Adgangen til å behandle opplysninger ved bruk av informasjonskapsler

Et spørsmål om hvordan tilbyder rettmessig kan behandle opplysninger ved bruk av informasjonskapsler.

Handelshøgskolen ved Universitet i Stavanger

Master i forretningsjus

Masteroppgave

15.06.2023

Kandidatnummer: 3220 **Forfatter:** Pia Berntzen **Antall ord:** 13 476

Universitetet i Stavanger

HANDELSHØGSKOLEN VED UIS

MASTEROPPGAVE

STUDIEPROGRAM: MFJMAS - Master i forretningsjus	OPPGAVEN ER SKREVET INNEN FØLGENDE SPESIALISERINGSRETNING: Personvern ER OPPGAVEN KONFIDENSIELL? Nei

TITTEL: Adgangen til å behandle opplysninger ved bruk av informasjonskapsler

ENGELSK TITTEL: The right to process information through the use of cookies

FORFATTER(E)		VEILEDER:
Kandidatnummer: 3220	Navn: Pia Berntzen	Milos Novovic

Innholdsfortegnelse

1 Innledning

1.1 Tema, problemstilling og aktualitet

Temaet for oppgaven er bruk av informasjonskapsler, herunder tilbyders grunnlag for å behandle opplysninger og krav til rettslig gyldig samtykke. Med «informasjonskapsel», ofte kalt en cookie, forstås en liten tekstfil som lastes ned og lagres på brukerens terminalutstyr når brukeren åpner en nettside.[1] En informasjonskapsel gir terminalutstyret, for eksempel en datamaskin, et nettbrett eller en mobiltelefon, en unik verdi som representerer informasjon om brukeren. Verdien setter tilbyder i stand til å gjenkjenne den enkelte bruker.[2] En informasjonskapsel kan for eksempel benyttes til å lagre en brukers innloggingsdetaljer, til å kartlegge og analysere brukerens elektroniske bevegelser, eller til å huske brukerens handlekurv i en nettbutikk.

Dagens samfunn blir stadig mer digitalisert. Fysisk kommunikasjon og oppslagsverk er blitt erstattet av digitale løsninger som nettaviser og egne nettsider for den konkrete virksomheten. I tillegg har en rekke nye sosiale medieaktører kommet på markedet, hvor utveksling av informasjon nå forgår gjennom digitale plattformer som Instagram, Snapchat, Facebook og Tiktok. Når en bruker er inne på en ny nettside, blir vedkommende ofte møtt med et informasjonskapselbanner. Informasjonskapselbanneret informerer den fysiske eller juridiske personen som bruker det elektroniske kommunikasjonsnettet, «bruker»[3], om at rettssubjektet som tilbyr tilgang til den aktuelle elektroniske kommunikasjonstjenesten, «tilbyder» [4], henter inn opplysninger om den konkrete brukeren til ett eller flere formål.

Informasjonskapslene som plasseres på brukerens terminalutstyr deles inn i to grupper. Førstepartsinformasjonskapsler settes av tilbyder på den aktuelle nettsiden brukeren er inne på, mens tredjepartsinformasjonskapsler er informasjonskapsler som plasseres av en annen tilbyder av elektronisk kommunikasjonstjeneste enn den tilbyderen som tilbyr tilgang til den aktuelle nettsiden brukeren besøker. Som et resultat av at en tilbyder, fra den enkelte nettside og på tvers av ulike plattformer, kan hente inn og lagre opplysninger om en bruker ved bruk av informasjonskapsler, settes tilbyder i stand til å spore vedkommendes adferd. Behandling basert på sporingsteknologi gjør det mulig å opprette profiler om brukerne, med et ofte påfølgende formål om å analysere og trekke konklusjoner basert på brukerens personlige

[1] Datatilsynet, «Cookies og informasjonskapsler»
[2] Information Commissioner`s Office (ICO), «Cookies and similar technologies»
[3] Jf. legaldefinisjon i Lov av 4.Juli 2003 nr.83 om elektronisk kommunikasjon (ekomloven) § 1-5 nr.14
[4] Jf. legaldefinisjon i ekomloven § 1-5 nr.16

preferanser, holdninger og interesser.[5] Kunnskap om personer danner grunnlaget for verdifulle data for næringsvirksomheter til å utvikle sin forretningsmodell og optimalisere bruken av den enkelte nettside eller applikasjon m.m.

Informasjonskapslene bidrar med å effektivisere og skape en mer brukervennlig utnyttelse av den elektroniske kommunikasjonstjenesten. Dette vil kunne være til fordel for brukeren selv, som mottar innhold tilpasset sine egne interesser. Det vil i enda større grad være til fordel for tilbyderen, i form av mulighet for økt omsetning og profitt.

Spesielt innenfor reklameindustrien har den digitale forretningsutviklingen bidratt til at bedrifter har kunnet skreddersy reklamer og annonser den enkelte bruker blir eksponert for.[6] Som følge av den teknologiske utviklingen og mulighetene til å håndtere og utnytte store mengder informasjon, kan den elektroniske forfølgningen informasjonskapslene forårsaker imidlertid virke invaderende. At opplysninger brukes til å danne profiler og sende spesialtilpasset reklame, kan føles overvåkende og inngripende i en brukers private sfære.

Frykten for at opplysninger om personlige forhold og preferanser gjøres tilgjengelig for allmennheten kan ytterligere legge begrensninger på brukeres utfoldelse og meningsutveksling, som er nødvendig for et velfungerende demokratisk samfunn.[7] Personvern utgjør en del av retten til respekt for sitt privatliv og er en grunnleggende menneskerettighet.[8] Som en del av personvernet inngår også retten til å kontrollere opplysninger om seg selv. På bakgrunn av dette er hovedregelen, både etter internasjonal og nasjonal rett, at behandling av opplysninger ved bruk av informasjonskapsler er forbudt.[9] I norsk lov er dette regulert i lov om elektronisk kommunikasjon (ekomloven) § 2-7 b.[10] Det følger av forarbeidene til ekomloven at hovedhensynet bak den norske bestemmelsen for bruk av informasjonskapsler nettopp er «å sikre brukerens personvern på ekomområdet».[11] Forarbeidene uttrykker videre at regelverket ikke skal vanskeliggjøre lovlig bruk av informasjonskapsler for å fremme

[5] Se Europaparlaments-og rådsforordning (EU) 2016/678 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) [PVF, GDPR] fortalepunkt 24
[6] Store norske leksikon, «reklame», av Birger M. Vikøren, Roger Phil og Even Ruud, 12.01.2023. https://snl.no/reklame ; Datatilsynet, «Sporing i det offentlige rom»
[7] Datatilsynet, «Hva er personvern?»
[8] Lov av 17.Mai 1814 Kongeriket Norges Grunnlov (Grl.) § 102; Convention for the Protection of Human Rights and Fundamental Freedoms, Roma, 4. November 1950. (Den europeiske menneskerettighetskonvensjonen, EMK) Artikkel 8
[9] Ekomloven § 2-7 b; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, ePrivacy-direktivet) Art. 5 (3)
[10] Lov av 04.juli 2003 nr.83 om elektronisk kommunikasjon (ekomloven)
[11] Prop.69 L (2012-2013) s.102

innovasjon og stimulere til næringsutvikling. Det må således foretas en interesseavveining mellom hvor langt lovgiver og myndighetene skal gå i å beskytte brukerens rett på vern, eller å fremme økonomisk vekst og utvikling for virksomheter.

Etter dagens rettskildebilde, etableres det strenge krav for hvordan en tilbyder lovlig kan behandle opplysninger om juridiske og fysiske personer ved bruk av informasjonskapsler. *De lege lata*, er eneste lovlige behandlingsgrunnlag for bruk av informasjonskapsler, å hente inn et frivillig og informert samtykke. Dette har resultert i at brukere utsettes for såkalte samtykkestrømmer. Hver gang en bruker går inn på en ny nettside, dukker det opp et informasjonskapselbanner som ber om samtykke. Dette betyr at brukeren må ta stilling til om vedkommende aksepterer at den enkelte nettside behandler opplysninger om seg eller ikke. Imidlertid kan informasjonskapselbanneret oppleves mer som et forstyrrende element som hindrer tilgang til den egentlige informasjonen brukeren ønsker. For brukere er det utmattende å stadig måtte sette seg teknisk og informasjonsmessig inn i informasjonskapslenes omfang. Samtykkeforespørslene medfører samtykketrøtthet, som igjen øker sannsynligheten for at bruker godtar å bli sporet uten egentlig å tenke over hvilke konsekvenser dette får. Dette problematiserer igjen lovligheten av behandlingsaktiviteten for tilbyder, ettersom tilbyder ikke kan vite hvor informert eller frivillig det avgitte samtykke fra brukeren er.

For at vilkåret om et rettslig gyldig samtykke skal anses oppfylt, stilles det en rekke krav knyttet til den tekniske, innholdsmessige og visuelle utformingen av en informasjonskapsel. Kravene har bidratt til vanskeligheter med å tolke regelverket, og setter en høy terskel for når en tilbyder lovlig kan samle inn og lagre opplysninger ved bruk av en informasjonskapsel. Utfordringene ligger blant annet i adgangen til å kunne avslå at en informasjonskapsel plasseres, muligheten for å tilbakekalle et samtykke, at samtykke er gitt eksplisitt, at design, fargeknapper og kontraster ikke er utilbørlig manipulerende, samt adgangen til å viderebehandle opplysningene.

På bakgrunn av stadig nye teknologiske utviklinger, tilveksten av tilbydere og nye markedsføringsmodeller, er ikke lenger dagens regelverk ansett å være tilstrekkelig for å ivareta personvernet til den enkelte bruker. Manglende harmonisering på tvers av medlemsland i EU og EØS har bidratt til et usikkert regelverk. Uklarhetene gjør det vanskelig for næringsvirksomheter å drive sin forretning i samsvar med loven og dermed vite hvordan de gyldig kan behandle opplysninger.

For å imøtekomme samfunnsendringene er det, både etter norsk rett og på EU-rettslig nivå, satt i gang en moderniseringsprosess. I Norge ligger forslag til ny lov om elektronisk kommunikasjon (ekomloven) på høring. Samtidig er det fremmet forslag om ny kommunikasjonsvernforordning i EU.

Formålet med masteroppgaven er å belyse utfordringene som reises ved gjeldende og foreslått regulering av behandling av opplysninger ved bruk av informasjonskapsler. Problemstillingen er hvordan tilbyder rettmessig kan behandle opplysninger ved bruk av informasjonskapsler. Oppgaven vil foreta en rettsdogmatisk analyse på bakgrunn av den norske ekomloven, ePrivacy-direktivet og fremmet forslag til ny kommunikasjonsvernforordning.

1.2 Metode, rettskilder og avgrensninger

Masteroppgaven tar utgangspunkt i direktiv 2002/58/EC (ePrivacy-direktivet), da medlemsland i EU og EØS baserer seg på denne ved utformingen av sitt nasjonale regelverk. Ettersom lovligheten av å behandle opplysninger om brukere ved bruk av informasjonskapsler ikke er et rent nasjonalt anliggende, vil det være sentralt å se på rettskilder utenfor norsk rett. Imidlertid er rettskildebildet knapt og det eksisterer få rettskilder som klarlegger oppgavens tema og problemstilling. Området for elektronisk kommunikasjon er komplekst og under stadig utvikling. Bruken av informasjonskapsler berører flere fagfelt, slik at også andre informasjonskilder benyttes for å trekke rettslige slutninger. De sentrale rettskildene og informasjonskildene, samt deres rettslige betydning, vil bli gjennomgått fortløpende i oppgaven.

Det vil i oppgaven være sentralt å se på hvordan tilsynsmyndigheter i andre land enn Norge gjennomfører direktiv 2002/58/EC for å få til en komparativ analyse, herunder se på avgjørelser truffet av det irske og det franske Datatilsynet. Ytterligere vil avgjørelser fra EU-domstolen, samt veiledning fra EUs personvernråd underlegges en rettslig analyse.

I forhold til personvernforordningen, vil oppgaven kort belyse dens forhold til ePrivacy-direktivet og kommunikasjonsvernforordningen. Dette fordi reguleringen av elektroniske kommunikasjonstjenester på ekomområdet anses som spesiell rett sammenlignet med den generelle personvernforordningen.

