig virkeområde

Ekomloven § 2-7b presiserer at den gjelder behandling av «opplysninger». Den er dermed ikke kun begrenset til personopplysninger, men omfatter alle slags opplysninger.

Det innebærer at personopplysningsforordningen er spesiell lovgivning i forhold til ekomloven. Ifølge lex specialis-prinsippet må ekomloven da gå foran i tilfelle hvor samme forholdet er regulert.

På den annen side, er ekomloven en spesifisert lov ettersom den gjelder behandling av opplysninger kun innenfor elektronisk kommunikasjon. Det vil f.eks. gjelde kun opplysninger som blir behandlet på internett, og vil ikke gjelde hvordan disse vil ellers blir misbrukt i andre sammensetninger utenfor internett.

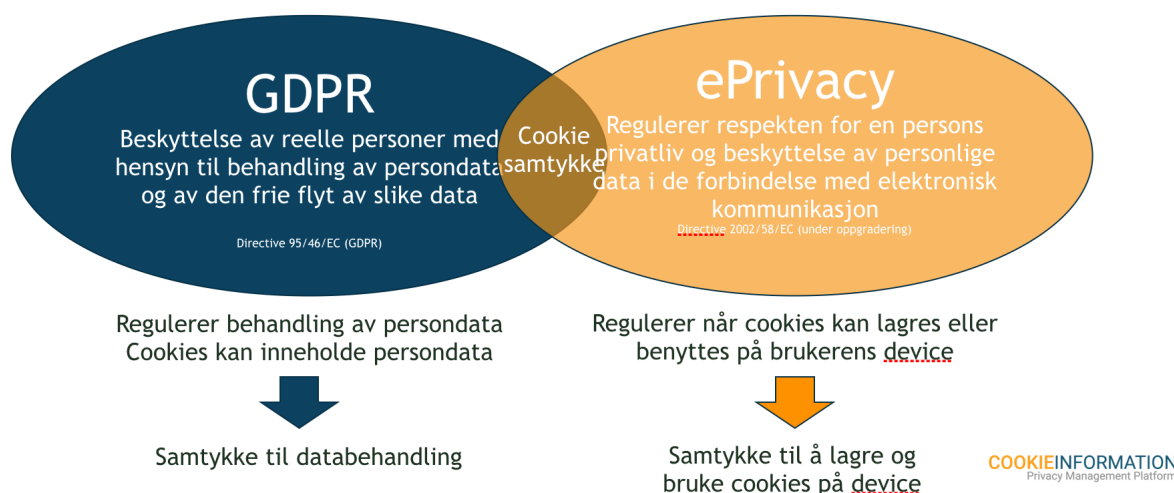
Det har derfor vært uklarheter om hvilke regler som skal gjelde for samtykke i forhold til cookies etter innføring av GDPR.

Ekomloven har ingen bestemmelser som klargjør forholdet mellom det saklige virkeområdet til ekomloven i forhold til personopplysningsloven eller forordningen når det gjelder informasjonskapsler. Ekomloven er fra tiden før GDPR trådte i kraft og inkorporert i norsk lov. Det kan være årsaken til at loven ikke inneholder en bestemmelse som klargjør forholdet mellom lovenes virkeområder.

På den annen side, både forordningen og ekomdirektivet har bestemmelser om forholdet mellom ekomdirektivet og forordningen. Ettersom ekomloven er en gjennomføring av ekomdirektivet kan det være retningsgivende å tolke forholdet til ekomdirektivet og forordningen for å se forholdet mellom ekomloven, personopplysningsloven og personvernforordning.

I denne delen skal det gjøres et forsøk på å klargjøre rettsstillingen ved å fastsette materielle virkeområder for rettsaktene og sameksistensen av begge.

3.2.5.1. Nyansere sondringen i virkeområdene til ekomdirektivet og personvernforordningen vedrørende cookies



GDPR gjelder for alle slags dataansvarlige/ behandlere som “behandler” “personopplysninger ikke kun i elektroniske kommunikasjonsfeltet”.

Med behandling menes “enhver operasjon” f.eks. «*innsamling, konsultasjon, bruk, registrering organisering, lagring, strukturering, tilpasning, endring, gjenfinning, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring*»⁵⁷ [min utheving] av opplysninger. Derimot gjelder ekomdirektivet kun lagring av og anskaffelse av adgang til lagrede opplysninger. GDPR-forordningen dekker derfor et større område enn ekomdirektivet.

Med personopplysninger siktes det til enhver opplysning om en “identifisert eller identifiserbar fysisk person. “Identifiserbar er definert som følger: en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator; f.eks. navn, ID-nummer, osv.

Det skal i det følgende først klargjøres innholdet av art. 1(2) av ekomdirektivet. Deretter tolkes art. 95 av forordningen.

⁵⁷ GDPR art. 4 nr. 2

Art. 1(2) av ekomdirektivet uttrykkelig sier at bestemmelsene i dette direktivet “particularise and complement Directive 95/46/EC (...)”⁵⁸. Det må foretas en tolkning for å fastsette innholdet av disse begrepene.

3.2.5.2. *Particularise*

Som tidligere nevnt, gjelder GDPR generelt for alle type behandlinger av personopplysninger. Ekomdirektivet er en særregulering og skal “particularise” forordningen innen elektronisk telekommunikasjons område. Direkte oversettelse av begrepet på norsk, er å spesialisere eller spesifisere.

Det følger av lex specialis-prinsippet at den spesielle reguleringen vil gå foran det mer generelle i det enkelte regulerte område. Det tilsier at i situasjoner hvor ekomdirektivet spesifiserer (particularise) konkrete bestemmelser som skal gjelde, går disse foran reglene i GDPR, som er mer generelle. Derimot går reglene i GDPR foran dersom enhver behandling av personopplysninger, ikke er nærmere regulert i ekomdirektivet.

I fortalen 173 av GDPR er det også vist til denne måten å løse sameksistensen av begge rettsaktene.

Dessuten, har arbeidsgruppen-29⁵⁹ også avgitt en uttalelse, hvor de støtter denne fremgangsmåten og konklusjonen. Uttalelsen er ikke bindende, men i fravær av andre rettskilder vil uttalelsen tillegges stor vekt ved tolkningen.⁶⁰

Et eksempel kan være art. 6 av GDPR som gir alternative ansvarsgrunnlag for behandling av personopplysninger. Når det gjelder cookies i ekomdirektivet fremgår det av art. 5 (3) at dette kan kun skje dersom samtykke fra brukeren er blitt innhentet, når det gjelder lagring av opplysninger og tilgang til lagrede opplysninger gjennom cookies og lignende teknologier. Med et snevert unntak til situasjoner hvor lagring eller tilgang er “stricly necessary”.

Det ekomdirektivet gjør her er å innskrenke muligheten til å utføre lagring og anskaffelse av tilgang til lagrede opplysninger gjennom alternative ansvarsgrunnlag. På den annen side, regulerer den ikke vilkårene for et slikt samtykke og referer tilbake til reglene i den generelle lovgivningen, GDPR.

⁵⁸ GDPR Art. 94(2) tilsier at alle referanser gjort til det opphevede direktivet skal bli konstruert som referanser til forordningen

⁵⁹ European Data protection Board, Opinion 5/2019, s.13-15.

⁶⁰ *ibid*, s.13.

Her reises det spørsmål om hvorvidt det gjelder kun personopplysning eller alle slags opplysninger

Ved første øyekast, kan det tenkes at i tilfeller hvor informasjonskapsler lagrer/får adgang til opplysninger som ikke utgjør personopplysninger, vil ikke reglene i GDPRs samtykkekrav gjelde. Ettersom GDPR kun verner personopplysninger.

Imidlertid, fremgår det av art. 5 (3) av ekomdirektivet at bestemmelsen referer til “information” altså enhver opplysning. Den er ikke kun blitt avgrenset til personopplysninger. Dette sier noe om hva selve direktivet har som materiell område. Når bestemmelsen forstås slik at vilkårene for gyldig samtykke skal være de samme som i GDPR, så trekker det i retning av at selv når cookies ikke inneholder personopplysninger må samtykke innhentes i samsvar med reglene i GDPR.

Direktivets fortaler punkt 24 tilsier at hvilken som helst opplysning lagret i brukerens terminallutstyr utgjør en del av vedkommende sin private sfære, som krever vern under den europeiske konvensjonen for vern av menneskerettigheter og de fundamentale frihetene. Det peker også i retning av at vernet gjelder for enhver opplysning som blir lagret eller fås tilgang til, uavhengig av om det er personopplysning eller ei.

Dessuten har Advokat generalens rådgivende uttalelse i sak planet49⁶¹ i punkt 107 også i en av sine uttalelser uttalt at hensikten med art. 5 (3) er å verne brukeren fra innblanding med vedkommende privat sfære uavhengig av hva slags opplysninger det er snakk om. Noe som også er i samsvar med direktivets fortaler. EU-domstolen avsa en avgjørelse ,planet49, den 1.oktober 2019 og la til grunn det samme perspektivet og henviste til advokat generalens uttalelse.

Det samme fremgår også av uttalelser fra arbeidsgruppen-29 som ikke er bindende, men tillegges fortsatt noe vekt ved tolkning av samspillet mellom de to rettsaktene.

EU-domstolens tolkning i dette tilfelle er bindende, og vil gjelde som en fast regel i dette område.

⁶¹ Planet49 gjennom sin nettside organiserte en lotteri. For å kunne delta, måtte brukeren avkrysse eller fjerne avkrysning av noen bokser ved påmeldingen. Disse boksene var anmodninger på samtykke til bruk av cookies. Saken reiste spørsmål om hvorvidt brukeren har et reelt valg, og om samtykke kreve en aktiv handling for å være gyldig. EU-domstolen kom til at forholdet mellom rettsaktene er slik at samtykke for bruk av cookies må være sammenfallende med samtykkeregulene etter GDPR. Domstolen kom til at det kan ikke foreligge et reelt valg, der tjenesten er gjort betinget av samtykke. Den konkluderte videre med at det kreves en aktiv handling fra brukere.

Konklusjonen på underproblemstillingen er at reglene i GDPR vil gjelde i tilfeller der det er henvist til GDPR eller når forholdet er ikke regulert av ekomdirektivet.

Denne konklusjonen gir svaret på vår hovedproblemstilling om hvorvidt ekomdirektivets krav til samtykke er det samme som samtykke krav under GDPR. Begge lovgivningene stiller krav til samtykke, men det nærmere innholdet er ikke regulert i ekomdirektivet. Svaret er dermed at vilkårene for samtykke i GDPR gjelder også for krav om samtykke etter ekomdirektivet.

3.2.5.3. *Complement*

“to complement” betyr å utfylle eller supplere. Ekomdirektivet sikter også til å beskytte den fundamentale retten til vern av personvern. Den bygger dermed på samme tankegangen som GDPR, og skal supplere den innen elektronisk kommunikasjons sektor.

For å nevne et eksempel det opphevede personverndirektivet og GDPR-forordningen, begge sikter å beskytte fysiske personer. Ekomdirektivet derimot verner også juridiske personer. (fortale punkt 12) Slik supplerer den GDPR.

3.2.5.4. *Artikkel 95 av GDPR*

Art. 95 av GDPR regulerer forholdet til ekomdirektivet.

Forordningen skal ikke «*innføre ytterligere forpliktelser for fysisk og juridiske personer når det gjelder behandling i forbindelse med levering av offentlige tilgjengelige elektroniske kommunikasjonstjenester ... med hensyn til aspekter der de er underlagt*» [min utheving] særlige forpliktelser med samme formål” som det er fastsatt” i ekomdirektivet.

Formålet med denne bestemmelsen er å hindre overlapp av byrder overfor pliktsubjekter. I forordningens fortale 173 heter det det at ekomdirektivet må endres i henhold til det som til enhver tid er i overensstemmelse med reglene i GDPR. I forbindelse med innhenting av samtykke spiller ikke denne bestemmelsen noen sentral rolle. Den skal dermed ikke behandles mer i denne oppgaven.

3.2.5.5. *Vil de samme forholdene gjelde i forhold til ekomloven?*

Etter behandling av forholdet mellom ekomdirektivet og personvernforordningen, er det gode grunner for å anta at det samme gjelder i reglenes implementering i norsk rett i form av

ekomloven. Personopplysningslovens virkeområde er også likestilt med personvernforordningens, med unntak av noen få tillegg som ikke er til hinder for den forståelsen som vi kom frem til overfor.

3.3. Hva krever den EU/EØS rettslige forpliktelsen av norsk rett når det gjelder krav til samtykke til cookies, og hvordan er disse implementert i norsk rett?

3.3.1. Metodisk tilbakeblikk

EU-retten skal være homogen i hele område, og må tolkes uavhengig av nasjonal rettens innhold.

Fast rettspraksis viser at ikke bare ordlyden, men også formålet, konteksten og øvrige bestemmelser av EØS-retten, må tas med for å tolke en bestemmelse. Naturen av bestemmelsen av EU-retten kan også være et relevant moment ved tolkningen.⁶²

3.3.2. Innholdet av reglene i område

Hovedregelen⁶³ er at brukerens terminalutstyr og enhver opplysning lagret i de er beskyttet av menneskerettslige regler⁶⁴ og de europeiske fundamentale frihetene⁶⁵.

Det kan være en serie av skadelige software, som spyware og gjemte identifiserende mekanismer, som kan spore brukerne uten deres kunnskap. Disse kan være en alvorlig trussel for deres rett på beskyttelse av personvern. Det er med andre ord forbudt å lagre informasjonskapsler eller skaffe seg tilgang til slike opplysninger i brukernes terminalutstyr.⁶⁶

Unntaket er regulert i art. 5(3)⁶⁷ som tillater legitimert bruk av cookies. Det gjør cookies til et verktøy som oppfyller viktige formål f.eks. verifikasjon av en transaksjon eller analysere effektiviteten av en nettsidens struktur og utforming, se punkt 2 for nærmere redegjørelse av hva cookies er og deres funksjon.

⁶² Wightman and Others, C-621/18, paragraf 47 og Planet49, C-673/17

⁶³ fortale 24 av ekomdirektivet, EU 2002/58/EC

⁶⁴ Den europeiske menneskeretts konvensjonen art. 8 om retten til respekt for privatliv og familieliv

⁶⁵ Den europeiske unions charter om grunnleggende rettigheter art. 8 om retten til beskyttelse av personligopplysninger

⁶⁶ fortale 24 av ekomdirektivet EU 2002/58/EC

⁶⁷ Ekomdirektivet artikkel 5 nr. 3

I direktivet EU 2002/58/EC var det oppstilt to krav for å lagre eller få tilgang til opplysninger på brukernes terminalutstyr. Det første var at det måtte gis tilstrekkelig klar informasjon om formålet med lagring av opplysninger til brukeren i henhold til det nå opphevede personverndirektivet⁶⁸. Det andre var at brukeren måtte gis muligheten til å nekte å få lagret opplysninger i sitt utstyr.

Direktivet ble endret i 2009, og innførte regler for blant annet cookies i art. 5 (3) som lyder som følger:

« Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. «

En nevneverdig endring er endring av varsel og samtykkekravet fra en informert opt-out⁶⁹ system til en omtrent helt informert opt-in.⁷⁰

Hovedregelen var at det var lov å lagre opplysninger eller få tilgang. Retten til å nekte lagring, kom som et unntak fra denne. Det spesielle er at når man kommer seg inn på en nettside, så er opplysninger allerede overført via cookies. Behandlingen begynte derfor før brukeren kunne nekte lagring. Man kunne eventuelt nekte fremtidige lagring av opplysningene.