Etter norsk rett reguleres bruk av informasjonskapsler av ekomloven § 2-7 b. Bestemmelsen er flyttet fra ekomforskriften og innebærer en skjerpelse av samtykkekravet.[12] Ved forslag til ny ekomlov er reguleringen av informasjonskapsler nedfelt i § 3-7. Bestemmelsen vil presisere og i hovedsak være en videreføring av gjeldende § 2-7 b. Ny ekomlov § 3-7 vil basere seg på, og gjennomføre, direktiv 2002/58/EC artikkel 5 (3).[13] At Stortinget, som lovgivende makt i Norge,[14] vedtar ny ekomlov, til tross for å kjenne til arbeidet med ny kommunikasjonsvernforordning, og som Kommunal- og distriktsdepartementet konkluderer med å være EØS-relevant,[15] gir klare indikasjoner på det akutte behovet for endring av regelverket på området for elektronisk kommunikasjon. På bakgrunn av de EU-relevante rettskildenes påvirkning på norsk rett, avgrenses masteroppgaven mot inngående fremstilling av den norske reguleringen for bruk av informasjonskapsler. Norsk rett vil likevel bli belyst for å sammenligne og klargjøre rettstilstanden der dette er hensiktsmessig.

Oppgavens tema aktualiserer også en tilbyders adgang til å fravike kravet til samtykke etter unntakene 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[16]

Problemstillingene knyttet til disse nevnte unntakene vil ikke redegjøres for innenfor masteroppgavens omfang. Oppgaven vil videre avgrense mot andre sporingsteknologier enn informasjonskapsler, likevel slik at enkelte mekanismer nevnes for illustrasjonens del.

Etter norsk rett er det Nasjonal Kommunikasjonsmyndighet (Nkom) som forvalter ekomloven og har ansvaret for å kontrollere og føre tilsyn med tilbyderne av elektroniske kommunikasjonstjenester.[17] Dette i motsetning til Datatilsynet, som skal føre tilsyn med at behandling av personopplysninger skjer i tråd med personvernforordningen.[18] Selv om noen av uklarhetene rundt hvordan en tilbyder innhenter et rettslig gyldig samtykke delvis har bakgrunn i usikkerheten rundt grensene for forvaltningsmyndighetene og forholdet mellom

[12] Prop.69 L (2012-2013) s.9 og 42
[13] Regjeringen, «Høring-Forslag til ny ekomlov, ny ekomforskrift og endringer i nummerforskriften»
[14] Grl. § 49
[15] Regjeringen, «Forslag til kommunikasjonsvernforordning»
[16] Ekomloven § 2-7 b
[17] Regjeringen, «Nasjonal kommunikasjonsmyndighet/Nasjonal kommunikasjonsmyndigheit (Nkom)»
[18] Regjeringen, «Datatilsynet»

personvernforordningen og ekomsektoren, faller det utenfor oppgavens kjerne og vil ikke bli belyst videre.

Et annet uklart rettslig forhold, er anvendelsesområdet til GDPR for juridiske personer. Det følger eksplisitt av fortalepunkt 1 i fremmet forslag til kommunikasjonsvernforordning, at forordningen vil gjelde både for rettslige og fysiske personer.[19] I henhold til fortalepunkt 3 skal «where necessary, provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council, also apply mutatis mutandis to end-users who are legal persons».[20] Kommunikasjonsvernforordningen anerkjenner altså at også rettslige subjekter har krav på, og behov for, rettssikkerhet for opplysninger om dem. Kommunikasjonsvernforordningen viser særlig til behovet for å beskytte bedriftshemmeligheter. Til tross for at fortalens rettskildemessige vekt kan diskuteres, gir den en anvisning på formålet med rettsakten. Den rettslige konsekvensen er at fortalen er EØS-relevant «i den utstrekning det er nødvendig for en riktig fortolkning».[21] Innlemmelsen av juridiske personer i fortalen påpeker viktigheten av bedrifters mulighet til å forutberegne sin rettsstilling. Dette er meget viktig og sentralt for samfunnsutviklingen. Et samfunn er fundamentalt avhengig av at bedrifter er villig til å ta risikoer og sjanser for å fremme innovasjon og økonomisk utvikling, som igjen bidrar til samfunnsvekst.

Imidlertid, lagt til grunn at personvernforordning kun gjelder for fysiske personer, kan det stilles spørsmål ved hvor grensen går for hvilke bestemmelser som også skal få anvendelse for juridiske personer. At personvernforordningen får utvidet anvendelsesområde, hvor det er nødvendig, indikerer en høy terskel. Ordlyden åpner for en rettslig standard, hvor det må foretas en konkret skjønnsmessig vurdering. Å gå i dybden på dette ligger imidlertid utenfor denne oppgaven.

Oppgaven baseres delvis på analyse av foreliggende forslag til rettsakter. Det foretas derfor en avgrensning mot rettslige kilder som offentliggjøres etter 30.mai 2023, da masteroppgaven redegjør for det gjeldende rettskildebilde. Endringer i endelig vedtatte rettsakter kan endre rettstilstanden.

[19] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communication) av 21.feb 2021 (kommunikasjonsvernforordningen)
[20] Kommunikasjonsvernforordningen av 21.feb 2021
[21] EØS-avtalen av 2.mai 1992 nr.1 Protokoll 1 om gjennomgående tilpasning punkt 1; Fredriksen mfl., *EØS-rett,* s.338-339

1.3 Fremstillingen videre

I kapittel 2 vil det innledningsvis redegjøres for gjeldende rett og forholdet mellom norsk og europeisk rett, for videre å belyse syv typetilfeller som problematiserer et rettslig gyldig samtykke. Det vil i punkt 2.4 foretas en rettslig vurdering av samtykkekravets egnethet som behandlingsgrunnlag.

Kapittel 3 vil se på hvordan reguleringen av adgangen til å behandle opplysninger ved bruk av informasjonskapsler blir, på bakgrunn av et fremmet forslag til ny kommunikasjonsvernforordning. Det vil først foretas en generell redegjørelse av lovgivningsprosessen til kommunikasjonsvernforordningen og se på hvordan kommunikasjonsvernforordningen vil stå seg i forhold personvernforordningen. Videre det i punkt 3.3 gås mer i dybden på kommunikasjonsvernforordningens artikkel 8, som åpner opp for at tilbyder, i tillegg til samtykke, kan behandle opplysninger på alternative rettslige grunnlag. Punkt 3.4 vil avslutningsvis se på innvirkningene av kommunikasjonsvernforordningens ikrafttredelse.

Del 4 består av avsluttende bemerkninger knyttet til hvordan regelverket regulerer tilbyders rettmessige adgang til å behandle opplysninger ved bruk av informasjonskapsler.

2 Rettslig gyldig samtykke

2.1 Introduksjon

Norge har en dualistisk tilnærming til implementeringen av folkerettslige forpliktelser for at de skal gjelde som norsk rett.[22] Som følge av at folkeretten og norsk rett anses som to separate systemer, innebærer dette at rettsakter inntatt i EØS-avtalen særskilt må gjennomføres for å gjelde som norsk lov eller forskrift. Dette er også bekreftet i rettspraksis.[23] I norsk rett skilles det mellom inkorporasjon, hvor norsk lov eller forskrift direkte viser til og uttrykker at rettsakten gjelder som norsk rett, eller gjennom transformasjon, hvor rettsaktene omskrives og gjengis.[24]

I norsk rett gjelder det et alminnelig presumsjonsprinsipp. Prinsippet innebærer at norsk rett presumeres å være i samsvar med Norges folkerettslige forpliktelser, herunder EØS-avtalen. EØS-avtalen regnes å være den største, mest kompliserte og rettslig sett mest inngripende folkerettslige avtalen Norge har inngått. Reguleringen for bruk av informasjonskapsler faller inn under avtalens vedlegg XI. om elektronisk kommunikasjon og er således en sekundærrett av EØS-avtalen.[25]

Historisk stammer reguleringen av informasjonskapsler fra det europeiske ePrivacy-direktivet (ePD).[26] Den såkalte Cookie-bestemmelsen er nedfelt i ePD Artikkel 5 (3) og lyder;

> «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.»

[22] Fredriksen mfl., *EØS-rett*, s.390-391
[23] Se Rt.2000 s.1811 P (Finanger I)
[24] Fredriksen mfl. *EØS-rett*. s.391
[25] Fredriksen mfl. *EØS-rett,* s.47-49
[26] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, ePrivacy-direktivet)

Til forskjell fra forordninger, står nasjonale medlemsstater, herunder Norge, mer fritt til å bestemme form og midler for gjennomføring av et direktiv. Dette forutsetter at formålet med direktivet er oppfylt.[27] Transformasjon utgjør dermed en mindre inngripende akt i norsk suverenitet enn forordninger som har direkte bindende virkning i medlemsstatene. På den ene siden gis det rom for stater til å tilpasse reguleringen til sin nasjonale særegenhet. På den andre siden skaper nasjonale tilpasninger forskjeller, som svekker en konsistent tolkning av samtykkekravet til informasjonskapsler. Dette bidrar til at samme bestemmelse kan gis ulike rettsvirkninger i de forskjellige medlemsstatene. En naturlig konsekvens av redusert harmonisering av regelverket, er at det skapes usikkerhet rundt hvilke rettigheter og plikter som faktisk gjelder.

Et eksempel på hvordan nasjonal gjennomføring av cookie-bestemmelsen i ePD medfører ulikt omfang av rettigheter og plikter mellom medlemsstatene, er det franske Datatilsynets (CNIL) bøteleggelse av Google[28] og Facebook[29]. CNIL la til grunn at selskapene ikke ga tilstrekkelig informasjon ved innhenting av samtykke. Ytterligere var den omstendighet at det var vanskeligere for en bruker å trekke tilbake sitt samtykke enn det var for en bruker å akseptere en informasjonskapsel, krenkende sett i forhold til kravet om frivillig avgitt samtykke. Innhenting av samtykke som behandlingsgrunnlag var dermed i strid med Artikkel 82 av the French Data Protection Act, som gjennomfører ePrivacy-direktivet Artikkel 5 (3).[30] Google ble ilagt en bot på 150 millioner euro, mens Facebook ble ilagt en bot på 60 millioner euro.

Motsetningsvis anfører det norske Datatilsynet at «de to selskapene i disse sakene neppe [ville] vært i strid med det norske cookie-regelverket».[31] Datatilsynet begrunner påstanden i uttalelser i ekomlovens forarbeider, som legger til grunn at «også forhåndsinnstilling i nettleser om at brukeren aksepterer informasjonskapsler/cookies anses å utgjøre et samtykke [...]».[32] På bakgrunn av dette hevder Datatilsynet at «internettbrukere i Norge [har i dag] dårligere vern mot sporing på nett enn internettbrukere i EU».[33] Uttalelsene ble gitt i

[27] Lov av 27.november 1992 nr.109 om gjennomføring i norsk rett av hoveddel i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven) Artikkel 7 bokstav b); direktiv bindende for «tilsigtede mål», jf. Treaty on the Functioning of the European Union (TEUV), OJ C 202. (Romatraktaten) Artikkel 288 (3)
[28] SAN-2021-023
[29] SAN-2021-024
[30] SAN-2021-023 Avs.63
[31] Datatilsynet, «Datatilsynet sender brev til statsråden om cookie-regelverket»
[32] Prop.69 L (2012-2013) s.102
[33] Datatilsynet, «Vedrørende forslag til ny ekomlov § 3-7 – Bruk av informasjonskapsler mv.»

forbindelse med høring angående forslag til ny ekomlov § 3-7 for bruk av informasjonskapsler.

2.2 Typetilfeller som problematiserer et rettslig gyldig samtykke

Det sentrale, både i EU-retten og norsk rett, er behovet for å oppklare hva som faktisk ligger i et gyldig innhentet samtykke som behandlingsgrunnlag for bruk av informasjonskapsler. Som det fremkommer av både ekomloven § 2-7 b og ePD artikkel 5 (3), oppstilles det en rekke krav knyttet til vilkårene om et informert og frivillig samtykke. Selv om cookie-bestemmelsen uttrykker selvstendige vilkår, vil de gli over i hverandre og må leses som sådan.