De grunnleggende rettighetene om beskyttelse av opplysninger og retten til privatliv tilsier at opplysningene om internettbrukere er vernet og kan ikke brukes av andre de opplysningene tilhører.

⁶⁸ GDPR art. 94 tilsier at enhver henvisning gjort til personverndirektivet regnes som henvisning til det nye forordningen GDPR.

⁶⁹ Formuleringen før var at lagring av opplysninger eller tilgang til slike opplysninger kun er tillatt når brukeren "is provided with..information...and is offered the right to refuse" som gjorde at brukers data ble lagret helt til vedkommende fremmet ønske å trekke samtykket sitt tilbake, en så kalt opt-out løsning.

⁷⁰ Bond, (2012), s.215

En hovedregel som gir lov til lagring av opplysninger er dermed ikke i samsvar med de grunnleggende rettighetene om beskyttelse av opplysninger, og retten til privatliv. Selv om den gir brukeren rett til å nekte underveis. Rettsteknisk blir utgangspunktet gjort om til et unntak. Den faktiske betydning er at man svekker beskyttelsen som brukere egentlig skal ha i henhold til grunnleggende rettigheter og direktivets formål som jo er å styrke vernet.

Det tilsier at hovedregelen for lagring og anskaffelse av tilgang til lagrede opplysninger, skal i utgangspunktet være forbudt og legitimert bruk av disse kan være et unntak.

Den endrede formuleringen av bestemmelsen tilsier at lagring og anskaffelse av tilgang til opplysninger, er kun tillatt når brukeren «*has given his/her consent, having been provided with information.*» Slik at opplysninger blir først lagret etter at brukeren gir sitt samtykke. Med et snevert unntak for tilfeller hvor lagring av cookies en «*strictly necessary*», noe vi kommer tilbake til i punkt 3.2.4.

Direktivet innfører dermed en opt-in løsning, hvor opplysningene skal bli lagret først etter at brukeren er blitt informert, og har gitt sitt samtykke. Slik styrker direktivet vernet om beskyttelse av opplysninger.

Regulering av bruk av cookies var først gjennomført i 2004 i ekomforskriften § 7-3. Ved lovendringen i 2013 ble bestemmelsen endret og flyttet til i ekomloven § 2-7b. Ifølge forarbeidene til ekomloven § 2-7b gjennomfører artikkel 5 nr.3 av ekomdirektivet. Den nye bestemmelsen ble derfor endret og utvidet fra tidligere bestemmelsen i ekomforskriften. Dette gjort for at bestemmelsen skulle være i samsvar med endringene som ble gjort i 2009 i ekomdirektivet art.5 nr.3.

Ekomloven § 2-7b lyder som følgende:

«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.»

At brukeren «er» informert og «har» samtykket, peker klart i retning av at ordlyden legger en opt-in løsning til grunn. Slik at lagring av opplysningene kan begynne etter at brukeren har fått informasjon, og gitt sitt samtykke til behandlingen. Dette er i samsvar med ekomdirektivet. Ekomloven styrker dermed verne for internetbrukere i like stor grad.

Oppsummeringsvis, kan det sies at utgangspunktet er at lagring og anskaffelse av adgangen til slike opplysninger i brukerens datamaskin, mobil, laptop eller andre teknologiske utstyr, er forbudt, jf. Ekomloven § 2-7b. Unntaket fra dette utgangspunktet foreligger der brukeren har gitt informert samtykke til dette. I annet punktum, gjør loven unntak fra dette unntaket. Det gjelder ingen samtykkekrav dersom omstendighetene nevnt i bestemmelsens annet punktum nr.1 eller nr. 2, er oppfylt. Unntaket fra samtykkeregelen kommer jeg tilbake til i punkt 3.5.

Det skal først drøftes hva som ligger i kravet «informert samtykke».

3.3.3. Informert samtykke

Det er mange deler til dette spørsmålet: hva slags informasjon skal det gis til brukeren, på hvilket tidspunkt skal informasjonen gis, hvordan samtykke skal begjæres, og hvordan skal samtykke gis.

En felles problemstilling for alle disse underproblemstillingene nevnt overfor er, **hvorvidt samtykkereglene i personvernforordningen gjelder for samtykke til informasjonskapsler.**

Ordlyden av bestemmelsen i ekoml. § 2-7b er taus, og gir ingen avklaring om forholdet til personopplysningsloven, herunder personvernforordningen. I forarbeidene⁷¹ til bestemmelsen heter det, at kravet til samtykke er «av praktiske årsaker ikke sammenfallende med krav til samtykke etter personopplysningsloven».⁷² Det kan trekke i retning av at samtykke etter ekomloven ikke er sammenfallende med krav til samtykke etter personopplysningsloven.

På den annen side, er det uttrykkelig nevnt i ekomdirektivets art.5 nr. 3 at samtykkereglene skal avgis i henhold til bestemmelsene i det opphevede direktivet 95/56/EC – som nå er omplassert av personvernforordningen.

Advokat generalen i sak planet49, avsa en uforbindende uttalelse om at informasjonskapslenes samtykke skal følge reglene til samtykke i GDPR. Dette synspunktet ble senere i

⁷¹ Prop.69 L (2012.2013) Til ny § 2-7b

⁷² ibid, 5.avsnitt siste punktum

samme sak fulgt av domstolen. EU-domstolen i en prejudisiell avgjørelse, som ble avsagt nylig, har klargjort at samtykkereglene for informasjonskapsler etter ekomdirektivet er sammenfallende med samtykkereglene i personvernforordningen. Det klargjør forholdet mellom ekomdirektivet og personvernforordningen. Dommen også viser at det samme gjaldt under det opphevede direktivet, slik at medlemslandenes lovgivning måtte henvise til personverndirektivet for vilkårene om samtykke.

Ettersom ekomloven gjennomfører ekomdirektivet blir problemstillingen om det samme bør gjelde om forholdet mellom ekomloven, personopplysningsloven og personvernforordningen.

Som tidligere nevnt, fremgår det av forarbeidene til ekomloven at samtykkereglene sammenfaller ikke med samtykkekravene etter personopplysningsloven. Utgangspunktet er at forarbeidene har stor vekt når ordlyden er taus, men det er også andre momenter som kan være avgjørende f.eks. hvorvidt forarbeidene er godt drøftet, og hvorvidt det har skjedd utviklinger i rettsområde siden.⁷³

Forarbeidene er klare og uttrykkelig nevner at reglene om samtykke skal ikke sammenstilles mellom disse to reguleringene, noe som trekker i retning av at den skal tillegges avgjørende vekt.

Imidlertid, er begrunnelsen avgitt for å være «praktiske årsaker». Det foreligger ingen nærmere redegjørelse for hva disse «praktiske» årsakene innebærer. Slik at forarbeidene på dette punktet har noe dårlig kvalitet, og viser ikke til eventuelle avveielser som er blitt gjort for å avvike den riktige gjennomføring av regelen. Det i seg selv kan trekke i retning av å tillegge forarbeidene lite vekt.

Dessuten har «Praktiske» årsaker muligens sin bakgrunn i at da dette ble skrevet fantes det ikke gode tekniske løsninger for å samle inn samtykker. Teknologien for dette er nå tilrettelagt, og det finnes seriøse aktører som har løsninger som muliggjør innsamling av samtykker på en oversiktlig og effektiv måte bl.a. Cookie Information AS. Basert på dette, kan det argumenteres for at «praktiske årsaker» muligens ikke er relevant lenger.

En annen merkbar poeng, er at forarbeidene til ekomloven er fra før GDPR og Planet49-avgjørelsen. Det er derfor blitt foretatt viktige rettsavklaringer i område som ikke er blitt revidert på lovgivernivå. Tidsmessige aspektet trekker derfor i retning av at forarbeidene ikke skal tillegges mye vekt.

⁷³ Dersom regelen utvikler seg annerledes enn det ble forutsett av den norske lovgiver, er det grunn til å vektlegge forarbeidene mindre, jf. Rt. 2015s.138, og Arnesen (2015)

Dessuten var det behov for en avklaring på EU-nivå. Personverndirektivet var implementert ulikt i EU/EØS-land på grunn av den skjønsmessige marginen som statene gis til å gjennomføre lovgivningen i sitt rettssystem. Det tyder på at flere land var i tvil om innholdet av hvordan reglene skulle forstås. Reglene var praktisert ulikt, og det var derfor ikke enkelt å gi et konkret og entydig svar på hvilke krav skulle gjelde for samtykke. Man kan ut ifra dette argumentere at norske myndigheter heller klarte å forstå den riktige tolkningen, noe som tilsier at kvaliteten på forarbeidene ikke er helt optimal. Dette momentet trekker også i retning av at forarbeidene skal ha lite vekt.

Personvernforordningens formål var nettopp å øke harmonisering av reglene på feltet, slik at individene skulle ha likt vern til beskyttelse av sine personopplysninger uansett hvilket EU/EØS-land de tilhørte. Forordningen gir ikke statene friheten til å lage sine egne lover innenfor avgitt rammer. Den gjelder heller som ferdigutformet lov i deres rettssystemer. Det fører til at personvernforordningen er likt i alle land. Derfor er nå lettere å gi en bindende klargjøring på hva som den riktige tolkningen mellom forholdet til ekomdirektivet og GDPR-forordningen. Noe EU-domstolen gjorde i Planet49-avgjørelsen.

For EFTA-statene vil ikke avgjørelsene fra EU-domstolen ha direkte virkning. Imidlertid, slik rettspraksisen til EFTA-domstolen viser, pleier de omtrent alltid å følge avgjørelsene fra EU-domstolen.⁷⁴ Dersom det vil bli presentert en sak foran EFTA-domstolen med samme spørsmål, vil den med stor sannsynlighet få samme tolkningsresultatet. Dette trekker også i retning av at samtykke for cookies etter ekomloven må anses for å være sammenfallende med samtykkereglene i GDPR-forordningen.

Det foreligger derfor sterke grunner for å tolke ekomloven § 2-7b slik at samtykke for informasjonskapsler etter ekomloven må gis i samsvar med reglene for samtykke i personvernforordningen. Forarbeidene på dette punktet tillegges derfor lite vekt.

Dette sett sammen med irrelevans av «praktiske årsaker» for hvorfor reglene for samtykke ikke kan være sammenfallende, tilsier at en revurdering av bestemmelsen etter personvernforordningen og avsagte EU-dommen ville ha sammenstilt vilkårene for samtykke i begge lovgivninger.

På den annen side, kan det hevdes at ordlyden i ekomloven § 2-7b er ikke identisk med art.5 nr.3 i ekomdirektivet, hvor ordlyden direkte gjør henvisninger til reglene i det opphevede direktivet- nå GDPR. Den norske regelen viser ikke direkte til forordningen, slik det er foreslått i ekomdirektivet.

⁷⁴ ODA-avtalen art. 3; EØS-avtalen art. 6

Det kan tilsi at en slik utelattelse kan muligens tyde på at lovgiverviljen var ikke å gi en regel samme innhold som den har i EØS-rett. Noe lovgiver har adgang til som vi tidligere nevnte. Det vil trekke mot fortolkning av ekomloven § 2-7b for å sammenstille vilkårene om samtykke med de som er regulert i personopplysningsloven.

Det fremgår imidlertid av ekomforskriften § 7-4 at med «samtykke etter reglene § 7-1 og § 7-2 menes samtykke slik de er anvendt i personopplysningsloven». §§ 7-1 og 7-2 gjelder ikke direkte bruk av informasjonskapsler. I fravær av annen definisjon for samtykke i loven og forskriftene, kan det tale for at definisjonen skal også gjelde for bruk av informasjonskapsler. Dette er ikke et avgjørende moment, men sett i lys av det som ble resonert ovenfor, tyder det på at den samme regelen kan gjelde for informasjonskapsler.

Det kan også nevnes at datatilsynet har på sine hjemmesider uttrykkelig sagt at samtykke for informasjonskapsler, må innhentes i samsvar med reglene for samtykke i GDPR- altså personopplysningsloven. Dette ble sagt basert på uttalelser fra arbeidsgruppen-29, som jo ikke er bindende, men følges som oftest vektlegges og følges av EU-domstolen.

NKOM har også publisert på sine hjemmesider at det er behov for presisering i regelverket om vilkårene for samtykke når det gjelder cookies. De nevner også at det er en ny ekomforordning på vei, og at denne avgjørelsen vil ha betydning for hvordan informasjonskapsler vil bli regulert i den. Dette tilsier kanskje ikke direkte at det er den tolkningen som følger av dommen som skal legges til grunn, men den viser at også de ser behovet for klargjøring av hvordan reglene er å forstå i dette området.

Forarbeidene utdyper ikke hva som utgjør praktiske årsaker, og de eventuelle praktiske årsakene er ikke relevante lenger, som drøftet ovenfor. Det foreligger dermed ikke tilstrekkelige grunner for å anta at en presisering av regelverket fra dialogen mellom NKOM og Kommunal-moderniseringsdepartementet, vil fravike tolkningen av EU-domstolens avgjørelse. Reelle hensyn på et dynamisk rettsområde tillegges mye vekt, særlig når rettskildefaktorene ellers er uklare. Disse trekker i retning av at samtykkereglene i GDPR må gjelde ved bruk av cookies.

Det fremgår av det resonerte ovenfor at med stor sannsynlighet er ekomloven § 2-7b å forstå slik: samtykke til bruk av informasjonskapsler er sammenfallende med reglene for samtykke etter personopplysningsloven, herunder personvernforordningen. Regelen gir større vern til individers beskyttelse av personvern og harmoniserer regelverket med slik den er å forstå i EU/EØS-retten.

Konklusjonen på dette spørsmålet i denne avhandlingen blir dermed at reglene for et gyldig samtykke i forhold til bruk av cookies, er sammenstilt med reglene i personopplysningsloven – personvernforordningen.

I det følgende skal det redegjøres for vilkårene for samtykke i personopplysningsloven, og deretter blir det drøftet underproblemstillingene knyttet til ulike deler av samtykke i forhold til informasjonskapsler.

3.3.4. Samtykke etter GDPR

For å kunne behandle personlig opplysninger om brukeren, må det foreligge et grunnlag som følger av personvernforordningen art.6 nr.1⁷⁵. Samtykke er et av de grunnlagene som kan anvendes for å kunne behandle personopplysninger. Det er den dataansvarlige som må beslutte hvilket grunnlag vedkommende skal anvende for å kunne behandle opplysningene.

Samtykke er definert i GDPR art. 4 nr. 11 som «enhver frivillig, spesifikk, informert og utvetydig viljesytring» der den registrerte ved en «erklæring eller en tydelig bekreftelse» gir samtykke til behandling av personlige opplysninger om vedkommende. For at samtykke skal anses gyldig, må disse vilkårene være oppfylt.

Definisjonen har også eksistert under det opphevede direktivet. GDPR har bare klargjort betingelsene for samtykke nærmere.

Betingelser for et gyldig samtykke er nedfelt i art. 7 av GDPR. For det første, stilles det krav til den dataansvarlige om å kunne påvise at brukeren har samtykket. For det andre, er det stilt krav til formen under visse tilfeller samt presisering av når en erklæring ikke kan være bindende. For det tredje, skal brukeren ha rett til tilbaketrekking av samtykket til enhver tid. I artikkelens fjerde punktum beskrives det betingelsene for hva som anses «frivillig».