Sett fra et EU-rettslig perspektiv, har uklarhetene medført at EUs personvernråd (EDPB)[34] har opprettet en «taskforce on cookie banners» (arbeidsgruppen). Hensikten med arbeidsgruppen er å styrke og sikre en harmonisert anvendelse av personvernreglementet.[35]

Arbeidsgruppen, bestående av en rekke (18) datatilsynsmyndigheter fra medlemsstatene, er satt sammen etter flere klager mottatt fra NOYB, en ideell organisasjon fra Østerrike.[36] Arbeidsgruppen kom frem til en rapport som drøfter gjeldende praksis og kommer med veiledning for minstestandarden til hvordan medlemsstatene konsistent bør tolke kravene til samtykke for bruk av informasjonskapsler ved syv typetilfeller.[37] Rapporten er således ikke en rettslig bindende rettsakt og er dermed av mindre rettskildemessig verdi. Imidlertid bidrar rapporten til oppklaringer og en bevisstgjøring om hvordan sakkyndige oppfatter og skal oppfatte regelverket. Kommisjonens uttalelser har således «betydning for praktiseringen av den EØS-relevante EU-retten».[38] Veiledningen gjør det vanskeligere for tilbydere som benytter seg av informasjonskapsler på sin nettside, å kunne hevde at reglene for sporing ved bruk av samtykke er uklare. De forsøksvise avklaringene fra personvernrådet kan bidra til å forebygge muligheten for omgåelse. Det er likevel viktig å huske at det er nasjonal lovgivning, hvor folket utøver den lovgivende makten ved Stortinget, som utgjør det rettslige rammeverket og hvor norske statsborgere utleder sine rettigheter og plikter fra.[39]

[34] The European Data Protection Board (EDPB)
[35] European Data Protection Board (EDPB), «letters»
[36] My Privacy is None of Your Business, jf. noyb, «Our Detailed Concept»
[37] EDPB, Report of the work undertaken by the Cookie Banner Taskforce Adopted on 17 January 2023
[38] Fredriksen mfl. *EØS-rett*, s. 52
[39] Jf. Folkesuverenitetsprinsippet nedfelt i Grl. § 49

2.2.1 Adgangen til å avvise behandling på første nivå

Første typetilfelle arbeidsgruppen tar for seg, er «No reject button on the first layer».[40] Flertallet av datamyndighetene var enige om at fraværet av et «avslå alle»-alternativ, på lik linje og nivå som å «godta alle», utgjør en krenkelse av ePrivacy-direktivet artikkel 5 (3).

Når samtykke innhentes på første nivå, gjennom et informasjonskapselbanner, må samtykke kunne nektes på første nivå. Med første nivå forstås det informasjonskapselbanneret som dukker opp med en gang en bruker går inn på en nettside. Dersom en bruker må trykke videre inn på nettsiden, uavhengig av om nettsiden viser tilgangen til å avslå gjennom link på cookiebanneret,[41] eller om bruker må lete på nettsiden for å finne avvisningsadgangen, er dette en rettsstridig utforming av samtykkeerklæringen. Slik manipulerende utforming krenker et gyldig innhentet samtykke. Dette betyr at bruker av en nettside, like lett som å godta en informasjonskapsel, skal kunne nekte at en informasjonskapsel blir satt. Kun da anses samtykke å være frivillig avgitt.

Presiseringen fra arbeidsgruppen er et skritt mot å sile ut virksomheters adgang til å lage tungvinte løsninger og mange trykk unna for å kunne avvise en informasjonskapsel. Denne formen for å utelukke villedende design og unødvendige hindringer forebygger såkalt samtykketrøtthet. Situasjonen karakteriseres ved at en bruker godkjenner plassering av en informasjonskapsel fordi vedkommende ikke tar seg tid til å gå gjennom mange steg for å kunne avvise. Bruker velger å ta den lette veien og aksepterer. En slik manipulerende måte å styre en brukers beslutningstaking på, er ikke i tråd med kravene til et rettslig gyldig samtykke og utgjør en krenkelse av regelverket.

Adgangen til å avvise behandling på første nivå må sees i sammenheng med informasjonskravet. Et rettslig gyldig samtykke forutsetter at bruker har samtykket på bakgrunn av en lett tilgjengelig, forståelig og tilstrekkelig informasjon til at brukeren, på det nivået, kan gjøre seg opp en oppfatning om å gi eller avslå sitt samtykke. At bruker ikke skal måtte trenge å oppsøke informasjonen selv, har også en side mot prinsippet om åpenhet.[42]

[40] EDPB, Cookie Banner Taskforce, s.4-5
[41] Se punkt 2.3
[42] Jf. Europaparlaments- og rådsfordning (EU) 2016/679 av 27.April 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt oppheving av direktiv 95/46/EF (GDPR) Art.5 nr.1 bokstav a); jf. Treaty on European Union (TEU), OJ C 202. (EU-traktaten) Art.1 (2) og Art.11 (2)

Rapportens veiledning etablerer dermed en streng linje for tilbyderes adgang til gyldig å behandle opplysninger på bakgrunn av samtykke.

2.2.2 Forhåndsavkryssede bokser

Et annet typetilfelle baserer seg på «Pre-ticked boxes».[43] Arbeidsgruppen bekrefter at forhåndsavskryssede bokser, såkalt «opt out»- løsning, ikke utgjør et gyldig innhentet samtykke, verken etter personvernforordningen (GDPR) eller ePrivacy-direktivet. Uttalelsen er kommet i ettertid av at EU-domstolen har avsagt to dommer der dette ble bekreftet.[44]

I sak C-673/17, tok domstolen stilling til om nettselskapet Planet49 sin innhenting av samtykke fra deltakerne i et salgsfremmende lotteri var i tråd med ePD artikkel 2 f) og artikkel 5 (3).[45] Samtykket gjaldt overføring av deltakernes personopplysninger til selskapets sponsorer og partnere, samt tilgang og lagring av informasjon i terminalutstyret til deltakerne. Domstolen foretok en ordlydstolkning av «user´s consent may be given by any appropriate method enabling a freely given specific and informed indication of the user´s wishes» og uttrykker at det må foreligge en utvetydig, aktiv handling fra brukeren. Det er dermed ikke lovlig behandling i de tilfeller hvor brukeren må velge bort at opplysninger blir behandlet.[46] Samtykke er derfor noe tilbyder av elektronisk kommunikasjon må innhente før en informasjonskapsel plasseres. Kravet til at bruker eksplisitt må krysse av en boks beskriver en «opt in» - løsning.

EU-domstolen fastsetter ytterligere i Planet49-saken at kravet til aktivt samtykke etter ePD gjelder uavhengig av om informasjonen innhentet og/eller lagret om en bruker utgjør en personopplysning eller ikke. Det følger av ePD fortalepunkt 24 at enhver informasjon lagret i terminalutstyret til brukere av elektronisk kommunikasjonsutstyr er en del av den private sfære og faller dermed inn under EMK artikkel 8 (retten til privatliv).[47] Det overordnede formålet og bakenforliggende hensynet med reguleringen av kommunikasjonsvernsektoren,

[43] EDPB, Cookie Banner Tasckforce, s.5
[44] Sak C-673/17 og C-61/19; EU-domstolener den europeiske unions dømmende makt, og har til formål å kontrollere at medlemsstatene overholder EU-lovgivningen, herunder sikre at EU-lovgivningen tolkes og anvendes likt, jf. European Union, «Court of Justice of the European Union (CJEU)»
[45] Dom av 1. oktober 2019 [GC], *Planet49*, C-673/17, ECLI:EU:C:2019:801
[46] Direktiv 2002/58/EC fortalepunkt 17; Planet49 avs.49-52
[47] Vern av elektronisk kommunikasjon og data er en del av retten til respekt for sitt privatliv og faller inn under det vide begrepet «korrespondanse» i EMK artikkel 8.1; Prop.69 L (2012-2013) s.27

ligger nettopp i å beskytte brukere fra den risikoen at skjulte identifikatorer og andre innretninger kan få tilgang til opplysninger uten at brukeren har kontroll.[48]

I C-61/19 gjaldt saken spørsmålet om Orange Romania, leverandør av mobile telekommunikasjonstjenester, gyldig hadde innhentet samtykke for innsamling og oppbevaring av kopier av identitetsdokumenter. EU-domstolen henviser tilbake til Planet49-dommen og fastsetter at det er behandlingsansvarlig som er ansvarlig for å påvise at kunden gjennom aktiv handling frivillig gir sitt informerte samtykke. Samtykkeerklæringen skal baseres på en lett og tilgjengelig informasjon, som ved bruk av klart og tydelig språk har satt brukeren i stand til å forstå konsekvensene av et samtykke. Domstolen la vekt på flere forhold som samlet sett medførte at Orange Romania ikke ble ansett for å ha hentet inn et rettslig gyldig samtykke. Selskapet hadde blant annet lagt inn en på forhånd avkrysset klausul før kundene signerte. Videre ble vilkårene i kontrakten ansett for å være i stand til å villede brukeren til å tro at vedkommende måtte samtykke til at opplysninger om seg ble behandlet for å kunne inngå den aktuelle kontrakten. Ytterligere var den omstendighet at brukeren måtte fylle ut et tilleggsskjema for å kunne nekte samtykke ansett som en urimelig påvirkning. Orange Romania hadde dermed hentet inn ett rettsstridig samtykke.[49]

Avgjørelsene viser at det ikke er tilstrekkelig at tilbyder henter inn et samtykke gjennom en stilltiende, forhåndsavkrysset boks eller annen inaktivitet. Til tross for at EU-domstolens dommer ikke er direkte bindende for Norge (og andre EFTA-land), følger det av homogenitetsprinsippet at EU-domstolens praksis er relevante og tungtveiende momenter ved tolkningsspørsmål knyttet til EØS-avtalen.[50] EU-domstolens avgjørelser har dermed i praksis stor betydning for norsk rett. At et samtykke må gis før en informasjonskapsel plasseres på brukerens terminalutstyr kan i tillegg utledes av ekomloven § 2-7 b. Bestemmelsen uttrykker at behandling av opplysninger som utgangspunkt er forbudt og at slik behandling kun unntaksvis er lovlig.

Til tross for et klart krav til aktiv handling, viser en undersøkelse, foretatt av CookieInformation februar 2023, at 89% av de skannede nettsidene som benyttet informasjonskapsler plasserte informasjonskapselen før samtykke var innhentet.

[48] Direktiv 2002/58/EC fortalepunkt 24; Planet49 avs.70
[49] Dom av 11. November 2020 [SC], *Orange Romania,* C-61/19, ECLI:EU:C:2020:901
[50] EØS-avtalen artikkel 6; Avtale av 2. Mai 1992 nr.2 mellom EFTA-statene om opprettelse av et overvåkningsorgan og en domstol, med protokollene 1 – 7 (ODA) Artikkel 3

Undersøkelsen tok utgangspunkt i topp 557 nettsider i Norge, som totalt viste at kun 8% av nettsidene var i samsvar med regelverket for bruk av informasjonskapsler.[51]

At et rettslig gyldig samtykke forutsetter en aktiv handling, er fulgt opp i forslag til ny ekomlov § 3-7 og merknadene til ny ekomlov § 3-7. Bestemmelsen vil i første punktum presisere at bruker må ha «gitt sitt samtykke»,[52] hvor merknadene til forslaget eksplisitt fastsetter at «et samtykke ikke er gyldig avgitt når det er gitt gjennom et på forhånd avkrysset/forhåndsutfylt felt som brukeren kan velge å fjerne».[53] Ny ekomlov § 3-7 vil bidra til en mer uniform gjennomføring av cookie-bestemmelsen inntil ny regulering kommer på plass ved implementering av nye EØS-relevante rettsakter. Dermed styrkes det norske regelverket og lovene harmoniseres med øvrige EU-medlemsland.[54]

Arbeidsgruppens rapport, rettspraksis fra EU-domstolen og forslaget til ny ekomlov, viser samlet sett at bruker må ha akseptert at en tilbyder kan samle inn og lagre opplysninger om seg før sporing finner sted. Det er kun gjennom en utvetydig viljesstyring, hvor bruker direkte erklærer eller tydelig bekrefter at det plasseres en informasjonskapsel, at samtykket anses for frivillig avgitt og tilbyder lovlig kan behandle opplysninger.

2.2.3 Villedende linkdesign

Arbeidsgruppen uttrykker videre at kravet til frivillig samtykke ikke anses for å være oppfylt der tilbyderen designer informasjonskapselbanneret på nettsiden på en slik måte at den gir inntrykk av at brukeren må samtykke for å få tilgang til innholdet på nettsiden.[55]

Arbeidsgruppen ble enige om en ikke-uttømmende liste over situasjoner som presumerer samtykke for ikke å være gyldig innhentet. Et informasjonskapselbanner anses å være villedende designet når;

1) eneste alternative handling, annet enn å samtykke, består av en lenke bak ordlyden «avslå» som enten

i) er innebygd i et tekstavsnitt i informasjonskapselbanneret, eller

[51] CookieInformation, «Cookie Compliance in the Nordics»
[52] Kommunal- og distriktsdepartementet, Høringsnotat; *Forslag til ny lov om elektronisk kommunikasjon,* § 3-7
[53] Kommunal- og distriktsdepartementet, Høringsnotat; *Forslag til merknader til ny lov om elektronisk kommunikasjon*, § 3-7
[54] Se punkt 2.1 som illustrerer problematikken
[55] EDPB, Cookie Banner Taskforce, s.5-6

ii) er plassert utenfor informasjonskapselbanneret, og

2) som ikke tilstrekkelig er tilpasset den informasjon en alminnelig bruker visuelt forstår.