Det er ikke nærmere spesifisert i selve ordlyden hva som ligger i de ulike elementene, og hva skal til for at de skal anses for å være oppfylt.

En veiledning om hvordan man skal forstå de ulike elementene fremgår av forordningens fortaler. Retningslinjer av arbeidsgruppen (European Data Protection Board) for artikkel 64

⁷⁵ GDPR artikkel 4 nr. 11.

nr. 17 er også oppklarende for tolkning og forståelse av elementene i samtykket kravet. Samt den nylige avsatte dommen fra EU-domstolen, Planet49. Dommen Fashion-ID.

3.3.4.1. *Vilkårene*

Med «frivillig» siktes det til at individet etter reelt valg og vilje, har et ønske om å gi samtykke i tillegg til å være i stand til å nekte eller trekke det tilbake uten skade.⁷⁶

Med «informert» siktes det til at datasubjektet, i det minste, er informert om identiteten til dataansvarlige og formålet med databehandlingen.⁷⁷

Uttrykket «spesifikk» refererer til formålet med behandlingen av personopplysninger. Slik at samtykke må forholde seg til alle behandlingsaktivitetene. Der behandlingen har flere formål, må det foreligge uttrykkelig avgitt samtykke for hvert av formålene.⁷⁸

«Utvetydig» er ikke uttrykkelig definert i selve GDPR, men det fremgår av uttalelsen⁷⁹ om samtykke at det må foreligge «ingen tvil» at datasubjektet hadde intensjonen om å gi samtykke. Det er den dataansvarlige som har bevisbyrden. Slik at vedkommende må ha klare prosedyrer på plass for å sikre at samtykke er klart avgitt. Det er ikke tilstrekkelig å utlede at det foreligge samtykke.⁸⁰

For å kunne gjøre dette, må dataansvarliges forespørsel om samtykke være laget på en «intelligible and easily accessible form, using clear and plain language»⁸¹. Dette drøftes ytterligere under punkt 3.3.6.

I det følgende skal vi se hvordan hver av disse vilkårene innebærer innholdsmessige krav til et gyldig samtykke i forhold til informasjonskapsler. Fremstillingen under tar opp utvalgte problemstillinger som er aktuelle og praktiske. Som tidligere nevnt, er ikke hensikten å gi en fullstendig innholdsmessig analyse av alle vilkårene til et gyldig samtykke.

⁷⁶ Fortalene punkt 42, GDPR art. 7(2), (3) og (4) Se punkt 3.3.5.1 for nærmere behandling av vilkåret frivillig

⁷⁷ Fortalene punkt 42, andre relevante opplysninger er oppgitt i en liste i fortale punkt 39: i tillegg må informasjonen som gis, sikre en «fair and transparent» behandling i forhold til individer det gjelder og deres rettigheter om å få bekreftelse og kommunikasjon av personopplysninger som blir behandlet og er relatert til dem. Mer om dette under punkt 3.3.7.

⁷⁸ Se fortalene punkt 33 og 39

⁷⁹ Opinion 15/2011, s. 21.

⁸⁰ GDPR art. 7 nr.1, fortalene punkt 42

⁸¹ Fortalene punkt 42

3.3.5. Er samtykke gyldig under tilfeller hvor samtykke til cookies er en forutsetning for bruk av tjenesten på nettsiden?

Et spørsmål er om samtykke for lagring av opplysninger eller anskaffelse av tilgang til lagrede opplysninger, **er gyldig i tilfeller hvor samtykke til informasjonskapsler er en forutsetning for at brukeren skal kunne fortsette å bruke nettsiden.**

Problemstillingen reiser spørsmål om vilkåret til frivillighet. De øvrige vilkårene reiser ikke særlige vanskeligheter, og kan lett anses for å være oppfylt. Forutsatt at samtykket er spesifikk nok, og det er gitt tilstrekkelig informasjon.

3.3.5.1. Frivillig

Definisjonen gir ingen nærmere veiledning om hva som ligger i frivilligkravet. Imidlertid, skal det tas hensyn størst hensyn til «blant annet» om «oppfyllelse av en avtale, «herunder» om yting av en tjeneste, er gjort betinget av samtykke til behandling av personopplysninger som ikke er nødvendig for å oppfylle nevnte avtale», jf. GDPR-forordningen art. 7 nr.4.

Informasjonskapsler som tjener for levering av nettopp den tjenesten brukeren ønsker å bruke eller oppnå, er unntatt fra denne regelen. Et samtykke avgitt til slike informasjonskapsler, vil dermed anses gyldig etter en analogisk anvendelse av siste leddet i bestemmelsen. For en nærmere vurdering av hvilke informasjonskapsler som faller under denne kategorien, se punkt 3.4. Det minnes om at samtykkekravene er de samme, uavhengig av om informasjonskapselen inneholder personopplysninger eller ei, se overfor punkt 3.2.5.2.

Denne bestemmelsen presiserer størrelsen av vekten som dette momentet skal ha i frivillighetsvurderingen, men den er taus når det gjelder om det slår i det ene eller den andre retningen. Formålet med samtykke er å gi individet et reelt valg og styring over behandlingen. Dersom ytelsen er betinget av samtykke til informasjonskapsler, er det grunn til å tro at brukeren vil i så fall ikke gis noen reelt valg.

Dessuten heter det videre i fortalene at: «*samtykke **antas** ikke å være frivillig avgitt dersom ... oppfyllelsen av en avtale, **herunder** yting av en tjeneste, avhenger av samtykket, til tross for at et slikt samtykke ikke er nødvendig for å oppfylle avtalen [min utheving].*»⁸² Dette er i samsvar med tolkningsalternativet om at individet ikke gis et reelt valg og kontroll, og at dette

⁸² GDPR, Fortale punkt 43

momentet trekker derfor i retning av at det ikke anses som et frivillig avgitt samtykke/ erklæring.

Herunder

Begrepet «herunder» tyder på at den oppgitte listen i bestemmelsen ikke er uttømmende. Derfor kan man også legge vekt på andre forhold som er gjort betinget av samtykke. Arbeidsgruppen-29⁸³ har avsagt en uttalelse, hvor de presiserer begrepet. Det nevnes at i tillegg til konkrete omstendigheter av å binde samtykke til kontrakter, kan også ethvert generelt upassende press eller påvirkning på brukeren føre til at samtykket ikke anses frivillig avgitt.

Flere tilfeller vil kunne falle inn under «upassende press og upassende påvirkning». Noe som på den ene siden er bra ettersom den beskytter individet, og fører til at et reelt valg foreligger.

På den annen side, fører det til at terskelen senker for å anse et samtykke ugyldig. Siden forutsetningen er at det skal foretas en helhetsvurdering i hvert enkelt tilfelle, vil dette muligens føre til at ulike domstoler og ulike land tolker det forskjellig. Noe som kan føre til forskjellig praksis i ulike land, og som igjen er i strid med forordningens formål om å harmonisere reglene for alle EU/EØS-land for å verne lik beskyttelse til alle borgere.

Dessuten er ikke uttalelser fra arbeidsgruppen bindende til tross for at de kan tillegges mye vekt i praksis. I fravær av relevant praksis i område er det vanskelig å si hva som vil være den riktige tilnærmingen.

Rettstilstanden er dermed i øyeblikket uklar og en eventuell avklaring om dette, må komme fra EU-domstolen.

Blant annet

Begrepet «blant annet» tilsier, at man kan også legge vekt på andre forhold i den konkrete vurderingen om frivillighet. Et forhold som kan muligens tillegges vekt på er, hva slags nettside er det snakk om. Om det er nettside som ut ifra et objektivt perspektiv *tilbyr mindre viktige tjenester/produkter* eller om nettsiden tilbyr *essensielle tjenester eller tjenester* som brukeren ikke få tilgang til ellers.

Det kan, for eksempel, være snakk om skatteetatens nettsider hvor man er avhengig av å logge seg inn, og bruke nettsiden for å hente informasjon om sin skatterettslige posisjon. Dette får man ikke gjort i papirversjon lenger. Mange tjenester er blitt digitalisert, og krever bruk av nettsider for at man skal få gjort det man må gjøre. Det samme gjelder lånekassens

⁸³ Artikkel 29-gruppen, Opinion 15/2011, s. 5

nettsider, hvor det er snakk om låneopptak som kan anses en nødvendig tjeneste for studenter osv.

Dette kan tyde sterk i retning av at man ikke har et reelt valg, å velge mellom en digitalisert eller en papirversjon. Frivillighet i slike tilfeller kan være et konsept man kan bruke for å argumentere i den ene eller den andre retningen.

Både forordningen og ekomdirektivet sikter å gi brukeren kontroll over behandlingen av sine opplysninger. Det er imidlertid nevneverdig at denne kontrollen skal også ha visse grenser. Andre samfunnsmessige hensyn bl.a. økonomiske eller effektivitetsårsaker, gjør at institusjoner og bedrifter velger å bruke de nye teknologisk metodene for å utføre sine gjøremål.

Tillit er imidlertid et grunnleggende prinsipp for den globale økonomien, og den globale økonomien er digital. En av de viktigste utløsende årsakene til GDPR, er nettopp den sterke økning av bruk av personopplysninger gjennom teknologi. Det var ikke særlig stort fokus⁸⁴ på dette rettsområde helt til man ble kjent med hvordan disse opplysningene kan misbrukes⁸⁵.

Det ville føre til at mange brukere ville ikke lenger hatt tilstrekkelig tillit til teknologien, og minske eller unngå bruk av teknologien eller nærmere sagt internett. Noe som ville føre til at økonomien kunne bli svakere. Derfor heter det i fortalene⁸⁶ til GDPR at det er viktig «å skape den nødvendige tillit som vil gjøre at den digitale økonomien utvikler seg i det indre marked [min utheving]», noe som er historisk kjernen av det EU driver med⁸⁷.

Det vil derfor si at teknologier vil uansett bli brukt av institusjoner og bedrifter, det er uunngåelig, men forsøket her er likevel å verne individet og gi vedkommende en viss kontroll over behandling av disse personopplysninger om han eller hun. Ut ifra dette kan det sies at konseptet om frivillighet skal ikke tolkes dit hen, at brukeren gis kontroll over hvilken metode en netteier skal bruke for å gjennomføre sine gjøremål/ tjenester de tilbyr. Den skal heller gi et reelt valg til individet over hva slags opplysninger netteieren kan bruke.

Samtidig vil begrensning av kontrollen individet har, være styrkende for sikkerheten av opplysningene mot angrep fra uvedkommende. Til tross for et samtykke fra individet, pålegges

⁸⁴ Personvernregler eksisterte før denne tiden også, men det var mer snakk om regler som var milde og ikke-bindende, såkalt «soft law»

⁸⁵ Se f.eks snowden reviliations som opplysninger brukes i overvåkningssammenheng eller det faktum at markedsførende annonser har tatt helt av og rapporter viser at de kan få brukerne til å betale mer for enn vare enn de må.

⁸⁶ GDPR, fortale punkt 7

⁸⁷ EØS-avtalen art.1, EU-traktaten art.1

den dataansvarlige å minimere bruk av personopplysninger til det som er rimelig for å utføre sine tjenester på en «fair» måte, og i henhold til forordningens generelle prinsipper⁸⁸. Noe som kan leses ut ifra forordningens og direktivets kontekst.

Art. 5 (3) tilsier at individet selv kan tillate at netteieren lagrer opplysninger i vedkommendes utstyr og kan få tilgang til disse. Likevel fører ikke samtykke til at netteieren kan gi avkall på sine forpliktelser i henhold til prinsippene om rettferdig, lovlig og minimum bruk av opplysninger. Disse prinsippene er preseptoriske, og kan derfor ikke avtales til skade for brukeren.

Derfor kan det ,oppsummeringsvis, sies at individet har et reelt valg å bruke eller la være å bruke, men dette er ikke alltid like klart. For nettsider som tilbyr nødvendige tjenester, kan det tenkes at frivillighetselementet er ikke like sterk.

Likevel tilsier argumentene ovenfor at for slike nettsider skal det mye til for at de skal lagre opplysninger eller få tilgang til opplysninger, utover det som er strengt nødvendig for utførelse av tjenesten. Ofte kan disse også være unntatt fra kravet om innhenting av samtykke.⁸⁹

Derimot om det er en nettside man kan fint la være å gå inn på, så kan det tenkes at man selv velger i større utstrekning å akseptere informasjonskapslene.

Et annet element kan falle under «blant annet» er om det vil spille en rolle hvorvidt nettsiden er en *offentlig nettside*.

På den ene siden, skal brukerne ha tillit til det offentlige. De skal stole på at en offentlige nettsideeier vil ikke lagre opplysninger på dere terminalutstyr, utover det som er nødvendig for drift av nettsiden.

På den annen side, viser en empirisk undersøkelse at 97% av norske offentlige nettsider deler opplysningene av brukerne med tredjeparter, som i en stor grad benyttes i markedsføringsammenheng. Det kan svekke tilliten til det offentlige generelt, men særlig ved bruk av deres nettsider.

⁸⁸ GDPR art. 5 om generelle personvernrettslige prinsipper

⁸⁹ Se under punkt 3.4 for en nærmere presentasjon av hvilke informasjonskapsler anses å være strengt nødvendige.

Dette kan derfor i lys av EU/EØS lovgivningens formål om å verne personopplysninger til individer og de generelle prinsippene om behandling av personopplysninger⁹⁰, være et sterkt moment mot at brukeren er gitt et reelt valg.

Antas

Uttrykket «antas» i fortalen, kan tyde på at det ikke er en absolutt regel. Det kan derfor tenkes at til tross for at oppfyllelse av avtale var gjort betinget av samtykke til behandling av personopplysninger, vil samtykke likevel anses for å være frivillig avgitt. Imidlertid, siden dette er nevnt i fortalene og ikke i selve bestemmelsen, er det noe svakere grunnlag å basere seg på denne tolkningen. En slik tolkning vil uansett svekke personvernet til nettbrukere.

Det er derfor gode grunner for at et slikt unntak burde ha vært formulert i selve bestemmelsen. Motsatte kan kun legges til grunn dersom EU-domstolen kommer frem til denne tolkningen i en av sine senere avgjørelser.

Oppsummering og konklusjon:

Det konkluderes derfor med at samtykke for lagring av opplysninger eller anskaffelse av tilgang til lagrede opplysninger, **er gyldig i tilfeller hvor samtykke til informasjonskapsler er en forutsetning for at brukeren skal kunne fortsette å bruke nettsiden. Dette gjelder dog**, så lenge disse er nødvendige for å oppfyllelse av avtalen brukeren ønsker å inngå.

3.3.6. På hvilke måter kan samtykke innhentes?

Det foreligger ingen klare holdepunkter i ordlyden til ekomloven § 2-7b som kan indikere måten samtykke må gis i. Det finnes heller ingen rettspraksis. Forarbeidene⁹¹ nevner midlertid at det anses gyldig samtykke når «sluttbruker benytter en **teknisk innstilling i nettleser eller tilsvarende** i de tilfeller dette er teknisk mulig og effektivt.»

NKOM har også i sin veiledning om hvordan akseptere og avslå cookies sagt at «også Forhåndsinnstilling» i nettleser om at bruker aksepterer cookies. Forutsatt at det foreligger klar og tydelig info tilgjengelig på nettstedet, slik det også kommer frem av lovteksten.

Ingen krav til plassering er oppstilt. Det kan være nok at den er nevnt et eller annet sted. Det er heller ingen krav til separat advarsel eller krav til mengden av informasjon og oppsetnin-

⁹⁰ Disse er generelle prinsipper som gjelder innen personvern, og er nedfelt både i Convention 108+ og GDPR art.5 særlig punkt nr. 1.

⁹¹ Prop. 69 L 2012-2013

gen. NKOM sine veiledninger er dermed meget romslig og vid. Ingen veiledning om hva som er å anse «klar og tydelig».

Ekomdirektivet art. 5 nr.3 gir heller ingen veiledning, med unntak av «given» som tyder på at det kreves en handling for å anse samtykke gitt. Ekomdirektivets fortalen punkt 17 lest sammen med formålet tilsier at en bruker kan gi samtykke på en «rimelig måte». Hva som ligger i «rimelig» er ikke nærmere presisert i fortalene, men det kan være enhver form for handling som viser viljen til samtykke.

Det fremgår videre av fortale 32 til forordningen at samtykke kan være skriftlig, muntlig eller skje ved bruk andre elektroniske midler. Av bevismessige årsaker er det best å oppnå samtykke skriftlig, men det kan være vanskelig å få det til alltid. Andre former for elektroniske midler kan utgjøre lydopptak, forutsatt at informasjon om det er gitt før samtykket gis.

På den annen side, fremgår det av betraktning 66 av direktivet-2009 at samtykke til cookies «*may be expressed by using the appropriate settings of a browser or other applications*». Det vil si at, brukeren anses for å ha avgitt sitt samtykke til lagring eller tilgang til opplysninger i sitt terminalutstyr gjennom antesiperte innstillinger på nettleser som Safari, Internet Explorer, Chrome o.l.

Det innebærer at brukeren ikke må aktiv foreta en handling for å vise sin vilje. Vedkommende kan selvfølgelig nekte mottak av dette gjennom sin nettleser innstillinger. Det trekker i retning av at samtykke krever ikke en aktiv handling.

Når man kommer inn på en nettside, overføres dine personlige data allerede via informasjonskapsler. De sakkyndige i feltet mener derfor at det er meningsløst i etterkant å slå av informasjonskapsler gjennom innstillingene på nettleseren.⁹² Fra et teknisk perspektiv er dette derfor ingen god løsning for å hindre overføring av opplysninger.

Elementet om at det må være en «indikasjon av viljen» til brukeren peker på krav til aktiv handling. Dessuten, tilsier også bestemmelsens natur at gjennom endring av ordlyden i 2009 til “given” må det ha vært meningen å kreve en aktiv handling, se punkt ovenfor 3.3.2.

Dessuten la EU-domstolen vekt på at dersom aktiv handling ikke kreves, vil det være lite sannsynlig at brukere faktisk leser informasjon før de gir sitt samtykke som fører til at de

⁹² Personlig kommunikasjon i e-post med Konsernsjef i Cookie Information AS, Karsten Rendemann, 20. November 2019.

Øvrige vilkårene som «informert» vil heller ikke anses for å være oppfylt⁹³. Domstolen konkluderte med at ekomodirektivets bestemmelser lest sammen med bestemmelsene i oppevede direktivet tilsa at det måtte foreligge en aktiv handling for å anse samtykke gyldig⁹⁴.

EU-domstolen la til grunn i samme sak at den samme tolkningen gjelder i forhold til GDPR, men den ser til å stille enda strengere krav til samtykke enn det oppevede direktivet⁹⁵.

Begrunnelsen er at begrepet «utvetydig viljestyring» er blitt lagt til i definisjon av samtykke i art. 4 nr. 11. Det innebærer at det må ikke foreligge tvil om viljen til brukeren. Noe som anses vanskelig å bli oppfylt enn gjennom aktiv handling.

Dessuten krever GDPR uttrykkelig en «clear affirmative action» eller «tydelig bekreftelse» som tydeliggjør kravet om aktiv handling. Det betyr at brukeren må ha tatt en «deliberate action» eller «bevisst handling» for å gi samtykke til den spesifikke behandlingen⁹⁶

Fortale punkt 32 tilsier at det anses for å være «aktiv handling» når man kan oppnå samtykke ved avkrysning av. Samtidig ekskluderer den bruk av passiv, avkrysningsbokser som er avkrysset på forhånd eller inaktivitet.

Det er derfor klart at et samtykke innhentet gjennom innstillingene på nettleser, er ikke ansett gyldig samtykke.

Videre konkluderte dommen at samtykke for bruk av cookies ikke er gyldig, hvis den kan oppnås gjennom en forhåndsmarkert avkrysningsboks, hvor brukeren må aktivt fjerne avkrysningen for å kunne nekte samtykke.⁹⁷ Det stilles krav til hvordan anmodningen må være utformet.

På lik linje med disse kan heller ikke innstillinger på nettleser anses for å utgjøre en aktiv handling ettersom ofte vil nettlesernes vanlige innstilling gi fullstendig tillatelse til lagring av cookies. Det samme vil gjelde for når brukeren fortsetter bruk av nettside. Det er en passiv handling som ikke viser viljen til brukeren. Dette synspunktet har også vært støttet av arbeidsgruppen-29 i deres uforbindende uttalelser.⁹⁸

⁹³ *Planet49*, C-673/17, punkt 56.

⁹⁴ *Ibid.*

⁹⁵ *Ibid.*, punkt 61.

⁹⁶ Artikkel 29-gruppen A29WP, 17/EN WP259 rev.01 (2018), s. 16.

⁹⁷ *Planet49*, C-673/17, punkt 65.

⁹⁸ Artikkel 29-gruppen A29WP, 17/EN WP259 rev.01 (2018), s.17.

Konklusjonen blir dermed at det må foreligge en aktiv handling for å anse samtykke for å være gyldig for lagring av opplysninger eller for å få tilgang til allerede lagrede opplysninger gjennom cookies på en brukers terminalutstyr.

Ettersom GDPR er en moderne rettsakt, kan det være mange måter en bruker kan gi samtykke gjennom aktiv handling. Dette kan, for eksempel, være gjennom å vinke til mobilen eller se til sidene. Forutsatt at informasjon om at også slik kan samtykke til lagring eller gi tilgang til cookies er gitt på en klar og sammensatt måte.

3.3.7. Hva slags krav stilles det til informasjonsplikten?

Det fremgår av ordlyden til ekomloven § 2-7b at det skal gis informasjon om hvilke informasjonskapsler som anvendes, hvilke opplysninger som behandles, formålet med behandlingen, og hvem som behandler opplysningene.

I forarbeidene⁹⁹ heter det at det må i tillegg gis informasjon om hvilke informasjonskapsler som anvendes. Denne informasjonen må være gitt på en klar og tydelig måte i tillegg til å være lett tilgjengelig på nettsiden.

Ekomdirektivet art 5(3) krever at ved bruk av cookies, brukeren skal få «*clear and comprehensive information*» i henhold til GDPR, herunder, om formålet med behandlingen. Det refereres til GDPR art. 12, 13 og 14.

EU-domstolen i sin nylig avgitte avgjørelse, Planet49, ble presentert nettopp for dette spørsmålet. Avgjørelsen ble tatt med henvisning til advokat generalens synspunkt.¹⁰⁰

Det ble lagt til grunn at vilkåret om «*clear and comprehensive information*» innebærer at brukeren er i en posisjon til å kunne lett beslutte konsekvensene av hvilket som helst sam-

⁹⁹ Prop. 69 L 2012-2013, kapittel 12 merknader til de enkelte bestemmelser, til ny § 2-7b

¹⁰⁰ se punkt 74 av dommen

tykke hun/han vil gi. Vedkommende må også kunne være sikker på at samtykket er tilstrekkelig informert¹⁰¹.

Det fremgår også at informasjonen må klart være sammenhengende, og tilstrekkelig detaljert. Slik at den muliggjør at brukeren forstår funksjonen av og formålet ved informasjonskapsler i bruk. Ut fra hvilket vedkommende skal kunne forutberegne konsekvensene for et eventuelt samtykke.

Ekomdirektivet art. 5 nr. 3 viser til bestemmelsene i GDPR om hva slags informasjon som skal gis. GDPR art. 13 som gir en liste over informasjon som skal gis til datasubjektet, når oppsamlede opplysninger stammer fra vedkommende selv. GDPR art. 14 derimot, gjelder tilfeller hvor opplysningene anskaffes fra andre¹⁰².

Begrepet «herunder» i art. 5(3)¹⁰³ sikter til at lista over informasjonen som skal avgis ikke er uttømmende. Dette tilsier at også andre opplysninger der det er nødvendig, må også avgis. Det kan, for eksempel, være informasjon om hvem mottakere av opplysningene er. Angitt enten spesifikt eller bare kategorisert. Så lenge slik videre informasjon er nødvendig under konkrete omstendigheter for å sikre en rimelig behandling i forhold til datasubjektet.¹⁰⁴

Problemstillingen er om det samme gjelder i norsk rett. Nærmere sagt, er spørsmålet hvorvidt informasjonskravet i ekomloven likestilt med informasjonskravet i bestemmelsene til GDPR-forordningen.

For dette spørsmålet henviser jeg til drøftelsen gjort ovenfor om hvorvidt samtykkekravet likestilles i ekomloven og personvernforordningen under punkt 3.3.3.

Dessuten fremgår det av forarbeidene til bestemmelsen at endringen medfører «skjerpet» krav til informasjon(...) for å gi brukerne mulighet til å ivareta sine rettigheter. I tillegg til at bestemmelsen er en gjennomføring av art. 5 (3) noe som tilsier at til tross for at det ikke uttrykkelig fremkommer av ordlyden i ekoml. § 2-7b, er rammen av artikkelen i direktivet at denne informasjonen må være i samsvar med bestemmelsene i det opphevede direktivet (GDPR- nå)¹⁰⁵.

¹⁰¹ Informert samtykke foreligger når brukeren får informasjon før vedkommende gir sitt samtykke.

¹⁰² Databehandlere som er tredjeparter, offentlige tilgjengelige kilder, andre rettssubjekter, databrokers mv.

¹⁰³ Ekomdirektivet artikkel 5 nr. 3

¹⁰⁴ Planet49, punkt 76

¹⁰⁵ GDPR art. 94 nr.1

Det fremgår av presumpsjonsprinsippet at norske bestemmelser som gjennomfører en EU/EØS rettslig artikkel, må anses å ha vært gjennomført med samme innhold som EU/EØS retten krever¹⁰⁶.

Det er klart at ekomdirektivet henviser til bestemmelsene i opphevedirektivet, nå GDPR. En riktig gjennomføring av ekomdirektivets art. 5(3) innebærer at informasjonen må angis i samsvar med reglene i GDPR.

I og med at det fremdeles er tvil om lovgiveren har gitt uttrykk for at gjennomføringen skal fravike vår eøs-rettslige forpliktelsen, legges det til grunn at det var ønskelig med å gjennomføre samme innholdet som det fremgår av art. 5 (3) av ekomdirektivet.

Det konkluderes derfor med at ekoml. § 2-7b er å forstå slik at informasjonskravet etter denne bestemmelsen må være i samsvar med reglene i personvernforordningen.

3.3.7.1. Må det informeres om lengden av behandlingen?

Art.13 av GDPR nevner ikke uttrykkelig at det må informeres om lengden til behandling av opplysninger. Imidlertid, inneholdte art. 10 av opphevede direktivet begrepet «at least» som antyder at listen over hva slags informasjon som skulle gis, ikke var uttømmende.

Det at begrepet «at least» er fjernet fra ordlyden av artikkelen i GDPR, kan tyde på at lovgiver hensikten var å gi konkrete vilkår til hva slags informasjon som skal gis. Det samsvarer med lovens formål om å harmonisere reglene i dette område.

I en artikkel¹⁰⁷ sist oppdatert i 2013, viser analysen at det forelå ingen felles retningslinjer med nærmere spesifisering av hva slags formidling ville være i samsvar med gjeldende regler, bortsett fra retningslinjer som med vide forslag til informasjonskravet.

Nederlandske retningslinjer gir vid og generell veiledning mens de britiske er veldig detaljerte, kategoriske og standardiserte. Basert på dette samt fjerning av begrepet fra ordlyden, kan støtte argumentet om at fjerning av “at least” fra ordlyden skulle føre til presise vilkår til hva slags informasjon kreves å være gitt.

¹⁰⁶ Sejersted, (2011), s. 265; Finanger-I Rt. 2000s.1811, Presumpsjonsprinsippet er norsk rettskildesprinsipp som tilsier at der det er flere tolkningsalternativer, skal det tolkningsalternativet som er i samsvar med den internasjonale regel legges til grunn. Dette gjelder dog ikke dersom det fremkommer klart at norske lovgiveren ønsket å fravike den internasjonale forpliktelsen.

¹⁰⁷ Luzak (2014), s. 548-559

På den annen side, informasjon om lengden til behandling av opplysninger er ganske viktig for en å beregne sin stilling, og til enhver tid vite hvor man har sine opplysninger fremdeles lagret. Det gir en slags forutsigbarhet til individet.

Samtidig tilsier prinsippet om «fairness» og «transparency»¹⁰⁸ altså rimelighet og åpenhet, at man bør få informasjon om dette ettersom lengden av behandling kan være lang eller t.o.m ubegrenset behandling. Noe som betyr at et stort omfang av opplysninger om brukeren kan finne seg hos netteieren. Det vil også minske brukerens mulighet til å utøve andre rettigheter som f.eks. å kreve sletting av informasjonskapslene eller overføring av disse til en annen dataansvarlig.

Dessuten har EU-domstolen¹⁰⁹ fastlagt at det må informeres om lengden av behandlingen.

Det konkluderes dermed at lengden til behandlingen av opplysningene i cookies, må formidles til brukeren.

3.3.8. Hvilke krav stilles det til formidling av informasjonen om samtykke til cookies?

Uttrykket «klar» tilsier at det stilles krav til klar og enkel språkbruk, som er rettet mot allmennheten, ikke kun jurister. Setningene må ikke være lange, vanskelige å forstå eller innebære for mange juridiske terminologier.

I tillegg, tilsier prinsippet om åpenhet¹¹⁰ at informasjon om behandlingen og dens konsekvenser til datasubjektet må avgis på en kortfattet, åpen forståelig og lett tilgjengelig måte og på et klart og enkelt språk. Dessuten må visualiseringsmetoder også brukes, der det er passelig.¹¹¹

Et eksempel på implementering av visualisering for bedre forståelse kan vi se på Google sine retningslinjer¹¹² om personvern. Google har brukt video med lyd for enklere forståelse av hva deres personvernregler dreier seg om, og hvordan de gjør bruk av opplysningene. Dette

¹⁰⁸ GDPR, fortaler punkt 39.

¹⁰⁹ Planet49, punkt 78

¹¹⁰ Prinsippet er nedfelt i GDPR art.5 og fortale punkt 58, 60, 39, se også GDPR art. 10 nr. 2

¹¹¹ GDPR fortale, punkt 58

¹¹² Google (2019)

øker muligheten for å fange brukerens oppmerksomhet, og samtidig bidrar til en bedre forståelse av innholdet av informasjonen.