Her presumereres altså samtykke fra brukere å være gitt under tvang, med den rettslige konsekvens at tilbyderens behandlingsaktivitet er i strid med ePrivacy-direktivet.

Problemet betegnes ofte som «dark patterns» og beskriver nettopp situasjoner hvor tilbyderen bevisst benytter designelementer og brukergrensesnitt for å villede og/eller påvirke brukere til å samtykke.[56] Ved å spesifisere villedende linkdesign som et typetilfelle for dark patterns, styrkes brukernes evne til effektivt å beskytte egne opplysninger og ta bevisste valg.

Som eksempelet viser, har kravet til frivillig avgitt samtykke en side mot at det gis tilstrekkelig informasjon og måten denne informasjonen gis. Rapporten gitt av arbeidsgruppen uttrykker at vurderingen av om det foreligger rettsstridig villedende design, skal ta utgangspunkt i hva en alminnelig bruker forstår. Brukeren skal innholdsmessig forstå at vedkommende gir et samtykke til at tilbyder henter inn og lagrer opplysninger og til hvilket formål opplysningene blir behandlet for.

Informasjonen om tilbyderens innhenting av samtykke må, ifølge arbeidsgruppen, visuelt fremkomme på første nivå av informasjonskapselbanneret.[57] Arbeidsgruppens rapport gir således en veiledning på hvordan en tilbyder visuelt skal designe informasjonskapselbanneret for å være i samsvar med regelverket.

2.2.4 Villedende fargeknapper og kontraster

En annen form for manipulerende utforming av informasjonskapselbannere arbeidsgruppen tar opp, er bruken av farger og kontraster.[58] I likhet med typetilfellet over, referer problemet om villedende fargeknapper og kontraster seg til informasjonskapselbannerets visuelle uttrykk. Utfordringen viser seg ved at bruker av en nettside blir møtt med et informasjonskapselbanner preget av uthevingsfarger som visuelt påvirker oppmerksomheten og gjør det vanskeligere å se et avslagsalternativ.

[56] CookieInformation, *What are dark patterns in cookie banners?*
[57] Se tilbake til punkt 2.1 som også utgjør utilbørlig påvirkning
[58] EDPB, Cookie Banner Taskforce, s.6

I motsetning til veiledningen for villedende linkdesign, hvor arbeidsgruppen eksplisitt fastslår når et samtykke presumeres å være gitt under tvang og uten tilstrekkelig informasjon, åpner arbeidsgruppen opp for tolkning av når informasjonskapselbannerets farger og kontraster er villedende. Arbeidsgruppen uttaler at det er en «case-by-case verification» hvor fargene og kontrastene benyttet «not obviously [are] misleading».[59] Ordlyden, «åpenbar», indikerer en høy terskel. Det må foreligge kvalifiserte forhold for at utformingen av et informasjonskapselbanner utgjør en utilbørlig påvirkning av en brukers beslutningsrett og dermed er i strid med ePrivacy-direktivet artikkel 5 (3).

Et sentralt spørsmål som reises er hvilket skjønn den konkrete helhetsvurderingen skal baseres på. Etter en objektiv vurdering, vil det avgjørende være hvordan en alminnelig person forstår informasjonskapselbanneret. Et spørsmål blir da om vurderingen av om informasjonskapselbanneret strider med rettmessig bruk av fargeknapper og kontraster skal ta utgangspunkt i en subjektiv vurdering, hvor den personlige og individuelle forståelsen er i fokus. Arbeidsgruppen tar utgangspunkt i hva en alminnelig bruker forstår ved typetilfellet for villedende linkdesign og dette taler for at tilsvarende vurdering bør legges til grunn for foreliggende typetilfelle. Tatt i betraktning at de sakkyndige ikke eksplisitt fastslår hva den konkrete helhetsvurderingen skal ta utgangspunkt i, skapes et diffust regelverk. Dette hindrer etableringen av forutsigbarhet for tilbydere og vanskeliggjør brukernes evne til å forstå hvilke rettigheter de har.

Rapporten veier delvis opp for denne usikkerheten med å legge til grunn en «minstestandard» i form av at kontrasten mellom teksten og bakgrunnen til informasjonskapselbannere ikke kan være så minimal at det i praksis er uleselig for brukeren.

2.2.5 Berettiget interesse

Et femte problem arbeidsgruppen tar opp, er tilbyders bruk av berettiget interesse som behandlingsgrunnlag i tillegg til samtykke.[60] Denne metoden for dobbelt behandlingsgrunnlag fremkommer på nettsiden ved å legge ekstra bokser ved siden av det samtykkerettslige grunnlaget eller ved å legge et avkrysningsfelt på et annet nivå. Problemet oppstår ved at informasjonskapselbanneret fremstilles med sikte på å villede en alminnelig bruker til å tro at vedkommende må nekte to eller flere ganger for ikke å få opplysninger om seg behandlet.

[59] EDPB, Cookie Banner Taskforce, s.6 avs.17
[60] EDPB, Cookie Banner Taskforce, s. 6-7

Arbeidsgruppen skiller mellom behandling av opplysninger i to faser, den første er innhenting og lagring av opplysninger gjennom bruk av informasjonskapsler på første nivå. Denne behandlingen må oppfylle vilkårene i ePD art. 5 (3). Den andre fasen gjelder eventuell etterfølgende behandling og hvor tilbyder benytter berettiget interesse.[61] Rapporten legger eksplisitt til grunn at lovligheten av behandling av personopplysninger etter personvernforordningen basert på informasjonskapsler, forutsetter at innhentingen og lagringen er i tråd med ePD art.5 (3). Bestemmelsen fungerer således som inngangsvilkår før behandlingsansvarlig i det hele tatt kan vurdere om behandlingen er gyldig etter berettiget interesse som behandlingsgrunnlag.

Til tross for rapportens presisering, åpner den også opp for nye uklarheter. Når arbeidsgruppen uttrykker at enhver påfølgende behandling må være i samsvar med GDPR, kan det implisere at behandling av opplysninger gjennom informasjonskapsler ikke trenger å være i tråd med GDPR. Imidlertid følger det av direktiv 2002/58/EC at «Bestemmelsene i dette direktivet presiserer og utfyller direktiv 95/46/EF», som er forgjengeren til Regulation 2016/679 (GDPR). Innlemmelsen innebærer at direktivet vil stå som *lex specialis* i forhold til den generelle personvernforordningen. Personvernforordningens prinsipper og praksis vil alltid være relevant som bakgrunnsrett.[62]

Som et resultat av at en bruker må avvise informasjonskapsler for hver gang vedkommende går inn på en ny side på samme nettsted, en strategi kjent som «samtykkestrømmer», øker sannsynligheten for at brukeren blir ´trøtt´. Samtykketrøtthet bidrar til at bruker samtykker til plassering av en informasjonskapsel på sitt terminalutstyr for å få vekk det forstyrrende elementet, uten å tenke over hvilke konsekvenser dette får. Som følge av stadig nye teknologiske utviklinger, og på bakgrunn av manglende kunnskap om hvordan og hvilke fremtidige analyseverktøy som vil eksistere, vil det være vanskelig å forutse hvordan behandling av opplysninger om brukere vil gripe inn og krenke brukernes private sfære. Regelverket bør derfor legge til rette for å utvise varsomhet, begrense ulike former for «dark patterns» og ta sikte på å sikre et reelt personvern.

Det er gjennomgående en interesseavveining mellom hvor langt lovgiver og myndigheter skal gå i å på den ene siden beskytte en bruker som i prinsippet har valget mellom å avslå eller

[61] GDPR artikkel 6 nr.1 bokstav f)
[62] Tilsvarende vil gjelde overfor ny kommunikasjonsvernforordning, se punkt 3.2.1 og punkt 3.2.2

godta plassering av en informasjonskapsel, og på den andre ikke stå i veien for å sikre økonomisk vekst og utvikling for virksomheter.

2.2.6 Unøyaktig klassifisering av «nødvendig» informasjonskapsel

Et særlig problem ved reguleringen av informasjonskapsler, er å vurdere hva som ligger i en «nødvendig» informasjonskapsel. Arbeidsgruppen begrunner manglende spesifikk regulering av typetilfellet i at funksjonene til informasjonskapsler endres regelmessig. Arbeidsgruppen hevder at dette hindrer etableringen av en stabil og pålitelig liste av hva som utgjør en nødvendig informasjonskapsel.[63]

Etter mitt syn kan det stilles spørsmål ved hvordan lovgiver åpner opp for den enkelte bedrift til å foreta en vurdering av hva de selv mener er nødvendig å innhente av opplysninger fra en bruker for sin virksomhet. En overvekt av virksomheter drives av kommersielle formål. Når EU kommisjonen har satt ned en sakkyndig gruppe for å vurdere rettstilstanden, er det kritikkverdig at de ikke er i stand til å i det minste komme med en ikke-uttømmende liste over situasjoner som enten taler for eller mot at en opplysning er «nødvendig» for en bedrift. En liste av momenter vil bidra til forutberegnelighet for virksomhetene, samt styrke rettssikkerheten. Et naturlig relevant moment å vurdere, er hvilken type analyse informasjonskapselen skal brukes til. En informasjonskapsel som benyttes til å lagre informasjon om hvilket skjema en bruker har fylt ut og sendt inn, er typisk av essensiell betydning for et apotek som tilbyr medisiner. Motsetningsvis skal det mer til for at en analyse med formål om å gjennomføre målrettet reklame, for eksempel for å øke omsetningen av hårstrikker, anses som «nødvendig» for den aktuelle tilbyderen.

Et eksempel som kan belyse hvordan samme forhold blir underlagt forskjellig perspektiv, og vurdering av hva som er nødvendig for å levere en tjeneste, er Schibsted og Mediebedriftenes Landsforening (MBL) sitt høringssvar til Kommunal- og distriktsdepartementet vedrørende forslag til ny ekomlov.[64]

Mediebedriftenes Landsforening representerer 325 medlemsbedrifter med 205 mediehus, herunder Schibsted, og 150 lokalaviser.[65] Schibsted, et nordisk mediekonsern med

[63] EDPB, Cookie Banner Taskforce, s. 7
[64] Ingvild Næss og Simen Breen, *Høringsuttalelse – Forslag til ny ekomlov, ny ekomforskrift og endringer i nummerforskriften.* Schibsted. 15.10.2021; Randi S. Øgrey, *Høringsuttalelse om forslag til ny ekomlov*. Mediebedriftenes Landsforening (MBL). 15.10.2021
[65] Mediebedriftene, «Våre medlemmer». https://www.mediebedriftene.no/om-mbl/vare-medlemmer/

merkevarer som VG, Aftonbladet, Aftenposten, Svenska Dagbladet, Bergens Tidende og Stavanger Aftenblad, tiltrer i sitt høringssvar MBL sin høringsuttalelse i sin helhet. I høringsuttalelsene viser MBL og Schibsted til at informasjonskapsler som er nødvendig for å opprettholde finansieringen av journalistikk må anses som nødvendige. De hevder at på bakgrunn av mediers samfunnsverdi som demokratisk infrastruktur, og ettersom norske mediers forretningsmodell baserer seg på brukerinntekter og annonseinntekter, må informasjonskapsler med annonsehensikt kunne anses som nødvendige. Den rettslige konsekvensen er at tilbyder får unntak fra kravet til samtykke. MBL og Schibsted argumenterer videre med at informasjonskapsler som tilrettelegger for målrettet annonsering er nødvendig for å forebygge svekkelse av deres konkurranseevne i møte med globale teknologigiganter som Google og Facebook.[66]

Høringsuttalelsene antyder at de, i likhet med flertallet av kommersielle tilbydere, ønsker å utnytte informasjonskapsler med formål om å få størst mulig fortjeneste. Det er normalt at virksomheter ønsker best mulig konkurranseevne og dette vil dermed alltid utgjøre et relevant argument for å kunne benytte informasjonskapsler. På den andre siden står hensynet til å verne brukerne og retten til respekt for privatlivet.[67] Fysiske og juridiske personer har rett på en «privat sfære» hvor vedkommende fritt skal kunne danne egne meninger og handle deretter, uten at det foreligger tvang eller innblanding fra myndighetene eller øvrige personer. Ved at bedrifter gis vide adganger til å kunne behandle opplysninger for å produsere annonser og reklame med persontilpasset innhold, er dette nettopp for å påvirke brukeren til enten å kjøpe ett produkt eller en tjeneste, eller for å endre mottakerens adferd til en bestemt retning.[68]

Lagt til grunn at utgangspunktet og hovedregelen er at det er forbudt å behandle opplysninger, må det foreligge kvalifiserende forhold for unntaksvis å kunne legitimere behandling. For at lovreguleringen skal sikre et reelt vern er det viktig at terskelen for å fravike hovedregelen ikke settes for lavt.

Unøyaktig klassifisering av en informasjonskapsels nødvendighet er spesielt fremtredende på markedsførings- og reklamesektorens område. Fraværet av ensartet praksis på området øker

[66] Ingvild Næss og Simen Breen, *Høringsuttalelse – Forslag til ny ekomlov, ny ekomforskrift og endringer i nummerforskriften.* Schibsted. 15.10.2021; Randi S. Øgrey, *Høringsuttalelse om forslag til ny ekomlov*. Mediebedriftenes Landsforening (MBL). 15.10.2021
[67] Grl. § 102; EMK Art.8
[68] Store norske leksikon, «annonse», av Roger Pihl, 16.04.2023. https://snl.no/annonse

risikoen for omgåelser og å skjule det reelle formålet med behandlingen av brukerens opplysninger.

Imidlertid viser arbeidsgruppens rapport til at det eksisterer spesifikke verktøy som kan benyttes for å analysere et nettsted, og til å lage en rapport som gir en oversikt over de informasjonskapslene tilbyder har plassert på en brukers terminalutstyr under besøket på nettstedet.[69] De ulike formålene bak plasseringen av en informasjonskapsel på brukerens terminalutstyr kan blant annet referere seg til nødvendige, analytiske, preferansebaserte, funksjonsbaserte, målrettede eller statistikkbaserte informasjonskapsler.[70] Bruk av informasjonskapsler kan således benyttes til alt fra tekniske tilpasninger på den enkelte nettside, til å ha en fungerende direktechat, hente inn statistikk på antall besøk eller besøkte nettsider, analysere brukermønstre og til å tilby og måle relevante annonser.

Til tross for at verktøyet får tilgang til hvilke informasjonskapsler som er plassert, er det ikke mulig å se innholdet. Dette er en klar indikator på at tilsynsmyndighetene får en svekket kontroll og oversyn over at tilbyderens innhenting og lagring av opplysninger er i tråd med det formålet behandlingen er satt for.

Rapporten uttrykker at verktøyet kun er ment å fungere som en ekstra hjelp til kompetente myndigheter for å søke avklaring og informasjon fra tilbyderen, som et tillegg til den informasjonen som gis på den aktuelle nettsiden. Verktøyet er således med på å skape en bevisstgjøring blant tilbydere som benytter informasjonskapsler for behandling av opplysninger. Nærliggende skaper tilsynskontroller insentiv for tilbydere av elektronisk kommunikasjonstjenester til å få forholdene på det rene med en gang. Særlig vil tilsynskontroller bidra til at tilbydere som krenker reguleringen på bakgrunn av manglende vilje til å sette seg inn i regelverket, kunne fanges opp. Verktøyet kan videre tjene til å skape ikke-rettslige konsekvenser i form av et press utad, ved at tilbydere som ikke er åpne om behandlingsaktiviteten med offentligheten kan fremstå som har noe å skjule. Verktøyet bidrar dermed til gjennomsiktighet, som i det store bildet gir bedre vern for brukerne. Til tross for at ytre press er av en ikke-rettslig konsekvens, vil altså forhold utenfor de rettslige rammene kunne bidra til økt etterlevelse av regelverket. Dette vil også skape mer forutsigbarhet mellom tilbydere om hva som faktisk er i tråd med regelverket og ikke.

[69] EDPB, Cookie Banner Taskforce, s.8
[70] Se for eksempel oversikt over hvilke informasjonskapsler HELP Forsikring og TV2s nettsteder benytter, jf. HELP Forsikring, «Informasjonskapsler (cookies)»; TV2, «Bruk av cookies på TV 2s nettsteder»

At det ikke eksisterer en mer konkret regulering av hvordan man kan vurdere hvilke opplysninger som er nødvendig for tilbyder av en tjeneste, er særlig problematisk med hensyn til hvilket vern en bruker nyter etter direktivet og ekomloven, sett opp mot personvernet etter GDPR.

Et sentralt spørsmål er dermed å definere hva som ligger i en «opplysning». Imidlertid følger det verken av direktiv 2002/58/EC, ekomloven, forslag til ny ekomlov eller fremmet forslag til ny kommunikasjonsvernforordning en definisjon av hva begrepet omfatter. En alminnelig språklig forståelse indikerer at opplysninger på området for elektronisk kommunikasjon nyter et videre vern enn fysiske personer etter personvernforordningen, ved at lovverkets anvendelsesområde ikke begrenses til personopplysninger.[71] En «personopplysning» er legaldefinert i GDPR artikkel 4 nr.1 som

> «enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet,»

Den vide definisjonen indikerer at nesten alle opplysninger er personopplysninger, så lenge de kan knyttes til enkeltpersoner. På ekomområdet kan en «opplysning» tas til inntekt for å inkludere enhver informasjon som avgis av en bruker i forbindelse med bruk av elektroniske kommunikasjonstjenester. Det følger av forarbeidene til ekomloven at «Personvernet i ekomsektoren (kommunikasjonsvernet) har tradisjonelt stått sterkt».[72] Forarbeidene legger videre til grunn at for å sikre at brukere til enhver tid har tilstrekkelig beskyttelse, uavhengig av teknologi som anvendes, må informasjon som anses som en opplysning tilpasses den markedsutvikling og den teknologiske utvikling som finner sted innenfor elektroniske kommunikasjonstjenester.[73]

Sett opp mot at formålet med lovreguleringen av ekomsektoren er å sikre at brukere har kontroll på opplysninger om seg, taler dette for at alle opplysninger som kan bidra til å skape en profil om brukere nyter vern. Den strenge linjen indikerer videre at vernet *mutatis*

[71] GDPR Art.2
[72] Prop.69 L (2012-2013) s.27
[73] Prop.69 L (2012-2013) s.27-28

mutandis skal gjelde for juridiske personer. Som følge av at enhver informasjon om en bruker nyter vern, blir det tilsvarende vanskelig for næringsvirksomheter å kunne behandle opplysninger ved bruk av informasjonskapsler.

Jeg mener det er kritikkverdig at den sakkyndige gruppen tydelig viser at de er klar over problemet, men likevel ikke kommer med en avklaring for hvordan videre å behandle dette typetilfellet av manipulativt design. Stadige endringer fra lovgivere og sakkyndige grupper skaper uforutsigbarhet både for tilbydere som benytter informasjonskapsler og brukerne. Uklarhetene svekker ytterligere enhetlig praktisering av cookie-bestemmelsen innen EU og EØS.

2.2.7 Manglende ikon for tilbakekall av samtykke

Siste typetilfelle rapporten tar for seg, er problemet for brukere til å trekke tilbake samtykke sitt.[74] Det at arbeidsgruppen kun anbefaler at tilbydere burde plassere en lett tilgjengelig mulighet for brukere til å trekke tilbake sitt samtykke, er problematisk. Arbeidsgruppen foreslår å sette et svevende eller permanent synlig ikon eller link plassert på et synlig og standardisert sted, og tar et forbehold om at «they cannot be imposed a specific withdrawal solution [...] only [...] easily accessible solutions».[75] Men hva er lette tilgjengelige løsninger? Arbeidsgruppen åpner igjen opp for skjønn som på den ene siden skaper usikkerhet og uforutsigbarhet for tilbydere og svekker rettssubjektenes evne til å forutberegne sin rettsstilling. På den andre siden gir en slik fleksibel løsning rom for individuelle tilpasninger som tilrettelegger for teknologiske utviklinger.

I undersøkelsen foretatt av CookieInformation, var et av kriteriene selskapet gransket, om nettstedet som benyttet en informasjonskapsel ga brukeren mulighet til å endre eller trekke tilbake sitt samtykke. Av de norske nettsidene var det kun 43% av tilbyderne som ga slik adgang. Sammenlignet med de øvrige nordiske landene, kom Norge dårligst ut av undersøkelsen.[76] Rapporten indikerer at det er et stort avvik i gjennomføringen av regelverket for norske næringsvirksomheter. Det kan spørres om avvikene skyldes uklare regler, at bedrifter bevisst velger å ikke behandle opplysninger i tråd med lovgivningen, eller om manglende samsvar skyldes at norske myndigheter har for milde sanksjoner ved brudd.

[74] EDPB, Cookie Banner Taskforce, s.8
[75] EDPB, Cookie Banner Taskforce, s. 8 avs. 35
[76] CookieInformation, «Cookie Compliance in the Nordics»

Brudd på regelverket har også ikke-rettslige konsekvenser. At nettsteder behandler opplysninger i strid med lovverket, går utover næringsvirksomheters evne til å etablere et godt omdømme. Gjennom en åpen og lovlig behandling kan selskapet bygge opp velvilje og tillit hos brukerne. Klare regler skaper forutsigbarhet. Sett fra et bruker-perspektiv vil nærliggende skepsisen mot å faktisk dele opplysninger være mindre, hvor risikoen for at opplysningene kommer på avveie er lav.

På den andre siden er det bra regelverket baseres på en rettslig standard, slik at uttalelsene og rådgivningen ikke mister relevans i møte med nye teknologiske utviklinger. Motsetningsvis er det viktig å minne om at rapporten kun har begrenset rettskildemessig vekt. Dermed kan det argumenteres for at arbeidsgruppen burde benyttet muligheten til å skape mer oppklaring og konkrete føringer for å styrke en mer konsistent og harmonisert gjennomføring av regelverket i alle medlemsstatene.

Imidlertid gis det en viss oppklaring og konkrete krav til tilbyder ved at tre kumulative vilkår må være oppfylt i tillegg til kravene for lovlig innhenting av samtykke.

1) Det må være mulighet for å trekke tilbake sitt samtykke
2) Det må være mulighet for å trekke tilbake sitt samtykke til enhver tid
3) Tilbaketrekking av samtykke skal være like enkelt som å gi et samtykke

Arbeidsgruppen presiserer at ePrivacy-direktivets referanse til samtykke i GDPR inkluderer definisjonen etter GDPR artikkel 4 nr. 11 og vilkår for samtykke etter GDPR artikkel 7.[77]

2.3 Samtykkekravets egnethet som behandlingsgrunnlag

De lege lata, er eneste rettmessige behandlingsgrunnlag etter norsk og europeisk rett for tilbyder på ekomområdet, å innhente et frivillig avgitt samtykke fra den enkelte bruker. På denne måten er det brukeren selv som autoriserer at opplysninger om seg behandles. Dette innebærer at den enkelte brukeren selvstendig må sette seg inn i og forstå hvordan den aktuelle tilbyders nettside rent teknisk fungerer og omfanget av informasjonen som gis. Som belyst over, reises det en rekke problemstillinger ved å benytte samtykke som behandlingsgrunnlag. Med den samtykkestrømmen brukere daglig utsettes for, kan det virke mer eller mindre tilfeldig om vedkommende aksepterer plasseringen av en informasjonskapsel eller ikke. En virksomhet som baserer seg på samtykke fra brukeren, kan heller ikke vite hvor

[77] EDPB, Cookie Banner Taskforce, s. 8 avs. 33

informert avgivelsen var og om brukeren reelt sett forstod hva aksepten innebar. Dette vanskeliggjør overholdelse av regelverket for bruk av informasjonskapsler for tilbyderne.

Samtidig som EUs personvernråd og arbeidsgruppen legger ned en streng og utfordrende linje for gyldig innhenting av samtykke, er det fortsatt uklarheter i hvordan tilbydere skal forstå foreliggende regelverk. Dette resulterer i en inkonsekvent og ineffektiv beskyttelse av personvernet, og utfordringer knyttet til konfidensialitet ved elektronisk kommunikasjon. Manglende forståelse av regelverket underbygges av det høye antallet klagesaker som er fremmet i EU. I den årlige rapporten publisert av Data Protection Commission (DPC) for 2022, kom det frem at de mottok 105 gyldige varsler om databrudd etter ePrivacy-direktivet. Dette utgjør en tredobling av bruddvarsler for samme tidsperiode i 2021. DPC fremhever at uoverensstemmelsene med regelverket er et resultat av endringer i lovgivningen, blant annet fordi definisjonen av «elektronisk kommunikasjonstjeneste» utvides til også å omfatte såkalte «over the top»-tjenesteaktører».[78] Et uklart regelverk vanskeliggjør tilbyders mulighet til å drive lovlig næringsvirksomhet.