Det er imidlertid også stilt krav til at i tillegg til å være klar, må informasjonen også være omfattende¹¹³. Hvor omfattende informasjonen skal være er i stor utstrekning avhengig av kunnskapen til mottakerne.¹¹⁴ Nettsideeier av en vanlig¹¹⁵ nettside skal ta hensyn til den gjennomsnittlig brukers kunnskap og forventninger.¹¹⁶

Mens nettsiden rettet mot funksjonshemmede, personer med utenlandskbakgrunn eller minoritetsbakgrunn, personer med dysleksi osv. Etter identifisering av mottakergruppene, må ta hensyn til deres språklige utfordringer¹¹⁷. Det vil dermed ut fra lovgivningens formål og generelle prinsippene om åpenhet stilles strengere krav til klarhet i språket, mindre bruk av juridiske uttrykk samt tilpasse hvor omfattende informasjonen bør være.

Ofte vil for mye informasjon også være forvirrende, og brukes som en metode for å øke sannsynligheten for at brukeren ikke leser hele informasjonen og samtykker. Dette skal det diskuteres mer om under punkt 3.3.10 om dark patterns.

3.3.9. Utformingen

Hvordan oppnår man et informert samtykke er blant annet avhengig av at brukeren er blitt informert fullt ut, har forstått informasjonen, og sier seg enig til behandling av sine opplysninger. Ofte er det slik at brukere ikke leser informasjonen avgitt, og samtykker uten å vite hva de samtykker til.

Spørsmålet blir derfor om loven stiller noen krav til hvordan informasjonen skal utformes og gis.

Som tidligere nevnt, stiller ekomloven § 2-7b krav til at informasjonen må være «klar og tydelig». Utfordringen er her å gi en enkelt, men samtidig sammenhengende informasjon.

¹¹³ «Comprehensive» ,jf. Ekomdirektivet art. 5 nr. 3.

¹¹⁴ Milne og Culnan (2004), s. 19

¹¹⁵ Som ikke er spesielt rettet mot noen spesifikke grupper

¹¹⁶ Dette kan leses i vilkåret «intelligible», lett forståelig, se Artikkel 29-gruppen, WP260 rev.01, punkt 9

¹¹⁷ Ibid, punkt 16

Det fremgår av ordlyden av dataansvarlige kan selv velge gjennom «appropriate measures» hvor mye og hvordan de skal formidle informasjonen.

Ordlyden er vid og gir ingen særlig veiledning om hvordan dette skal gjennomføres i praksis. Bakgrunnen for dette er at GDPR er en proaktiv lovgivning, som skal sikre at loven til enhver tid går i samme takt med den raske teknologiske utviklingen. Fordelen ved dette for dataansvarlige er at de gis friheten til å velge virkemidlene selv. Ulempen er at de får hele ansvaret om å gjøre dette på en tilstrekkelig riktig måte for å unngå enorme bøter.

I praksis bruker mange, så kalte «layers»¹¹⁸ eller lagdelte og detaljerte opplysninger. Disse løsningene er også anbefalt i retningslinjer om prinsippet om åpenhet under GDPR¹¹⁹, hvor det beskrives at teknikken kan forbedre søk av enkelte saker blant mange sider med tekst. Retningslinjen anbefaler dernest også bruk av «push and pull» erklæringer samt andre metoder¹²⁰. Denne friheten til å velge teknologiske midlene til å presentere informasjonen, kan også misbrukes gjennom Dark-patterns.

3.3.10. Dark Patterns

Dark patterns er metoder som nettsider og apper bruker for å få brukerne til å gjøre ting de ellers ville ikke ha hensikt til å gjøre, for eksempel, lettere si ja til informasjonskapsler på grunn av måten teksten er utformet på, fargen på alternativene eller skape forvirring gjennom å plassere samtykkevalget etter mange klikk for å gjøre det tungvint for brukeren.¹²¹

Forbrukerrådet i Norge kom med en rapport om hvordan teknologisk selskaper bruker dark patterns for å tvinge brukere til samtykke, og valg av mindre personvernvennlige innstillinger. Eksempelvis, misvisende/påtrengende standarder for innstillinger på nettsider, tvetydig ordbruk, valgstrukturer som gjør det vanskelig for brukeren å velge et mer personvernvennlig alternativ.¹²²

Spørsmålet er om personvernlovgivningen beskytter brukerne mot slik design og utforminger som kan manipulere dem til å gi samtykke.

¹¹⁸ På forsiden av nettsiden en liten fane er synlig med de mest sentrale informasjonen samt alternativene for å samtykke, ikke samtykke og et alternativ hvor man kan lese mer og justere samtykke i forhold til ulike former cookies. Se Arbeidsgruppen-29, WP260 rev.01 punkt 36

¹¹⁹ Arbeidsgruppen-29, WP260 rev.01, punkt 8 og 35

¹²⁰ Ibid, punkt 39

¹²¹ Forbrukerrådet (2019) s. 1-2

¹²² Ibid, s.6-7.

Ekomloven har ingen bestemmelser om personvern innebygd i design. Slik at det stilles ingen krav til implementering av design på nettsiden.

NKOM har imidlertid, kommet med noe veiledning¹²³ om dette. Det anbefales at informasjonen er lett synlig når brukeren kommer inn på nettstedet. Det kan formes som topp tekst, bunntekst eller en pop-up, hvor «cookies eller informasjonskapsler» brukes, slik at brukeren vet hva informasjonen dreier seg om. For det første, er ikke denne veiledningen bindende. For det andre, veileder den kun om plassering av informasjonen og hva som skal oppgis. Ekomodirektivet inneholder heller ingen forslag til utforming av design.

Problemstillingen retter seg først og fremst mot vilkåret om frivillighet, jf. Personvernforordningen art. 4 nr.11 og art. 7.

Verken forordningen selv eller fortalene nevner konkret noe om dette. I fortale 42 siste setningen nevnes det at samtykke ikke er frivillig avgitt der datasubjektet ikke er gitt et genuint eller fritt valg. At ulike teknologier brukes for å påvirke datasubjektets vilje til å selv foreta et valg uten å ha blitt påvirket av andre faktorer, taler sterkt mot at det er gitt noe genuint valg.

Imidlertid, må det på et eller annet tidspunkt settes grenser for hva som anses for å være forsvarlig. Forretninger er avhengig av å oppnå samtykke for innhenting av opplysninger som er meget viktig for deres virksomhet og den generelle økonomien i det indre markedet. Lovgivningen gir heller ingen konkret veiledning for hvordan dette skal gjøres. Det vil bero på utvikling av teknologien, og hvordan mennesker reagerer på ulike anvendte metoder. Det taler for at det må mye til før et design eller noe misvisende utforming, kan anses for å manipulere for brukerne.

På den annen side, det er det vises at store aktører i område som Facebook, Google og andre ressurssterke aktører, gjør bruk av slike teknikker for å lure vanlige mennesker. Makt ubalansen mellom dataansvarlige og datasubjektet i et slikt tilfelle ha stort gap. Det skal i slike tilfeller lite til før samtykke gitt under slike omstendigheter ikke kan anses for å være frivillig. Prinsippet om «transparency»¹²⁴ tyder i tillegg på at informasjonen om anmodningen må presenteres for brukeren på en enkel og lett forståelig måte. Det vil derfor heller ikke et helt fri og reelt valg for brukeren til å velge. Det vil derfor bli ansett ufrivillig.

¹²³ NKOM (2019)

¹²⁴ GDPR art. 5 nr. 1 og fortalene punkt 39

I tillegg til frivillighet, vil det være tvilsomt om vilkåret for tvetydighet anses for å være oppfylt. I og med at det skal være utvetydig at brukeren hadde intensjon til å gi sitt samtykke, er det gode grunner for å argumentere at dersom det er gitt mye informasjon og brukeren er nødt til å klikke på flere sider for å komme seg til samtykkealternativene øker dette sannsynligheten for at en påvirkning på valget hennes er blitt gjort. Det fører til at samtykke ikke er utvetydig at samtykke er gitt frivillig.

Bevisbyrden ligger dessuten på den dataansvarlige som må bevise at samtykke er gitt frivillig. Jo mer utformingen og designet er manipulerende, des vanskeligere blir for dataansvarlige å bevise utvetydigheten av brukerens vilje til samtykke. Noe som også tilsier at vilkåret om frivillighet er heller ikke oppfylt.

Oppsummeringsvis kan det sies at design-og utformingsteknikker som kan være manipulerende for datassubjektet og påvirker vedkommendes valg, er å anse i strid med frivillighetselementet som kreves av et gyldig samtykke.

3.3.11. **Hvem** er ansvarlig for at vilkårene er oppfylt?

Det fremgår ikke direkte av ekomloven hvem som ansvarlig er for at vilkårene for et gyldig samtykke, skal være oppfylt. Før lovendringen i 2012, var det databehandleren i henhold til personopplysningsloven som skulle opplyse formålet med behandlingen.¹²⁵ Opplysningene som ble lagret eller anskaffet adgang til, inneholdte ikke bare personopplysninger. Slik at man ikke alltid hadde en behandlingsansvarlig i henhold til personopplysningsloven.

Etter lovendringen ble selve handlingen «lagring eller hente informasjon» omfattet av bestemmelsen.¹²⁶ Det er dermed den som er ansvarlig for handlingen som må påse at vilkårene blir oppfylt. Med ansvarlig menes den som «bestemmer midler og formål for lagring eller henting av informasjon, og ikke nødvendigvis den som utfører den.»¹²⁷ Dette er i samsvar med ekomdirektivets art. 5(3).

¹²⁵ Prop. 69 L 2012-2013

¹²⁶ *ibid*

¹²⁷ *ibid*

For tredjepartsinformasjonskapsler (typisk er en annonse på et annet nettsted) har NKOM¹²⁸ i henhold til bestemmelsen, instruert at den som setter en slik informasjonskapsel, vil være ansvarlig for å oppfylle informasjonskravet på sitt eget nettsted.¹²⁹ Mens den som tillater bruk av tredjepartsinformasjonskapsler på sin egen nettside, må informere om dette i tillegg til informasjon om sine egne informasjonskapsler.¹³⁰

Det er tvilsomt hvorvidt det er den som tillater bruk av tredjepartsinformasjonskapsler, som må innhente samtykke for bruk av disse informasjonskapslene.

Loven er taus. Forarbeidene nevner ikke noe uttrykkelig om hvem som må innhente samtykke i et slikt tilfelle. Ut ifra hvem som er ansvarlig for å gi informasjonen, kan det sies at vedkommende må også ha ansvaret for å innhente samtykke.

Det er derfor mest riktig å anta at det er den som tillater bruk av tredjepartsinformasjonskapsler på sin hjemmeside, som må innhente samtykke for bruken.

Både av hensyn til enkeltheten av prosessen for individet, og av hensyn til at det er selve nettsideeieren som gjør det mulig at disse kapslene kan lagres og gis videre til tredjeparter. Reelle hensyn taler derfor i retning av at den som er ansvarlig, og må gi informasjon til brukeren har også plikt til å innhente samtykke. Det konkluderes derfor med at den dataansvarlige som gir informasjon, er også pliktig til å innhente samtykke til bruk av informasjonskapsler.

Spørsmålet blir om det samme gjelder så kalte sosiale «plug-ins» f.eks, Facebook-like knapp eller en tweeter-knapp på sin nettside osv.

3.3.11.1. «social plug-ins»

Opplysningene som en nettside lagrer i en brukers mobil eller PC, kan i utgangspunktet ikke brukes eller gis adgang til en annen nettside. For eksempel, en bruker besøker VG sin nettside. VG lagrer opplysninger i brukerens mobil. Når brukeren besøker Facebook, gis ikke Facebook adgang til å innhente de lagrede opplysningene som VG har foretatt på brukerens mobil.

¹²⁸ NKOM, Nasjonal kommunikasjonsmyndighet, er et forvaltningsorgan som har til oppgave å administrere det offentlige regelverket i post- og teleområdet og sørge for konkurranseregulering, hvorav en av arbeidsoppgavene er å gi standarder i områder som mangler detaljer i lov eller forskrift, jf. Ekomloven §§ 1, 10-2.

¹²⁹ NKOM (2019)

¹³⁰ *ibid*

Det finnes et unntak fra dette i tilfeller, hvor det er for eksempel en «like»-knapp fra Facebook på f.eks. en bloggside. Ved at en bruker besøker bloggsiden og klikker på «like»-knappen, vil de informasjonskapslene som er blitt lagret for bloggsiden, bli sendt til facebook sin side. Bloggsiden vil ikke ha kontroll over opplysninger som nettserveren overfører eller hva facebook som tredjepart, vil bruke de opplysningene for.

På grunnlag av dette kan det argumenteres at bloggsiden ikke er dataansvarlig, og har dermed ikke plikt til å innhente samtykke for denne overføringen, og heller ingen informasjonsplikt.

Spørsmålet blir dermed hvem som har ansvaret for å formidle informasjonen og innhente samtykke i slike forhold. Mer presist handler problemstillingen om hvem som er den dataansvarlige.

EU-domstolen har avsagt en dom¹³¹ i den forbindelse. Operatør av nettsiden, Fashion ID, hadde valgt å ha en sosial plug-in (facebook-knapp) på sin nettside. Gjennom dette ble personopplysninger¹³² overført til Facebook. Et av spørsmålene i saken var hvorvidt nettsideoperatøren, Fashion ID, anses for å være dataansvarlig i et slikt tilfelle.

Domstolen besvarte spørsmålet bekreftende. Formålet med den vide definisjonen av «dataansvarlig» er at den tolkes slik at den skal være effektiv, og verner individets personvern fullt ut.¹³³

Deretter viser avgjørelsen til at man kan være dataansvarlig alene eller sammen «joint controller».¹³⁴

Det fastsettes også at en privatperson eller en juridisk person kan bli ansett som dataansvarlig. Det forutsetter er at vedkommende utøver innflytelse over behandling av personopplysninger, for sine egne formål, og deltar under beslutning av formålene ved behandlingen.¹³⁵

¹³¹ Fashion ID, C-40/17

¹³² ulike opplysninger gjennom metadata, cookies og andre informasjon som brukeren selv skrev inn i første nettsiden

¹³³ Ibid, punkt 66

¹³⁴ Ibid, punkt 67

¹³⁵ Ibid, punkt 68

Avgjørelsen også tydeliggjør at felles behandlingsansvar (joint controller) krever ikke at ansvaret skal deles likt mellom dataansvarlige. Ulike operatører kan være involvert i ulike stadiene av behandlingen av personopplysninger, og i ulike grader. Det vil derfor variere hvor mye ansvar hver av de skal ha. Noe som må vurderes konkret i hvert enkelt tilfelle¹³⁶.

Plikten om innhenting av samtykke og gi informasjon, må gjenspeile de prosessene som vedkommende operatør faktisk bestemmer formålet ved behandlingen og måten den skal gjennomføres på.¹³⁷ Utfallet i denne saken ble at FashionID ble ansett ansvarlig for behandling av personopplysninger, men kun for lagring og overføring av opplysningene til Facebook. Facebook selv er ansvarlig for hvordan de behandler de overførte personopplysningene.

Selv om denne saken ble resonnert basert på det opphevede personverndirektivet, har den fremdeles stor relevans for hvordan den ville ha blitt tolket under GDPR. Det er ikke blitt foretatt noen rettsendringer om dataansvarliges forpliktelser og terminologien dataansvarlig. Det foreligger dermed gode grunner for å anta at det samme ville bli tolkningsresultatet under personvernforordningen.

Dessuten er saken blitt avsagt etter ikrafttredelse av GDPR. EU-domstolen har dermed også tatt hensyn til den rettsutviklingen som har skjedd. Det må dermed antas at resultatet er i overensstemmelse med gjeldende rett.

Nettsideeieren vil dermed få opplysningene direkte fra datasubjektet i slike tilfeller, og må derfor selv sørge for å innhente samtykke.

Reglene i art. 13 av GDPR må følges om hva slags informasjon som gis til rettssubjektet når det gjelder den delen av behandlingen som den førstedataansvarlige (i vårt eksempel bloggsiden) kontrollere midler og formålet til. Mens den andre dataansvarlige (i vårt eksempel Facebook) må oppgi informasjon med innhold som kreves i art. 14 av personvernforordningen.

3.3.12. Tidspunktet for innhentes av samtykke

Lovens ordlyd «har samtykket» tyder på at samtykke må være avgitt før lagringen eller adgangen til lagrede informasjonen, kan gis. Forarbeidene er taus om tidspunktet for

¹³⁶ Ibid, punkt 70

¹³⁷ Ibid, punkt 100

innhenting. I norsk rett skal man derfor innhente samtykke før behandlingen starter. Dette er også i samsvar med hva gjeldende rett i EU/EØS- rett krever.

3.4. Unntak fra kravet om samtykke

Ekomloven § 2-7b første ledd krever informert samtykke for bruk av informasjonskapsler. Dette vilkåret gjelder alle former for cookies, med mindre den faller under de alternative kriteriene i annet ledd.

Det første kriteriet gjelder når informasjonskapselen er brukt «utelukkende for det formål å overføre kommunikasjon i et elektronisk kommunikasjonsnett». Det andre unntaket gjelder når informasjonskapselen er «nødvendig for å levere en informasjonssamfunnstjeneste etter brukerens uttrykkelige forespørsel».

Til tross for at det gjøres unntak fra samtykkekravet, er det uten betydning for retten til å bli informert og eventuelle andre rettigheter i henhold til GDPR, som anvendes til behandling av personopplysninger uavhengig av om cookies anvendes eller ei.¹³⁸

«utelukkende»

Det kan kun gjøres unntak når formålet med bruk av cookies, er «utelukkende» å utføre den elektroniske overføringen.

Hva som ligger i begrepet, fremkommer ikke klart av ordlyden. På den ene side, kan utelukkende innebære at dersom cookies ikke benyttes, vil det ikke være mulig å utføre overføringen. På den annen side, kan det innebære at den dataansvarlige velger å bruke cookies, men kun for å utføre overføringen. Det første alternativet tilsier at begrepet utelukkende krever et element av nødvendighet mens i det andre handler det mer om preferanser.

Forarbeidene til ekomloven og rettspraksis fra norske domstoler gir ingen avklaring.

Det foreligger heller ingen klare holdepunkter fra EU-domstolens rettspraksis om forståelsen av dette, men en uttalelse fra arbeidsgruppen-artikkel 29¹³⁹ berører dette. «*The transmission of the communication must not be possible without the use of the cookie*»¹⁴⁰. Det taler i retning av at det kreves et element av nødvendighet for bruk av dette. Slik at dersom cookies ikke brukes, vil ikke utføring av overføringen være mulig.

¹³⁸ Artikkel 29-gruppen, A29WP, 00879/12/EN WP 194 (2012), se punkt 2.1 s. 2

¹³⁹ *ibid*, se punkt 2.1 s. 3

¹⁴⁰ *ibid*

Som tidligere nevnt, er uttalelsene fra dette organet ikke bindende, men de tillegges ofte vekt i fravær av en oppklarende EU-dom og når den er i samsvar med formålet til den rettsakten.

Dette tolkningsalternativet er i samsvar med direktivets formål om å verne individets rettigheter, og av det generelle prinsippet om minimering¹⁴¹ av bruk av opplysninger. Bruk av cookies kan være risikabelt, og da foreligger det ikke grunn til å gjøre brukeren sårbar. I hvert fall når overføringen kan fint gjøres uten bruk av slike. Sikkerhetsaspektet tilsier dermed også at cookies må kun brukes der overføringen ikke kan skje via vanlig nettleser funksjon uten slik teknologi (cookies).

Spørsmålet blir videre hvorvidt cookies utelukkende brukes for å *hjelpe, fremskynde eller regulere* overføringen. Man befinner seg da utenfor ordlyden av det «eneste formålet». Derfor foreligger det ikke tilstrekkelige grunner for å gjøre unntak fra samtykkekravet i slike tilfeller. Dessuten ble alternativet «facilitating» fjernet fra ordlyden etter endringen av direktivet i 2009. Noe som tilsier at også den europeiske lovgivers vilje, var at unntaket skulle kun gjelde vanlig overføring av kommunikasjon.

Derfor tolkes kriteriet slik at så lenge overføringen kan gjøres uten bruk av cookies, må det innhentes samtykke dersom den dataansvarlige likevel bestemmer seg for å gjøre bruk av cookies. Det er teknisk vurderingen hvorvidt overføringen kan skje med eller uten cookies i hvert enkelt tilfelle.

Uttalelsen foreslår å se på tre elementer¹⁴² ved fastsetting av om bruk av cookies er det eneste formålet eller strengt nødvendig.

Evnen til å rute opplysningene over nettverket, særlig ved å identifisere kommunikasjonssendepunktene, avsender og mottaker.¹⁴³ Hvorvidt cookies muliggjør evnen til å utveksle opplysningene etter riktig rekkefølgen og det siste er om den muliggjør evnen til å oppdage feil og virus i systemet.

«**nødvendig**» vs. «strictly necessary»

Det andre kriteriet som fører til unntak av samtykkekravet, er formulert annerledes i ekomloven enn det som står i ekomdirektivet. I ekoml. § 2-7b står det at informasjonskaps-

¹⁴¹ GDPR art. 5 nr. 1 bokstav c, Personopplysninger skal være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for.

¹⁴² Artikkel 29-gruppen, A29WP, 00879/12/EN WP 194 (2012), s. 3

¹⁴³ *ibid*, se punkt 2.1.1 om hvordan internett fungerer og informasjonskapslene funksjon i denne prosessen.

lene må være «nødvendig» mens i ekomdirektivet står det at det må være «strengt nødvendig».

«strengt nødvendig» tilsier at det ikke er tilstrekkelig med at informasjonskapselen er nødvendig for overføring av kommunikasjonen, men den må i tillegg være «strengtatt» nødvendig. Noe som tilsier at terskelen for å gjøre unntak er meget høy. Det skal dermed tolkes snevert.

Det er en språklig forskjell, men det fremgår av forarbeidene til bestemmelsen at unntakene skal tolkes svært snevert. Ettersom det er ingenting i øvrige rettskildene som taler for at det har vært meningen å innføre en unntaksregel som er mindre streng enn direktivets, må det antas at terskelen er like høy som direktivet foreslår.

For at dette kriteriet skal anses for å være oppfylt, må to elementer være til stede.

Det første er at brukeren må ha *uttrykkelig sendt en forespørsel*, altså har foretatt en positiv handling for å be om gjeldende tjenesten med klart definert perimeter. Det andre er at informasjonskapselen er *streng tatt nødvendig* for å muliggjøre *informasjonssamfunnstjenesten*, dvs. at dersom cookies deaktiveres, vil ikke tjenesten funke.

I fortale 66 av direktiv 2009/136 EC stilles det i tillegg krav til en klar sammenheng mellom det strengtatt nødvendige informasjonskapslene og levering av forespurte tjenesten.

«Informasjonssamfunnstjeneste» kan bestå av flere komponenter, noen av disse vil ikke bli brukt av alle brukerne eller vil bare tilfører brukeren bedre opplevelse. Som et eksempel, kan vi nevne en avisnettside som er tilgjengelig f.eks. føre til at brukeren under innlogget modus kan skrive kommentarer til publiserte artikler på nettsiden.

På sin side kan disse tilleggsfunksjonene operere med sine egne informasjonskapsler. Det er anbefalt¹⁴⁴ at informasjonssamfunnstjeneste skal anses for å være summen av flere funksjonaliteter, og den konkrete rekkevidden av en slik tjeneste kan variere etter hvilke funksjoner brukeren spør etter. I denne vurderingen må informasjonskapselen være nødvendig for levering av den spesifikke funksjonaliteten som er etterspurt, og funksjonen som er uttrykkelig etterspurt av brukeren.

3.4.1. Hvilke informasjonskapsler er unntatt fra kravet om samtykke?

¹⁴⁴ ibid, s. 4

3.4.2. Nødvendige cookies

Disse består av rent tekniske opplysninger og data som er nødvendig for sikkerheten av opplysninger og interaksjonen med nettsiden¹⁴⁵. De opplysningene sørger for at tjenesten fungerer skikkelig. Blant annet sørger de for å utveksle opplysningene i riktig rekkefølge, slik at riktig innhold blir innhentet. I tillegg til at noen av de kan bidra til å blokkere skadende programmer, og uvedkommendes forsøk på tilgang. Dette vil ofte gjøres gjennom informasjonsskapsler som utfører autentisering av brukerens identifikasjon¹⁴⁶.

Sesjonsavhengige informasjonsskapsler faller under denne kategorien ettersom oftest fører de utelukkende til overføring kommunikasjonen mellom en nettleser og nettserver til generell velfungering av nettsiden. I tillegg til at de forsvinner etter at nettleseren lukkes, se punkt 2.2.1. Nødvendige informasjonsskapsler er dermed unntatt fra kravet om innhenting av samtykke.

3.4.3. Funksjonelle cookies

Disse sikrer ulike funksjoner på nettsiden, og gir brukeren en bedre opplevelse gjennom lagring av innloggingsdetaljer, varer i handlekurver, språkinnstillinger, menypreferanser mv.¹⁴⁷ Faste informasjonsskapsler¹⁴⁸ brukes for å oppfylle dette formålet. For å nevne et eksempel, bruk av cookie for lagring av varer i handlekurven, kan være en funksjon som gjør at brukeren får en bedre opplevelse.

Samtidig ser man ofte at når man har lagret en vare på handlekurven sin på en nettside, så ser man reklamer om det samme/lignende produktet på samme nettside, og på andre nettsider man besøker gjennom på samme pc/telefon og samme nettleser. Faste informasjonsskapsler muliggjør derfor bruk av tredjepartsinformasjonsskapsler. Noe som taler for at individet selv må kunne bestemme om vedkommende ønsker bruk av dette eller ei.

Disse funksjonene er ikke avgjørende for ordinær fungering av en nettside. Som tidligere nevnt er disse funksjoner som forbedrer opplevelsen av brukerens besøk. Det faller derfor ikke under første kriteriet om at informasjonsskapselen brukes utelukkende for overføring av

¹⁴⁵ Cookie Information AS (2019), s.6

¹⁴⁶ For en liste over hvilke cookies er unntatt, se Den Europeiske Kommisjonen (2019)

¹⁴⁷ ibid

¹⁴⁸ Disse er informasjonsskapsler fører til at nettserveren får en lengre hukommelse av opplysninger som angis av nettbrukeren. De slettes ikke etter endt sesjon, men de fleste har en utløpsdato der de slettes automatisk etter en viss periode. Se NKOM (2019).

kommunikasjonen på nettsiden. Spørsmålet blir derfor om den «uttrykkelig» forespurte funksjonen er «strengtatt nødvendig» for å levere informasjonssamfunnstjenesten.¹⁴⁹

For eksempel, for at en person skal kunne kommentere på en side, er hun nødt til å logge seg inn. Plassering av sesjonsavhengige informasjonskapsler anses for å være strengtatt nødvendig for å gi henne denne mulighet. Det samme gjelder, hvor brukeren ønsker å unngå gjentakelse av loggingsdetaljer, slik at nettserveren blir nødt til å lagre en fast informasjonsskapsel på brukerens data som gir den langtidshukommelse.

Imidlertid, lagres disse i en mye lenger tid og kan utsette opplysningene for sikkerhetsmessige risiko¹⁵⁰ i større grad enn sesjonsavhengige cookies. Noe som tilsier at man burde selv gi samtykke til hvorvidt man er enig i dette eller ei, til tross for at dette er strengtatt nødvendig for utføring av den forespurte tjenesten. Dette beror på en tolkning av «informasjonssamfunnstjeneste», som er blitt foretatt ovenfor i punkt 3.3.11.

Informasjonssamfunnstjeneste anses som summen av flere funksjoner, innloggingsdetaljer, lagring av varene i handlekurven kan dermed anses som en del den. I fravær av andre bindende rettskilder, vil det legges vekt på denne anbefalingen. Dessuten har man også anledning til å blokkere slike informasjonskapsler på innstillingene i sin nettleser.

Det er forståelig at det er irriterende for brukere å måtte bli møtt med samtykke-bannere på hver nettside, men det er samtidig viktig å understreke viktigheten av beskyttelsen av deres personvern og minimering av risikoen for samling av opplysninger som egentlig ikke er å bli ansett som strengt nødvendig.

I tillegg tilsier de generelle prinsippene om beskyttelse av personvern, særlig prinsippet om proporsjonalitet og prinsippet om dataminimering, at der man kan unngå behandling av opplysninger burde man gjøre det.

I dette tilfelle, er det snakk om å innskrenke valget av individet om hvorvidt vedkommende vil gi fra seg disse opplysningene eller ei. Valgfriheten av individet under slike tilfeller hvor opplysningene utsettes for en sikkerhetsrisiko.

På den annen side, kan det argumenteres at lovgivningen forplikter alle nettsider til å forsikre brukeren om at deres opplysninger er i god behold, og har ansvaret for sikkerheten til opplysningene. Det vil dessuten være til deres egen ugunst hvis sikkerheten av systemene

¹⁴⁹ Se punkt 3.3.11 for mer om “strictly necessary” / «strengtatt nødvendig» kravet

¹⁵⁰ Slike informasjonskapsler kan brukes av uvedkommende for å få tilgang til kontoen eller at informasjonen om handlekurven og ellers brukerens oppførsel anvendes i markedsførings formål.

deres ikke er optimal. Et eksempel, er cyberangrepet som Hydro gikk gjennom i sommeren 2019. Angrepet kostet selskapet opptil 450 millioner kroner.¹⁵¹ Ved sikkerhetsbrudd kan også netteierne risikere å bli møtt med store gebyr, i tillegg til tar det ekstremt lang tid å restituere systemene som fører til reduksjon i produksjon og andre nødvendige funksjoner.

Det finnes imidlertid ingen garanti for at sikkerhetssystemene vil alltid fungere optimalt etter som teknologien er stadig under utvikling. Hver dag oppdages det nye måter å angripe nettsider på, slik at det til tross for høy sikkerhet foreligger det fremdeles noe risiko for at opplysningene skal komme til en ødeleggende angriper. Denne risikoen må være et valg som individet selv avgjør om vedkommende vil ta eller ei. Det konkluderes derfor med at faste informasjonskapsler ikke utgjør en «informasjonssamfunnstjeneste».

Vilkårene for unntak fra samtykkekravet er ikke oppfylt. Unntaket får ikke anvendelse. Bruk av funksjonelle informasjonskapsler krever dermed informert samtykke fra brukeren.