Mediebedriftenes Landsforening viser i sin høringsuttalelse til at de på bakgrunn av de høye kravene for lovlig å kunne behandle opplysninger ved bruk av samtykke, har «valgt å benytte et annet rettslig grunnlag enn samtykke i henhold til personopplysningsloven [... i form av …] legitim interesse».[79] Det følger av kravet til berettiget interesse, at behandlingsansvarlig lovlig kan behandle personopplysninger hvor vedkommendes interesser overstiger den registrertes interesser og grunnleggende rettigheter og friheter.[80] Ved at virksomheter pålegges å foreta en konkret interesseavveining, vil de tvinges til å iverksette personvernfremmende tiltak for å sikre lovlig behandlingsgrunnlag. Profesjonelle bedrifter, som får flere besøk daglig, vil naturlig være bedre rustet til å vurdere og gjennomføre de tekniske og organisatoriske tiltakene som kreves for å sikre at all behandling av personopplysninger er forsvarlig og begrenset til det som er nødvendig. At ansvaret for å behandle opplysninger legges på tilbyder kan dermed bidra til at brukere reelt sett gis et bedre beskyttelsesnivå sammenlignet med en

[78] Data Protection Commission, «Annual Report 2022», 2022. https://www.dataprotection.ie/sites/default/files/uploads/2023-03/DPC%20AR%20English_web.pdf ; Kommunikasjonsvernforordningen av 21.feb 2021 fortalepunkt 11, jf. Directive of the European Parliament and of the Council (EU) 2018/1972 of 18 December 2018 establishing the European Electronic Communications Code (Elektronisk kommunikasjonskodedirektiv): Med over-the-top-tjenesteleverandør forstås teknologi som leverer strømmet innhold over internett, som Netflix, Youtube og Disney+, jf. adjust, «What is over-the-top (OTT)?»

[79] Randi S.Øgrey, *Høringsuttalelse om forslag til ny ekomlov*. Mediebedriftenes Landsforening (MBL). 15.10.2021; se GDPR artikkel 6 nr.1 bokstav f)

[80] Eva Jarbakk, *Karnov lovkommentar: personopplysningsloven artikkel 6 nr.1 bokstav f)*, Lovdata.no. Lest 18.04.2024

virksomhet som baserer seg på brukerens aksept. Dette vil spesielt kunne bidra til å styrke vernet for de svakere stilte personene i samfunnet, som barn, eldre og mennesker med nedsatt funksjonsevne.

Det kan stilles spørsmål med Mediebedriftenes Landsforenings uttalelse, som indirekte kan tas til inntekt for at MBL i realiteten ser bort fra kravet til samtykke og benytter andre rettslig grunnlag for behandling av opplysninger. Som det følger av gjeldende rett er det ikke anledning til å behandle opplysninger fra informasjonskapsler på andre grunnlag enn samtykke.[81] Behandling av opplysninger ved bruk av informasjonskapsler er dermed rettsstridig i de tilfeller hvor tilbyder ikke har hentet inn et på forhånd avgitt samtykke. Uttalelsene illustrerer problematikken knyttet til tilbyderes manglende samsvar med typetilfellene for berettiget interesse og unøyaktig klassifisering av en «nødvendig» informasjonskapsel.

Schibsted og MBL viser videre til at et skjerpet samtykkekrav, som fremmet ved ny ekomlov § 3-7, «ytterligere vil svekke norske redaksjonelle mediers posisjon i annonsemarkedet».[82] Et sentralt argument for hvorfor de mener mediene burde være unntatt fra kravet til samtykke, er deres samfunnsrolle for å sikre demokrati og at brukerne gis etterrettelig informasjon. En konsekvens av den frie adgangen til å spore og danne profiler om brukere har resultert i at mange land opplever en polarisering med etterfølgende fare for dannelse av ekkokamre. Med dagens sosiale medieplattformer, som Instagram, Facebook og TIKTOK, blir brukere gjennom algoritmer og informasjonsstrømmer dratt inn i en form for sosial boble, hvor de utsettes for ensidig informasjon, ideer og oppfatninger, uten å få utfordret meningene sine.[83] Dette er klart et relevant og reelt problem med dagens teknologiske utvikling. Uten tiltak risikerer vi at det skapes stor splittelse mellom ulike grupper, hvor mennesker går glipp av nyanser og et helhetsbilde.

På den andre siden har tilstrømningen av nye digitale medier senket terskelen for brukere til å delta i den offentlige debatten. De digitale plattformene har bidratt til å skape arenaer som gir rom for alminnelige personer til å kunne ytre seg om viktige samfunnsmessige spørsmål. Behandling av opplysninger og hensynet til demokratiet har dermed en side mot

[81] Jf. Ekomloven § 2-7 b og ePD Art.5 (3)
[82] Randi S.Øgrey, *Høringsuttalelse om forslag til ny ekomlov*. Mediebedriftenes Landsforening (MBL). 15.10.2021, s.3.
[83] Wolff-Hansen, E. S., Overland, J. (2021, 10. desember). Digitale og sosiale medier i offentligheten. NDLA. https://ndla.no/article/34509

ytringsfriheten.[84] Ved vurderingen av om hvor egnet samtykke er som behandlingsgrunnlag, er det sentralt å se på at kravene som stilles til norske aktører vil gjelde tilsvarende for de globale teknologigigantene. Lovreguleringen vil i realiteten likestille aktørene og bidra til like konkurransegrunnlag.

Et eksempel som viser at også de store teknologiselskapene har begrensede muligheter til å behandle opplysninger på bakgrunn av samtykke, er vedtakene fra det irske datatilsynet mot det amerikanske selskapet Meta. Meta, morselskapet til de sosiale nettverkene Facebook og Instagram, mottok et overtredelsesgebyr på til sammen 390 millioner euro for ulovlig behandling av personopplysninger til målrettet reklame. Det irske datatilsynet la vekt på at Meta hadde forsøkt å omgå kravet til samtykke etter personvernforordningen ved å innta samtykkebestemmelser i brukervilkårene. Avgjørelsen innebærer at Meta må innhente samtykke fra brukeren gjennom at vedkommende aktivt gir et samtykke, såkalte opt-in-løsninger. Som en konsekvens av dette må Facebook tilby sine tjenester til brukerne selv om de ikke gir sitt samtykke til målrettet reklame. Det irske datatilsynet la til grunn at det avgjørende ikke var at den relevante behandlingsaktiviteten er tatt inn i tjenestevilkårene, men at behandlingen knyttet til kontraktsforpliktelsen objektivt sett er nødvendig for å oppfylle kjerneelementet i avtalen med den registrerte. Meta fikk ikke medhold i anførselen om at de kunne benytte GDPR artikkel 6 nr.1 bokstav b), som åpner opp for å kunne behandle på grunnlag av kontraktsforpliktelse, som lovlig behandlingsgrunnlag. Datatilsynet så på at hovedformålet med bruken av Facebook og Instagram, sett fra brukernes perspektiv, er kommunikasjon og interaksjon med hverandre og ikke målrettet markedsføring.[85]

Avgjørelsen gir således et signal til tilbydere om hvilke behandlingsgrunnlag som lovlig kan brukes for profilering og målrettet markedsføring. Overført til Schibsted og andre nyhetsformidlere, vil det nærliggende kjerneelementet, og hva som utgjør rettslig ramme for lovlig behandling av opplysninger for tjenesten, være å gi uavhengig etterrettelig informasjon og nyheter, ikke motta reklame.

Avgjørelsen innebærer ytterligere at Meta, og andre virksomheter som baserer seg på avtale som rettslig grunnlag for målrettet markedsføring, står i fare for å måtte endre hele sin

[84] Wolff-Hansen, E. S., Overland, J. (2021, 10. desember). Digitale og sosiale medier i offentligheten. NDLA. https://ndla.no/article/34509 ; jf. Grl. § 100

[85] Gjessing, Marianne (2023, 5.januar). Historisk dom: Meta får ikke bruke persondata til målrettet annonsering. Digi.no https://www.digi.no/artikler/historisk-dom-meta-far-ikke-bruke-persondata-til-malrettet-annonsering/524798 ; Vågen, Kjetil mfl. (2023, 30.Januar). Skyhøye gdpr-bøter til Meta for ulovlig målrettet markedsføring. Cpl.no. https://clp.no/skyhoye-gdpr-boter-til-meta-for-ulovlig-malrettet-markedsforing/

forretningsmodell. Overført til rettmessig bruk av informasjonskapsler, vil behandling av opplysninger for å eksponere brukerne for annonser ikke kvalifisere til å kunne klassifisere som «nødvendig», med den rettslige konsekvens at tilbyder eksplisitt må hente inn et samtykke.

Det sentrale er altså brukerens selvbestemmelsesrett som legitimitetsgrunnlag. Ved å benytte samtykke som lovlig behandlingsgrunnlag, beholdes suvereniteten, friheten til å velge selv, hos det enkelte individ. På den andre siden begrenses tilbyderes inntektsevne, da manglende samtykke fra brukere naturlig hindrer virksomheter i å sende spesialtilpassede annonser og reklame. I punkt 3 nedenfor redegjøres det for hvordan forslag til kommunikasjonsvernforordningen introduserer ytterligere grunnlag for plassering av informasjonskapsler og behandling av informasjonen en bruker gir til tilbyder.

3 Kommunikasjonsvernforordningen

3.1 Introduksjon

Samtidig som arbeidet med oppklaring av hva som faller innenfor ePrivacy-direktivets artikkel 5 (3) pågår, har EU-kommisjonen fremmet forslag til en ny forordning for å regulere elektronisk kommunikasjon. Hensikten med reguleringen er å styrke tilliten og sikkerheten i en stadig mer digital verden.[86] Forslaget er således et ledd i en moderniseringsprosess for å imøtekomme de nye teknologiske utviklingene. Kommunikasjonsvernforordningen (ePR) vil blant annet åpne opp for flere behandlingsgrunnlag som kan legitimere behandling av opplysninger ved bruk av informasjonskapsler, samt sikre at rettighetene og pliktene nedfelt i forordningen omfatter de nye aktørene (som har kommet etter siste revidering av ePD i 2009).

3.2 Lovgivningsprosessen

Det opprinnelige forslaget til en ny forordning på ekomsektorens område ble fremmet allerede i 2017, med sikte på å tre i kraft samtidig som GDPR i 2018. EUs medlemsland har imidlertid ikke kommet til enighet om utformingen, hvor det i senere tid er blitt publisert en rekke utkast. Uenighetene har blant annet basert seg på behovet for klargjøring av forholdet mellom elektronisk kommunikasjon og GDPR, personverninnstillinger og anledningen til å tillate andre rettslige grunnlag for behandling av opplysninger enn samtykke.[87]

Det nyeste forslaget kom 5.januar 2021 fra det portugisiske presidentskapet. Den 21.februar 2021 ble det bekreftet enighet fra EUs ministerråd, og forordningen er per i dag underlagt en trepartsforhandling.[88] Kommunikasjonsvernforordningen tar sikte på å oppheve og erstatte ePrivacy-direktivet 2002/58.

3.2.1 Forholdet til personvernforordningen (GDPR)

I kommunikasjonsvernforordningens fortalepunkt 2a spesifiseres det at kommunikasjonsvernforordningen, i forhold til personvernforordningen (GDPR), gir ytterligere krav til beskyttelse av retten til privatliv og kommunikasjon. Fortalen uttrykker

[86] European Commission, «Proposal for an ePrivacy Regulation»
[87] European Parliament, «Proposal for a regulation on privacy and electronic communication»
[88] Trepartsforhandlingene, «trilogues», består av EU organene Europaparlamentet, Rådet og Kommisjonen. Formålet med forhandlingene er å bli enige om en foreløpig avtale med en akseptabel tekst, jf. European Parliament, «Interinstitutional negotiations»; European Parliament, «proposal for a regulation on privacy and electronic communication»

eksplisitt at «The provisions of this Regulation particularise and complement the general rules on the protection of personal data laid down in Regulation (EU) 2016/679».[89] Formuleringen indikerer at kommunikasjonsvernforordningen tar sikte på å stå som *lex specialis* i forhold til GDPR. At kommunikasjonsvernforordningen presiserer og utfyller personvernforordningen vil være en videreføring av gjeldende rett og medfører at sistnevnte forordning vil fungere som et sikkerhetsnett for brukerne etter kommunikasjonsvernforordningen.[90] På denne måten fører kommunikasjonsvernforordningens ikrafttredelse til at brukere i realiteten får et styrket vern. Tilbyders lovlighet av behandlingen av opplysninger må være i tråd med kommunikasjonsvernforordningen og personvernforordningen (GDPR). Tatt i betraktning hensynet til koherens i EU systemet, og at ePR er utformet i visshet av GDPR som eldre regulering, må forordningen leses på bakgrunn av dette.