3.4.4. Statistisk cookies

Statistiske informasjonskapsler støtter ofte analyse av nettsidens besøk for å forstå brukernes bruk av nettstedet. Det er ofte tredjeparter som utfører dette for nettsideeieren. Disse kan også føre til forbedring av opplevelsen til brukeren, ettersom nettsideeieren kan bli klar over hvordan informasjonen på nettsiden blir oppfattet og om det er endringer som må foretas.

I praksis er Google analytics ofte brukt for denne hensikt. Det merkbare er at Google analytics brukes også for markedsføring,¹⁵² og det er derfor stor sannsynlighet for at opplysninger samlet for dette statistisk formål, også brukes til markedsføring.

Det er klart at disse cookies faller ikke under første kriteriet om utelukkende overføring av kommunikasjonen.

¹⁵¹ Hovland (2019)

¹⁵² Google (2019)

Spørsmålet blir om det oppfyller det andre alternativet kriteriet.

Statistiske cookies utfører ingen tjeneste for fungering av nettsiden eller funksjoner ellers. Det er tvilsomt hvorvidt vilkåret om at brukeren selv «uttrykkelig» har forespurt om «tjenesten» kan anses for å være oppfylt. På den annen side, kan de føre til bedre opplevelse av nettsiden ettersom feiler kan f.eks. rapporterte feil kan føre til forbedring og tilgjengeliggjøring av tjenesten i normal tilstand. Vilkåret kan dermed anses for å være oppfylt.

Problemstillingen er videre hvorvidt statistiske cookies utfører en «informasjonssamfunnstjeneste».

Statistiske informasjonkapsler som utsetter opplysningene for lite personvern rettslige risiko, og fører til bedre bruker opplevelse er foreslått som et nytt unntak i ekomdirektivet art. 5 (3) annet punktum. Forslag er gitt til lovgiveren gjennom en uttalelse om ekomdirektivet som arbeidsgruppen-art.29.¹⁵³ Det kan tale for at gruppen mener at disse er unntatt samtykkekravet. Det vil da ikke innebære endring av gjeldende retten, men kun nedfelles unntaket uttrykkelig i artikkelen for å avklare forvirringer.

På den annen side, kan det argumenteres at gruppen tolker bestemmelsen slik at statistiske cookies faller utenfor ordlyden av bestemmelsen, men ser nødvendigheten for at disse skal være fritatt samtykkekravet. Derfor foreslås det en rettsendring. Ettersom uttalelsen er tvilsomt på dette punktet, skal den ikke tillegges særlig vekt.

Det vises til drøftelsen om «informasjonssamfunnstjeneste» under funksjonelle cookies. De samme hensynene gjør seg gjeldende når for statistiske cookies. Det vises dermed til drøftelsen overfor og konkluderes med at statistiske cookies faller ikke under informasjonssamfunnstjeneste. Vilkåret er dermed ikke oppfylt.

Statistiske informasjonkapsler er ikke unntatt samtykkekravet. Nettsideeiere er forpliktet til å innhente informert samtykke for bruk av statistiske informasjonkapsler.

3.4.5. Markedsførende/targeting cookies

¹⁵³ Artikkel 29-gruppen A29WP, 16/EN WP240, 19.juli 2016, s. 10

Disse cookies tillater tredjeparter å profilere og sende tilpassede annonser til brukerne basert på opplysninger om hvilke sider de brukeren besøkte, innholdet på sidene og annet.¹⁵⁴ Disse kalles ofte for tredjepartsinformasjonskapsler.

Vilkårene for unntak fra samtykke er klart ikke oppfylt for denne kategorien av informasjonskapsler. Det er nettopp denne kategorien som er mest skadelig mot individets personvern, og til dels også grunnen til at det er behov for samtykke og beskyttelse av denne retten.

Det konkluderes derfor med at bruk av markedsførende informasjonskapsler krever innhentning av informert samtykke.

Oppsummeringsvis, kan det sies at det er kun nødvendige cookies som er unntatt fra samtykkekravet. I motsetning til de øvrige kategoriene av cookies utsetter ikke disse individene for personvernrettslige risiko og dessuten slettes umiddelbart. Til tross for at faste cookies fører til bedre brukeropplevelse, faller de ikke innenfor vilkårene for unntak av samtykke. Det samme gjelder statistiske og markedsførende cookies.

Gjelder dette også for andre type teknologier?

Ekomloven § 2-7b anvendes på alle former for lagring av opplysninger eller tilgang til slike i brukers terminalutstyr, selv om diskusjonen er veldig sentrert mot bruk av cookies. Dette følger av forarbeidene til bestemmelsen som nevner at bestemmelsen gjelder cookies og «liggende teknologier».

Uttalelsen fra arbeidsgruppen tilsier at både ekomdirektivets art. 5 nr.3 kommer til anvendelse for slike teknologier, men også GDPR i de tilfeller hvor det handler om behandling av personopplysninger.¹⁵⁵ Det samme gjentatt i en annen uttalelse som handlet øpesikk om sporingsteknologien fingerprinting.¹⁵⁶

Loven er proaktiv, og har ikke begrenset seg kun til cookies. I fortalen til ekomdirektivet nevnes det også skadeprogrammer og andre typer tjenester som kan plasseres til brukers terminal. Men dersom det er teknologier som sporer uten at skal «plasseres» i terminalutstyret til brukeren, finner vi oss utenfor bestemmelsens ordlyd.

¹⁵⁴ Cookie Information AS, (2019), s.6

¹⁵⁵ Artikkel 29-gruppen A29WP, 00909/10/EN WP171, 22.juni 2010 s. 3

¹⁵⁶ Artikkel 29-gruppen, 14/EN WP 22, 25. November 2014, s. 3

Imidlertid, er personopplysninger fremdeles regulert av personvernforordningen uansett om disse lagres i brukers terminal eller ei. Det fremgår av fortalene til personvernforordningen i punkt at profilering gjennom andre sporingsteknologier er forbudt. Dessuten må formålet for slik profilering være lovlig i henhold til GDPR art. 5. Det må i tillegg foreligge et lovlig grunnlag i henhold til art. 6, hvorav samtykke er et av alternativene. Dette er også i samsvar med veiledningen i personvernhandboken.¹⁵⁷

3.5. Rettsvirkning av brudd

NKOM har muligheten til å pålegge gebyr for overtredelser på samtykkereglene i henhold til ekoml. § 10-7 og § 10-13.

GDPR Art. 7 (2) siste setning sier at enhver del av samtykket som avviker vilkårene for samtykke i GDPR-fordningen, skal ikke være bindende. dvs, at dersom et av kravene som stilles til et gyldig samtykke ikke er tilstede, er rettsvirkningen at samtykke ikke er gyldig. Det fører til at de lagrede opplysningene må slettes umiddelbart. En naturlig følge av det er at de operasjonene som har funnet sted inntil mangelen ved samtykket ble oppdaget, anses for ulovlig behandling av opplysninger.

Som konsekvens av ugyldig innhentet samtykke eller ulovlig bruk av cookies kan Datatilsynet pålegge den dataansvarlige gebyr¹⁵⁸. Datasubjektet kan bli erkjent erstatning for materielle og ikke-materielle skader som følge av bruddet¹⁵⁹.

4. Avsluttende tanker

Rettsområdet er blitt en del klarere etter den nylige rettsutviklingen i EU. Nye retningsgivende uttalelser samt den første avgjørelsen etter GDPR-regler, har gitt svar på mange tvilsomme problemstillinger.

Imidlertid, er det fremdeles mange uavklarte spørsmål. Det er EU-domstolen som har ansvaret og retten til tolkning av GDPR. Eventuelle tvil kan kun fjernes gjennom bindende rettsavgjørelser fra denne domstolen.

I norsk rett gjenstår det fremdeles uklarheter om kravene til samtykke ved bruk av cookies. Datatilsynets retningslinjer er nå blitt oppdatert i samsvar med tolkningen av EU-domstolen.

¹⁵⁷ Tønseth ,(2016), 8.8.2

¹⁵⁸ GDPR art. 83 nr. 5 bokstav a

¹⁵⁹ GDPR art. 82 nr. 1

NKOM har derimot ikke endret sine retningslinjer, men de har publisert en erklæring på sine nettsider. Erklæringen informerer om at en presisering av lovverket i området, vil bli vurdert.

Det har størst praktisk betydning for hvorvidt samtykke gjennom nettleser innstillinger anses som et gyldig samtykke. Mange har forholdt seg til dette, og spørsmålet blir om det må gjøres noen forandringer fremover. Det beror på hvordan man anser forholdet mellom ekomloven, personopplysningsloven og personvernforordningen.

Det første alternativet er at lovgiver foretar denne vurderingen, og kommer med en presiserende bestemmelse om forholdet mellom lovene. Imidlertid, kan dette ta lang tid. Inntil da, vil norske internettbrukere gis en lavere beskyttelse enn det som de egentlig burde hatt etter EU/EØS-reglene.

Det andre alternativet er å løse problemet ved å tolke forarbeidene i ekomloven innskrenkende, slik at forholdene mellom personvernlovgivningene i Norge, blir likestilt med det som kreves av EØS-retten.

Det er store uenigheter om innholdet av reglene i forordningen. Det ble foreslått oppmyking av reglene for cookies i mai 2019.¹⁶⁰ EU-domstolen avsa imidlertid avgjørelse i oktober 2019 om at samtykke for cookies, må være i samsvar med kravene for samtykke i GDPR. Det er ingen tvil i at hensynet om strenge krav for å ivareta personvern er blitt meget viktige i EU, men samtidig må disse være implementerbare. Mange argumenterer derfor for oppmyking av reglene om samtykke til cookies, men det som burde egentlig være fokuset er nye tekniske løsninger som kan ivareta de strenge kravene som beskytter individet best. Forenkling av reglene derimot, kan være gunstig både for netteiere og brukere.

Mine refleksjoner har vært at det er gode grunner for at forslaget vil bli endret i samsvar med avgjørelsen som EU-domstolen har kommet med. NKOM har også nevnt det i sin erklæring. Dessuten ligger forslagene fremdeles i Europaparlamentet og Rådet. Det vil muligens ta flere år før en enighet vil foreligge, og til det vedtas og endelig inkorporeres i norsk rett.

Slik situasjonen er i dag, vil det derfor, etter min mening, være gunstig for nettsideeiere å finne løsninger for innhenting av samtykke i samsvar med reglene i personvernforordningen.

¹⁶⁰ Stortinget (2019)

Litteraturliste

EU- og EØS- rettslige kilder

Traktater

EU-Charteret	Charter of Fundamental Rights of the European Union, 18. Desember 2000, 2000/C 346/01. http://data.europa.eu/treaty/char_2012/oj
EØS-avtalen	Avtale om Det europeiske økonomiske samarbeidsområde, 2.mai 1992.
ODA-avtalen	Avtale mellom EFTA-statene om opprettelse av et overvåkningsorgan og en domstol, 2. mai 1992.
TEU	Traktaten om den Europeiske Union. Konsolidert utgave 2016 (EUT 2016/C 202/01).
TEUV	Traktaten om den Europæiske Unions funktionsmåte. Konsolideret utgave 2016 (EUT 2016/C 202/01).

Sekundærlovgivning

Dir 1995/46 EF	Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og fri utveksling av slike opplysninger [personverndirektivet].
----------------	--

Dir 2002/58 EC	Europaparlaments- og rådsdirektiv 2002/58/EC av 12.juni 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon [Ekomodirektivet].
Dir 2009/136 EC	Europaparlaments- og rådsdirektiv 2009/136 av 25.november 2009 om endring av direktiv 2002/22/EF og direktiv 2002/58/EF om behandling av personopplysninger og beskyttelse av privatlivets fred i den elektroniske kommunikasjonssektor [cookie-direktivet].
For 2016/679 EU (GDPR)	Europaparlaments- og rådsforordning (EU) 2016/670 av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF [generell personvernforordning].

Forarbeider

COM (2012) 11 final	Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25. januar 2012.
Sec (2012) 72 final	Commission staff working paper Impact assessment, 25. Januar 2012.

COM (2017) 10 final

Forslag til Europaparlaments- og rådsforordning om respektiv for privatliv og beskyttelse av personopplysninger i forbindelse med elektroniske kommunikasjon og om opphevelse av direktiv 2002/58/EF (forordning om databeskyttelse innenfor elektronisk kommunikasjon), [Ekomforordningen/kommunikasjonsvernforordning]

Rettspraksis

Sak C-40/17 Fasion ID v Verbraucherzentrale NRW ECLI:EU:C:2019:629.

Sak C-673/17 Planet 49 v Verbraucherzentrale Bundesverband e.V. ECLI:EU:C:2019:801

Sak C-621/18 Wightman v Others ECLI:EU:C:2018:99

Rådgivende uttalelser

Artikkel 29-gruppen A29WP
00737/EN WP148, 4. April 2008

Opinion 1/2008 on data protection issues
related to search engines

Artikkel 29-gruppen A29WP
00909/10/EN WP171, 22.juni 2010

Opinion 2/2010 on online behavioural
advertising

Artikkel 29-gruppen A29WP
01197/11/EN WP187 (2011)

Opinion 15/2011 on the definition of
consent, 13. juli 2011, A29WP 01197/11/EN
WP187

Artikkel 29-gruppen A29WP
00879/12/EN WP 194 (2012)

Opinion 04/2012 on cookie consent exemption, 7. Juni 2012, A29WP 00879/12/EN WP194

Artikkel 29-gruppen A29WP
14/EN WP 22, 25. November 2014

Opinion 09/2014 on the application of Directive 2002/58/EC to device fingerprinting

Artikkel 29-gruppen A29WP
16/EN WP240, 19.juli 2016

Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)

Artikkel 29-gruppen A29WP
17/EN WP260 (udatert)

Guidelines on transparency under Regulation 2016/679, udatert, A29WP 17/EN WP260. Artikkel 29-gruppen A29WP

Artikkel 29-gruppen A29WP
17/EN WP259 rev.01 (2018)

Article 29 Working Party Guidelines on consent under Regulation 2016/679, 28. November 2017, revidert 10. april 2018, A29WP 17/EN WP250 rev.01.

European Data Protection Board
Opinion 5/2019

Opinion 5/2019 on the interplay between the ePrivacy directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, 12. mars 2019.

Advokat Generalens rådgivende uttalelse
I Planet49

Sak 673/17, 21.mars 2019,
Planet49 v Verbraucherzentrale Bundesverband
ECLI:EU:C:2019:246

Norske rettskilder

Lover og forskrifter

Grunnloven (Grl.) 1814	Kongeriket Norges Grunnlov 18. Mai 1814 (Grunnloven).
Personregisterloven (pregl.) 1978	Lov 09. juni 1978 nr. 48 om personregistre (personregisterloven).
EØS-loven 1992	Lov 27.november 1992 nr.109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v (EØS-loven)
Menneskerettsloven (mrl.) 1999	Lov 21.mai 1999 nr. 30 om styring av menneskerettighetenes stilling i norsk rett (menneskerettsloven)
Personopplysningsloven (proppl.) 2000	Lov 14.mars 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven)
Ekomloven (e-koml.) 2003	Lov 4. juli 2003 nr.83 om elektronisk kommunikasjon (ekomloven)
Personopplysningsloven (2018)	Lov 15.juni 2018 nr.38 om behandling av personopplysninger (Personopplysningsloven)
Ekomforskriften (2004)	Forskrift 16. februar 2004 nr.83 om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften)
Ekomforskriften (2013)	Forskrift 20. juni 2013 nr. 54 om endring i forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjenesten (ekomforskriften)

Forarbeider

NOU 1997:19	Et bedre personvern – forslag til lov om behandling av personopplysninger.
Ot.Prp.nr.58 (2002-2003)	Om endring av ekomloven
Innst. 256 L (2012-2013)	Innstilling fra transport- og kommunikasjonsskomiteen om endringer i ekomloven, 16. april 2013.
Prop.69 L (2012-2013)	Endringer i ekomloven
Prop.56 LS (2017-2018)	Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generelle personvernforordningen) i EØS-avtalen.