3.3 Kommunikasjonsvernforordningen artikkel 8

Tilbyderes adgang til å behandle opplysninger ved elektronisk kommunikasjon, er regulert i utkastet til ny kommunikasjonsvernforordning av 21.feb 2021 artikkel 8. Hensikten bak bestemmelsen er å beskytte brukerens terminalutstyr, det vil si deres smarttelefoner, datamaskiner og andre enheter, fra å uberettiget bli sporet av nettsteds- og appoperatører. Med «sporing» forstås først og fremst målrettet og systematisk bearbeidelse av brukere gjennom bruk av informasjonskapsler.[91]

Slik det legges til grunn i fortalepunkt 2 i fremmet kommunikasjonsvernforordning, kan innholdet av elektronisk kommunikasjon avdekke sensitiv informasjon om fysiske personer. Dette omfatter alt fra personlige erfaringer, følelser, medisinske forhold og politiske syn, samt metadata, som blant annet inkluderer hvem bruker har ringt, besøkte nettsider, geografisk lokasjon, tid, sted, mv.[92] Gjennom systematisk sporing av enkeltindivider, bygges det så opp profiler som gjør en tilbyder i stand til å trekke konklusjoner om brukeres hverdagslige adferd, interesser og aktiviteter. Dette er problematisk fordi nettsteds- og appoperatører gjennom små og 'usynlige' handlinger kan legge inn annonser og uoppfordret reklame som

[89] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communication) of 21. February 2021 (Kommunikasjonsvernforordningen)
[90] Jf. Direktiv 2002/58/EC artikkel 1 (2)
[91] CMS, «Tracking under the e-privacy regulation»
[92] Med metadata forstås informasjon som beskriver annen informasjon, altså «data om data», jf. Store norske leksikon, «metadata», av Aud Gjersdal og Tom Heine Nätt, 10.03.2023. https://snl.no/metadata

over tid og samlet sett påvirker brukeren. Slik manipulerende påvirkning hevdes å utgjøre en trussel mot demokratiet, ettersom eksponering av ensidig informasjon begrenser en brukers frie meningsdannelse og forståelse av andre synspunkter .[93] Det kan argumenteres for at det ligger mye makt i en aktørs evne til å påvirke en eller flere andre til å tenke eller handle på en annen måte enn vedkommende ellers ville gjort.[94] Det kan for eksempel tenkes at nettoperatøren gjennom å vise masse videoer og artikler om barn som sliter på skolen, dårlige lokaler og slitte bøker, indirekte og over tid påvirke brukeren til å stemme på det politiske partiet som nettopp har skole og barn i sitt partiprogram.

På bakgrunn av verdien som ligger i opplysninger om en bruker, samt retten til respekt for privatliv og kommunikasjon, er det gode grunner til å videreføre utgangspunktet om at behandling av opplysninger er forbudt.[95] I likhet med ePrivacy-direktivet, gjøres det unntak fra forbudet mot å samle inn og behandle opplysninger, med den rettslig konsekvens at nett- og appoperatører likevel kan spore brukere. I motsetning til gjeldende rett, hvor samtykke utgjør eneste mulige lovlige behandlingsgrunnlag for tilbyder til å samle inn og lagre opplysninger om en bruker ved bruk av informasjonskapsler, følger det av utkastet til ny kommunikasjonsvernforordning en utvidelse av alternative, gyldige behandlingsgrunnlag.[96] De foreslåtte, alternative, behandlingsgrunnlagene skal nå behandles i oppgaven.

3.3.1 Adgangen til sesjonsinformasjonskapsler

De lovfastsatte behandlingsgrunnlagene er nedfelt i kommunikasjonsvernforordningen artikkel 8 bokstav a) til h). I tillegg til samtykke, som det opprinnelige behandlingsgrunnlaget, åpnes det blant annet for såkalte «session cookies». Etter bokstav d), kan en sesjonsinformasjonskapsel benyttes der dette er nødvendig for å kunne tilby en elektronisk kommunikasjonstjeneste, tilby informasjonssamfunnstjenester brukeren spesifikt har bedt om og nettpublikumsmåleverktøy gjennomført av tilbyderen.[97] Hensikten med tilbyders adgang

[93] Romarheim, «Digital påvirkning som eksistensiell trussel», Strategem.no. 26.02.2021. https://www.stratagem.no/digital-pavirkning-som-eksistensiell-trussel/ ; se punkt 2.3 som drøfter tilsvarende fare for dannelsen av ekkokamre og sterk politisk polarisering.
[94] Store norske leksikon, «innflytelse», av Ole T. Berg,19.02.2021. https://snl.no/innflytelse
[95] Jf. Kommunikasjonsvernforordningen av 21.feb 2021 Artikkel 8 nr.1
[96] Jf. Kommunikasjonsvernforordningen av 21.feb 2021 Artikkel 8 nr.1 bokstav a) til h)
[97] «It is necessary for the sole purpose of audience measuring, provided that such measurement is carried out by the provider of the service requested by the end-user, or by a third party, or by third parties jointly on behalf of or jointly with provider of the service requested provided that, where applicable, the conditions laid down in Article 26 or 28 of Regulation (EU) 2016/679 are met", jf. Kommunikasjonsvernforordningen av 21.feb 2021 Artikkel 8 nr.1 bokstav d)

til å benytte seg av slike informasjonskapsler, uten et krav om å hente inn et samtykke fra brukeren først, ligger i behandlingsaktivitetens karakter. Sesjonsinformasjonskapsler anses for å være av begrenset betydning og nytte fordi informasjonskapslene ikke sporer brukeren på tvers av nettsider og forutsettes å utløpe i det brukeren lukker den aktuelle nettleseren.[98]

En sentral problemstilling som reises ved at det åpnes for sesjonsinformasjonskapsler, er hvordan den utvidende behandlingsadgangen reguleres, herunder spørsmålet rundt at samme informasjonskapsel benyttes på flere nettsider og hvor grensen for behandlingsgrunnlagets omfang skal gå.

Det følger av fortalepunkt 21 i fremmet kommunikasjonsvernforordning, at unntak fra kravet til å innhente samtykke fra brukeren bør begrenses til situasjoner som innebærer ingen eller kun svært begrenset inntrengning i personvernet. Fortalepunktet viser til at informasjonskapsler med varighet for en enkelt sesjon på et nettsted «to keep track of the end-user´s input when filling in online forms over several pages» vil være et slikt tilfelle som kan legitimere unntak fra hovedregelen.

Som utgangspunkt er informasjonskapsler som er laget av en tilbyder, kun lesbart for den konkrete tilbyderen. Problemet er hvordan tilbyder benytter de innhentede opplysningene i sesjonsinformasjonskapselen. Utfordringen kan illustreres ved at tilbydere av elektroniske kommunikasjonstjenester, som for eksempel teknologigigantene Facebook og Google, ofte har tilstedeværelse på flere nettsider samtidig. Google og Facebook kan dermed plassere samme informasjonskapsel på nettsider som blant annet VG, NRK og Cubus, typisk gjennom annonser, sosiale plugins osv. På denne måten kan den samme ID-informasjonskapselen, som egentlig ga brukeren en tilfeldig verdi, delta i å systematisk spore søkehistorikken og brukerens adferd som senere kan benyttes til for eksempel målrettet markedsføring. Dermed risikerer brukere at opplysninger som opprinnelig ble innhentet med grunnlag i førstepartsinformasjonskapsler etter kommunikasjonsvernforordningen artikkel 8, også kan være en sporingsinformasjonskapsel som det vil kreve samtykke for å lovlig kunne behandle.[99]

---

[98] Naithani, «Curtailing the Cookie Monster through Data Protection by Default». Tilburg Law Review. 17.02.2023. https://tilburglawreview.com/articles/10.5334/tilr.311?fbclid=IwAR2LmVHpPTAePV9dwP_cmXLct4OD55JQYCy1xkO01l9veHM6R7Axn7OIv6I ; CMS, «Tracking under the e-privacy regulation»

[99] Naithani, "Curtailing the Cookie Monster through Data Protection by Default". Tilburg Law Review. 17.02.2023. https://tilburglawreview.com/articles/10.5334/tilr.311?fbclid=IwAR2LmVHpPTAePV9dwP_cmXLct4OD55JQYCy1xkO01l9veHM6R7Axn7OIv6I

Ved at lovreguleringen åpner muligheten for tilbydere til å behandle opplysninger på andre grunnlag enn samtykke, kan tilføyelsene bidra til svekkelse av samtykkegrunnlagets realitet på ekomområdet. En naturlig konsekvens av alternative behandlingsgrunnlag, som ikke krever eksplisitt aksept fra den konkrete brukeren, er innsnevring av personers selvbestemmelsesrett.

Det vil gjennomgående være en fare for at tilbydere misbruker posisjonen sin og benytter seg av innsamlet informasjon til å spore brukeren til tross for at sesjonsinformasjonskapselen har utløpt. At kommunikasjonsvernforordningen gir unntak fra forbudet for nettpublikumsmåling etter bokstav d), kan tas til inntekt for at muligheten for omgåelse øker.

På den andre siden er fordelen med at lovgivningen åpner for flere behandlingsgrunnlag, at det legges til rette for bedrifter til å satse på innovasjon. Et samfunns utvikling og økonomisk vekst er elementært avhengig av at det skapes verdier på nye måter.[100] At lovgivningen legger til rette for at selskap kan gjøre seg selv i stand til å holde konkurransedyktigheten oppe og styrke muligheten for å foreta gode strategiske beslutninger, er derfor essensielt. Forslaget bygger på tillit, hvor sesjonsinformasjonskapsler vil bidra til at selskaper mer effektivt kan gjennomføre interne prosesser, forbedre sine produkter og tjenester.

3.3.2 Kompatibelt formål

Et særlig aktuelt behandlingsgrunnlag er tilbyderes adgang til å fastslå en formålskompatibilitet mellom det opprinnelige formålet for behandlingen og formålet med den videre tiltenkte behandlingen. Utkastet til kommunikasjonsvernforordningen av 21.februar 2021 artikkel 8 nr.1 bokstav g) legger til grunn en ikke-uttømmende liste over hensyn som tilbyder plikter å vurdere. Adgangen til å benytte formålskompatibilitet som behandlingsgrunnlag må underlegges en konkret skjønnsmessig helhetsvurdering. Tilbyder må for det første vurdere om og eventuelt hvilke forbindelser det er mellom formålet med den opprinnelige behandlingen- og lagringsevnen og den tiltenkte videre behandlingen.[101] Det andre hensynet refererer seg til konteksten opplysningene opprinnelig ble samlet inn for, hvor

[100] Regjeringen, «forskning og innovasjon for næringslivet»; Sander, «Hvorfor trenger vi innovasjon?». Estudie. 28.11.2019. https://estudie.no/hvorfor-innovasjon/

[101] «Any link between the purposes for which the processing and storage capabilities have been used or the information have been collected and the purposes of the intended further processing;», jf. kommunikasjonsvernforordningen av 21.feb 2021 Artikkel 8 nr.1 bokstav g) nr. (i)

det spesielt må sees på forholdet mellom bruker og leverandør.[102] Ytterligere plikter tilbyder å vurdere arten av innsamlingen, behandlingen og lagringsmulighetene, samt modaliteter for videre behandling, særlig hvor det er en risiko for at videre behandling kan avsløre spesielle kategorier av personopplysninger i henhold til GDPR artikkel 9 første ledd.[103] De to siste hensynene pålegger tilbyder å gjennomføre en konsekvensutredning av potensielle utfall en videre behandling vil ha på bruker[104], samt vurdere eksistensen av hensiktsmessige sikkerhetstiltak som kryptering eller pseudonymisering.[105]

Bestemmelsen har klare likhetstrekk med prinsippet om formålsbegrensning etter personvernforordningen artikkel 5 nr. 1 bokstav b) og unntaket i GDPR artikkel 6 nr.4, ved at behandling av opplysninger som ikke er forenlig med det opprinnelige formålet er rettsstridig. Det følger også av kommunikasjonsvernforordningens fortalepunkt 20aa, at de rettslige rammene for tilbyders utvidede adgang til å behandle opplysninger på ekomsektorens område, må vurderes i lys av disse.[106] Som drøftet tidligere, vil GDPR fungere som generell bakgrunnsrett på området for elektronisk kommunikasjon. De nedfelte prinsippene og øvrige artikler kan dermed utgjøre sentrale tolkningsmomenter i avklaringen av hva som ligger i rettsreglene etter kommunikasjonsvernforordningen. Dette vil spesielt ha betydning kort tid etter at kommunikasjonsvernforordningen har trådt i kraft, ettersom det naturlig vil eksistere få andre rettskilder som vil belyse det materielle innholdet i reglene.