Rettspraksis:

Rt.2000 s.1811, Finanger I,

Rt. 1997s.580 OFS,

Rt. 2015s.138

Litteratur

Bøker

- Arnesen (2015) Arnesen, Finn og Are Stenvik, «Internasjonalisering og juridisk metode», 2.utgave, Universitetsforlaget, 2015, ISBN:9788215023922
- Birmingham (2018) Birmingham, Karen. «*Informed consent: too much information*, The early development of the ALSPAC ethics and Law committee», Bristol University Press, 2018, ISBN 978-1-4473-4042-3.
- Bond (2012) Bond, Robert, «The EU e-privacy directive and consent to cookies», *The Business Lawyer*, Vol. 68 no.1 s.215-223, American Bar Association, <https://www.jstor.org/stable/23527086?seq=1> [sitter 27.08.19]
- Bygrave (2014) Bygrave, Lee A. «*Data Privacy Law, An international perspective*» Oxford University Press, 2014, ISBN:978-0-19-967555-5
- Dinnis (2012) Dinnis, Heather Harrison. «*Cyber warfare and the laws of war*», Cambridge University Press, 2012, ISBN: 978-1-107-01108-3
- Doyle (2016) Doyle, Charles. «*A dictionary of marketing*», 4th edition, Oxford University Press, 2016, ISBN:9780198737424
- Eckhoff (2001) Eckhoff, Torstein. «*Rettskildelære*», 5.utg., ved Jan Helgesen, Oslo: Universitetsforlag, 2001.
- Fredriksen (2018) Fredriksen, Halvard Haukeland og Gjermund Mathisen, «*EØS-rett*», 3.utg., Bergen: Fagbokforlaget, 2018.
- Gutwirth, Leenes, De Hert (2016) Gutwirth, Serge og Ronald Leenes og Paul De Hart, «*Data Protection on the move*», Brussels, 2016, ISBN: 978-94-017-7376-8.
- Jarbekk (2019) Jarbekk, Eva og andre. «*Personopplysningsloven og personvernforordningen (GDPR) med kommentarer*», 1.utg, Gyldendal, 2019 ISBN:9788205498273
- Kudyba (2014) Kudyba, Stephan og Thomas H. Davenport, «*Big data, mining and analytics, components of strategic decisions making*», Boca Raton, 2014, ISBN: 9781466568709

- Smith (2012) Smith, Eivind. «*Konstitusjonelt demokrati*», 2.utg, Oslo, 2012
- Sejersted (2011) Sejersted, Arnesen, Rogstad, Foyn, Kolstad, «*EØS-rett*», 3.utg, 2011, ISBN: 9788215017730
- Tønseth (2016) Tønseth, Malin, Marit Stubø, Thomas Olsen og Rune Ljostad. «*Personvernhandboken*», 1.utg, Gyldendal, 2016.
- Årnes (2018) Årnes, Andre, «Digital Forensics», Norwegian University of Technology and Science (NTNU), Norway and Telenor Group, Norway, 2018, ISBN:9781119262381

Nettartikler og nettsider

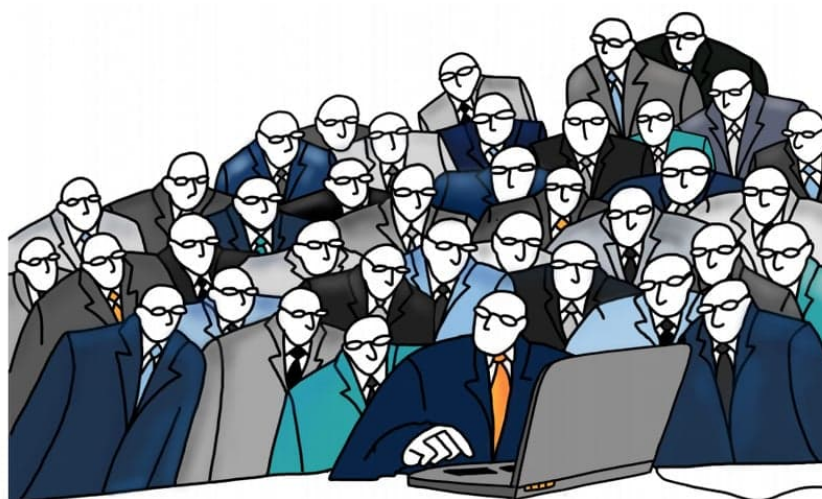
- Barth, (2011) Barth, A. «Http state management mechanism, RFC 6265», Internett Engineering Task Force (IETF), 2011, <https://tools.ietf.org/html/rfc6265> ISSN: 2070-1721
- Big Wave Media(udatert) Big Wave Media, « What is demographic data? », teknisk artikkel, <https://www.bigwavemedia.co.uk/blog/uses-of-demographic-data> [sitert 15.11.19]
- Cardinale (udatert) Cardinale, Corrine. « What is behavioral data and behavioral analytics?», Indicative, Inc, Teknisk artikkel, <https://www.indicative.com/blog/what-is-behavioral-data-and-behavioral-analytics/> [sitert 24.11.19]
- Cookie Information AS (2019) Studie av norske offentlige nettsteder, «Mottar tredjeparter informasjon om norske innbyggeres besøk på offentlige nettsteder?», publisert 1. April 2019, Cookie Information AS, rapporten er vedlagt i avhandlingen.
- Cucu, (2017) Cucu, Paul. «Session hijacking takes control of your accounts. Here's how», Heimdal Security, sist oppdatert 4. August 2017, <https://heimdalsecurity.com/blog/session-hijacking/#>, [sitert 24.11.19]

- Datatilsynet (2017) Rapport om «Big Data - personvernprinsipper under press», sist endret 06.06.17, Datatilsynet, <https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/big-data/>, [sitert 25.11.19]
- Datatilsynet (2019) Datatilsynet, retningslinjer, «Cookies og informasjonskapsler», publisert 20.06.2018, endret 10.10.2019, <https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/cookies/> [sitert 11.10.19]
- Den Europeiske Kom- Den Europeiske kommisjonens retningsgivende liste over hvilke misjonen (2019) informasjonskapsler er unntatt fra samtykkekravet, <https://wikis.ec.europa.eu/display/WEBGUIDE/04.+Cookies>, [sitert 11.10.19]
- Dibs (2019) Nets og Dibs, «Norsk e-handel i 2019», Rapport, https://info.dibs.no/norsk-ehandel-2019?utm_campaign=Norsk%20E-handel%202019&utm_source=Nettpilot.no [sitert 25.11.19]
- Difi (2015) Direktoratet for forvaltning og ikt, «bruksområdet gjelder protokoller for grunnleggende datakommunikasjon», publisert 23. november 2015, <https://www.difi.no/referanse katalogen/grunnleggende-datakommunikasjon> [sitert 09.09.19]
- Forbrukerrådet (2018) «Deceived by design», Forbrukerrådet, How tech companies use dark patterns to discourage us from exercising our rights to privacy, 27. Juni 2018, <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf> [sitert 25.11.19]
- Google (2019) Google, retningslinjer, 2019, <https://policies.google.com/privacy?fg=1> [sitert 25.11.19]
- Hovland (2019) Hovland, Kjetil Malkenes. «Cyberangrep har kostet Hydro opptil 450 millioner kroner», publisert 30.april 2019, <https://e24.no/boers-og-finans/i/7078VV/cyberangrep-har-kostet-hydro-opptil-450-millioner>, [sitert 25.11.19]

- Kaldestad (2018) Kaldestad, M, H. «Dette betyr de nye personvernreglene for deg», Forbrukerrådet, publisert 25. mai 2018, <https://www.forbrukerradet.no/siste-nytt/dette-betyr-de-nye-personvernreglene-for-deg/> [sisert 09.10.19]
- Kostic (2017) Kostic, Nojana and Emmanuel Vergas Penagos, «The freely given consent and the “bundling” provision under the GDPR», https://www.ivir.nl/publicaties/download/Computerrecht_2017_4.pdf [sisert 11.11.19]
- Kristol (2001) Kristol, David M. «Http cookies: Standards, Privacy, and politics», Bell Labs, Lucent Technologies, 9. Mai 2001, <https://arxiv.org/pdf/cs/0105018.pdf> [sisert 11.09.19]
- LaCroix, Loo, Choi (2017) LaCroix, Kenneth og Yin L. Loo og Young B. Choi, «Cookies and sessions: A study of what they are, how they work and how they can be stilen», International conference of software security and assurance (ICSSA), 25. Juni 2018, Institute of Electrical and electronics engineers, <https://ieeexplore.ieee.org/abstract/document/8392612>, ISBN:978-1-5386-4808-7 [sisert 08.10.19]
- Luzak (2014) Luzak, J.A. «Privacy notice for dummies? Towards European guidelines on How to give “clear and comprehensive information” on the cookies’ use in order to protect the internet users’ right to online privacy», <https://link-springer-com.ezproxy.uio.no/article/10.1007/s10603-014-9263-3> ISSN:0168-7034 [sisert 24.09.19].
- Milne og Culnan (2004) Milne, George og Mary J. Culnan. «Strategies for reducing online privacy risks: why consumers read(or don’t read) online privacy notices», Journal of interactive marketing, 18(3):15, 29. Juni 2004, https://www.researchgate.net/publication/227733192_Strategies_for_Reducing_Online_Privacy_Risks_Why_Consumers_Read_Or_Don't_Read_Online_Privacy_Notices [sisert 24.09.19]
- NKOM (2019) NKOM, Nasjonal Kommunikasjonsmyndighet, retningslinjer, «Cookies og informasjonskapsler», sist oppdatert 23.01.19 <https://www.nkom.no/teknisk/internett/cookies/informasjonskapsler-cookies> [sisert 10.11.19]

Publisert 1. april 2019 av Cookie Information AS

Mottar tredjeparter informasjon om norske innbyggers besøk på offentlige nettsteder?



Cookie Information AS
Nedre Storgate 37, 3015 Drammen
Telefon: 90592635
jma@cookieinformation.com

Sammendrag

Denne rapporten inneholder resultatet av en undersøkelse av om tredjeparter¹ mottar informasjon om norske innbyggers besøk på offentlige myndigheters nettsteder. Undersøkelsen ble utført i mars 2019, og inneholder 131 tilfeldig utvalgte norske offentlige nettsteder. Cookie Informations teknologi er benyttet til å identifisere og analysere hvilke cookies de offentlige nettstedene lagrer i innbyggernes nettleser, hvilke formål disse cookies har og hvilke tredjeparter som mottar informasjon om innbyggernes besøk ved å lese informasjonen i disse informasjonskapslene.

På 97% av de norske offentlige nettstedene mottar tredjeparter informasjon om innbyggernes besøk. Disse informasjonene bruker tredjepartene til profilering av innbyggerne og til målrettet markedsføring uten at innbyggerne forutgående har gitt samtykke til dette.

⁷ <https://www.cnil.fr/fr/cookies-traceurs-que-dit-ia-oi/>
⁸ <https://www.privacyshield.gov/welcome>

Konklusjon

Formålet med denne studien er å undersøke om tredjeparter mottar informasjon om innbyggernes besøk på norske offentlige nettsteder.

På 97% av de offentlige nettstedene kan innbyggere forvente at tredjeparter lagrer og leser personlig informasjon om deres besøk. Dette resulterer i profilering og målrettet markedsføring, uten at innbyggeren er blitt informert eller gitt eksplisitt samtykke til dette. Samlet sett er det sannsynlig at de offentlige nettstedene er være blant de største norske leverandørene av informasjon om innbyggerne til BigTech-selskapene. Disse benytter dette data-grunnlaget til kommersielle formål.

Vår vurdering:

Det er stor risiko for at 97% av de offentlige nettstedene ikke oppfyller kravene til gyldig samtykke, jfr. GDPR-nr. 32.

Offentlige nettsteder har ikke fulgt ekomlovens formuleringer i paragraf 2-7b om at det skal finnes en entydig og klar oversikt over hvilke informasjonskapsler som brukes på det aktuelle nettstedet. Denne oversikten skal inneholde informasjon om hvilken informasjon som behandles, formålet med behandlingen og hvem som behandler informasjonen, samt en oversikt over hvilke tredjepartstjenester som sporer brukernes besøk på nettstedet⁹. Nettstedene mangler i de aller fleste tilfeller også tilfredsstillende samtykkeløsninger.

NKOM angir i sin veiledning at cookieinnstillingene i brukerens nettleser er tilstrekkelig samtykke. Følgende elementer dokumenterer at dette ikke er korrekt eller hensiktsmessig:

- Samtykke via brukerens browser kan ikke dokumenteres i ettertid
- Cookies settes/tracking starter før brukeren får informasjon om hvilke cookies som benyttes
- Browserinnstillinger for cookies stopper ikke all deling av persondata
- Brukerne vil ha forskjellige cookiepreferanser på forskjellige nettsteder. Ingen er tjent med at brukerne setter globale innstillinger som stopper cookies på alle nettsteder.

Denne analysen gir en oversikt som viser at norske offentlige nettsteder er ute av kontroll både i forhold til gjeldende regelverk og i forhold til innbyggernes forventninger til at deres personlige informasjon ikke deles med tredjeparter. Mulige årsak til dette er at det ikke foreligger en utfyllende presisering av de lovkrav som gjelder, samt et fraværende kontrollapparat. Vår anbefaling er at det nedsettes et utvalg som gjennomgår problemstillingen og kommer med klare anbefalinger til løsninger som sikrer at de offentlig nettsteder implementerer løsninger som 1) informerer innbyggerne om informasjonskapsler, 2) innhenter gyldig samtykke, 3) sørge for at relevant data-behandling finner sted bare etter at samtykke er gitt, 4) gir en oversikt over varigheten av sporing og 5) gi innsikt i overføringer til usikre tredjeland.

⁹ <https://www.nikom.no/teknisk/internett/cookies/informasjonskapsler-cookies>

- Nyvold (2018) Nyvold, M. «Snart kan du selge eller donere bort de personlige dataene dine», Teknisk ukeblad, publisert 9. juni 2018, <https://www.tu.no/artikler/snart-kan-du-selge-eller-donere-de-personlige-dataene-dine/439467> [sitert 08.10.19]
- Stortinget (2019) Stortingets rapport om den kommende ekomforordningen, <https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/EU-EOS-informasjon/EU-EOS-nytt/2019/eueos-nytt---23.-mai/#eprivacy>, publisert 23. mai 2019, [sitert 09.11.19]
- Uzialko (2018) Uzialko, Adam. C. «*How businesses are collecting data*» *And what they are doing with it*, publisert 3. August 2018, teknisk artikkel, <https://www.businessnewsdaily.com/10625-businesses-collecting-data.html> [sitert 09.11.19]