Det følger av formålsbegrensningsprinsippet i GDPR artikkel 5 nr.1 bokstav b) at personopplysninger skal samles inn for «spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene [...]». Overført til området for elektronisk kommunikasjon, er utgangspunktet at tilbyder, som samler inn og benytter seg av behandlings-og lagringsmuligheter av terminalutstyr ved bruk av

[102] «The context in which the processing and storage capabilities have been used or the information have been collected, in particular regarding the relationship between end-users concerned and the provider; », jf. kommunikasjonsvernforordning av 21.feb 2021 artikkel 8 nr.1 bokstav g) nr. (ii)
[103] «The nature the processing and stoarge capabilities or the collecting of information as well as the modalities of the indtended further processing, in particular where such intended further processing could reveal categories of data, pursuant to Article 9 or 10 i of Regulation (EU)) 2016/679;», jf. kommunikasjonsvernforordningen av 21.feb 2021 artikkel 8 nr.1 bokstav g) nr. (iii)
[104] «The possible consequences of the intended further processing for end-users;», jf. utkast til kommunikasjonsvernforordning av 21.feb 2021 artikkel 8 nr. 1 bokstav g) nr. (iv)
[105] «The existence of appropriate safeguards, such as encryption and pseudonymization», jf. kommunikasjonsvernforordning av 21.feb 2021 artikkel 8 nr. 1 bokstav g) nr. (v)
[106] Se også Lovkommentaren til personvernforordningen artikkel 5 nr.1 bokstav b) som viser til GDPR artikkel 6 nr.4 for vurderingen av uforenlig formål, jf. Bergseng, Åste Marie mfl. Lovkommentar; Personvernforordningen, Juridika.no (lest 28.03.2023); Regjeringen, «lovteknikk og lovforarbeidelser» som uttrykker at norsk rett i likhet med andre land benytter en fragmentarisk lovgivningsteknikk, hvor flere bestemmelser må ses i sammenheng for å klarlegge rettsregelens innhold.

informasjonskapsler, er ansvarlig for å fastslå et konkret formål for behandlingsprosessen. Det fastsatte formålet må samsvare med alminnelige samfunnsnormer og skal formidles på en klar og tydelig måte til bruker.[107]

Hver behandlingsaktivitet skal som hovedregel stamme fra ett individuelt formål, med det naturlige resultat at bruk av opplysninger til nye formål må ha et nytt selvstendig rettslig grunnlag. Etter kommunikasjonsvernforordningen artikkel 8 nr.1, følger det av bokstav a) til f) alternative grunnlag som hver for seg kan legitimere plasseringen av en informasjonskapsel på brukers terminalutstyr. Etter at tilbyder har hentet inn data om en bruker til det opprinnelige formålet, åpner bokstav g) i realiteten for at tilbyder kan benytte de samme opplysningene til et nytt formål. Dette innebærer at der tilbyder benyttet samtykke for første behandlingsaktivitet, kan vedkommende rettmessig viderebehandle dataene til et nytt formål uten å innhente samtykke på nytt, et såkalt avledet samtykke. Avgjørende er om den videre behandlingen er forenlig med innsamlingsformålet.

Det kan på den ene siden hevdes at behandlingsaktiviteter på bakgrunn av formålskompatibilitet i realiteten svekker samtykke som lovlig behandlingsgrunnlag. Det er naturlig at bedrifter som tradisjonelt har kommersielle formål, nærliggende vektlegger kommersielle hensyn tyngre enn brukerens personvernbehov. Ved at adgangen til viderebehandling av opplysningene er tillagt den ansvarlige enhet, svekkes brukers kontroll over opplysninger om seg. Faren for misbruk av behandlingsgrunnlaget er særlig stort i perioden før det er etablert fast praksis på området. Ytterligere vil det oppstå et behov for å avklare terskelen for hvilke behandlingsformål som er forenlig og ikke.

Sett tilbake til problematikken tatt opp av EUs personvernråd for unøyaktig klassifisering av «nødvendig» informasjonskapsler og høringssvarene til MBL og Schibsted beskrevet i punkt 2.2.6 ovenfor, vil det eksistere tilsvarende fare for feilaktig klassifisering av kompatibelt formål. Et naturlig resultat er at tilbyder viderebehandler opplysninger til andre formål i et større omfang enn det som rettmessig omfattes av det opprinnelige behandlingsformålet.

Imidlertid er beskyttelsen av opplysningene forsøkt ivaretatt ved at det i kommunikasjonsvernforordningen artikkel 8 nr.1 bokstav h) oppstilles visse kumulative minstekrav for hvordan en forenlig viderebehandling skal gjennomføres for å være berettiget.

[107] Kommunikasjonsvernforordningen av 21.feb 2021 fortalepunkt 20aaa; Bergseng, Åste Marie mfl. Lovkommentar; Personvernforordningen, Juridika.no (lest 28.03.2023).

3.3.2.1 Anonymisering og sletting

For det første må informasjonen slettes eller gjøres anonym «as soon as it is no longer needed to fulfil the purpose».[108] Bestemmelsen uttrykker således en plikt for behandlingsansvarlig til å fjerne muligheten til å kunne identifisere den fysiske eller juridiske personen. En alminnelig språklig forståelse tilsier at plikten til å fjerne identifiseringsmuligheter inntrer på det tidspunktet behandlingsaktiviteten er utført. Tidsperspektivet «as soon as [..]» er vagt, hvor ordlyden indikerer at tilbyder gis et visst handlingsrom, sett opp mot ordet straks eller umiddelbart, før plikten inntrer. Kravet til at en opplysning må slettes eller anonymiseres har paralleller til prinsippet om riktighet etter GDPR Art.5 nr.1 bokstav d), som legger til grunn at personopplysninger som er uriktige med hensyn til formålene de behandles for, uten opphold slettes eller rettes. Hensikten med anonymisering er å legge til rette for at virksomheter får økt mulighet til å skaffe verdifull informasjon ved bruk av dataanalyse, samtidig som risikoen for inngrep i den private sfære reduseres.[109]

For at det skal foreligge en reell sletting eller anonymiseringsprosess skal det altså ikke være mulig å knytte den direkte eller indirekte opplysningen til det fysiske eller juridiske individet opplysningen angår. I dette kravet ligger det en forutsetning om at slettingen eller anonymiseringsprosessen ikke kan reverseres. Det skal ikke være mulig å reidentifisere personen.[110] En personopplysning anses for å være anonymisert hvor det personentydige fjernes og tilbyder sitter igjen med aggresjoner, som for eksempel data om antall salg per dag, uke, mv.[111] At dataene verken alene eller kombinert kan knyttes til en bruker resulterer rettslig med at behandlingsaktiviteten faller utenfor personvernforordningen.

3.3.2.2 Pseudonymisering

For det andre forutsetter lovlig forenlig viderebehandling at opplysningene er begrenset til informasjon som er pseudonymisert før den kompatible behandlingsaktiviteten gjennomføres.[112] Etter definisjonen i GDPR artikkel 4 nr.5 foreligger pseudonymisering når

> «personopplysningen ikke lenger kan knyttes til en bestemt registrert uten bruk av tilleggsopplysninger, forutsatt at nevnte tilleggsopplysninger lagres atskilt og omfattes av tekniske og organisatoriske tiltak som sikrer at

[108] Kommunikasjonsvernforordning av 21.feb 2021 artikkel 8 nr.1 bokstav h) nr. i)
[109] Datatilsynet, «anonymisering av personopplysninger» s. 4-6.
[110] Datatilsynet, «anonymisering av personopplysninger» s.6
[111] Svensson, Anders og Skogheim, Jan Ove, «Anonymisering og pseudonymisering». Gdprcontrol.no. 08.01.2023. https://gdprcontrol.no/anonymisering_og_pseudonymisering/
[112] Kommunikasjonsvernforordningen av 21.feb 2021 artikkel 8 nr.1 bokstav h) nr. ii)

personopplysningen ikke kan knyttes til en identifisert eller identifiserbar fysisk person,»

I motsetning til anonymisering forblir den pseudonymiserte opplysningen en personopplysning etter GDPR. En pseudonymisert opplysning innebærer at det fortsatt er mulig å spore en opplysning tilbake til en fysisk eller juridisk person. Pseudonymisering gir dermed et lavere beskyttelsesnivå enn ved full anonymisering. Behovet for å beholde en personopplysning kan være ønskelig til for eksempel å analysere de ulike transaksjonene den enkelte kunden foretar. De direkte identifiserende parameterne omdannes til unike identifikatorer hvor tilbyder for eksempel sitter igjen med alder, kjønn, yrke, nasjonalitet, mv.[113] Ettersom lovreguleringen på ekomområdet tar sikte på å likestille fysiske og juridiske personer må kravene *mutatis mutandis* gjelde tilsvarende for juridiske personer. Avgjørende er at det er gjort tiltak for at den aktuelle opplysningen ikke kan knyttes direkte til vedkommende uten å benytte tilleggsinformasjon.

Det kan imidlertid stilles spørsmål om hvilken type informasjon som skal underlegges en pseudonymisering, sett i forhold til hva som faller inn under definisjonen av metadata. Metadata defineres som «informasjon som beskriver annen informasjon, altså data om data», og som innen IT «ofte vil være tilleggsinformasjon i elektroniske filformater».[114] En alminnelig språklig forståelse tilsier at metadata er pseudonymisert i sin natur, med den rettslig konsekvens at metadata kvalifiserer som en opplysning som nyter vern på området for elektronisk kommunikasjon.

I tråd med GDPR artikkel 5 nr.2 er det behandlingsansvarlig som er ansvarlig for og skal kunne påvise at de grunnleggende prinsippene om personvern etter nr.1 overholdes. Lagt til grunn personvernforordningens overføringsverdi, vil tilbyder som har hentet inn og lagret opplysninger fra en bruker gjennom bruk av en informasjonskapsel, ha tilsvarende bevisbyrde. Det er tilbyder som etter en objektiv vurdering må finne det nødvendig å viderebehandle opplysningene. Innebygd i prinsippene om dataminimering og lagringsbegrensning, forutsettes det at tilbyder må foreta en konkret helhetsvurdering av om det overhodet er nødvendig å behandle en opplysning, hvilke opplysninger som er nødvendig for å nå det fastsatte formålet, samt om det etter behandlingens art, omfang og varighet tilsier

[113] Datatilsynet, «anonymisering av personopplysninger» s.6; Svensson, Anders og Skogheim, Jan Ove, «Anonymisering og pseudonymisering». Gdprcontrol.no. 08.01.2023. https://gdprcontrol.no/anonymisering_og_pseudonymisering/
[114] Store norske leksikon, «metadata», av Aud Gjersdal og Tom Heine Nätt.10.03.2023. https://snl.no/metadata

at behandlingsaktiviteten er berettiget. En opplysning skal på et tidspunkt slettes, hvor pseudonymisering er et teknisk og organisatorisk tiltak som kan begrunne at en ytterligere lagringsperiode likevel kan gi et visst beskyttelsesnivå.[115]

I takt med den teknologiske utviklingen skapes det stadig nye analyseverktøy, som kombinert med den tilfallende høye mengden av offentlig tilgjengelig informasjon, utgjør en trussel for anonymiserings- og pseudonymiseringsprosessene. Avgjørende er således om den konkrete tilbyderen, etter de faktiske omstendighetene, har foretatt en tilstrekkelig risikovurdering for reidentifisering på bakgrunn av de til enhver tid eksisterende analysemidlene.

3.3.2.3 Bestemmende for arten eller egenskapene

Det siste minimumskravet i forslagets Artikkel 8 nr.1 bokstav h) viser til at tilbyder ikke forenlig kan viderebehandle informasjon som kan brukes til å bestemme arten eller egenskapene til en bruker, eller å bygge en profil av en bruker. [116] «Profilering» er legaldefinert i GDPR Artikkel 4 nr.4 som

> «enhver form for automatisert behandling av personopplysninger som innebærer å bruke personopplysninger for å vurdere visse personlige aspekter knyttet til en fysisk person, særlig for å analysere eller forutsi aspekter som gjelder nevnte fysiske persons arbeidsprestasjoner, økonomiske situasjon, helse, personlige preferanser, interesser, pålitelighet, atferd, plassering eller bevegelser.»

En behandling vil for eksempel ikke være forenlig i situasjoner der en bruker legger inn søknader knyttet til kreditt eller ansettelser, eller hvor tilbyder henter inn opplysninger som alder, hvor ofte en bruker bytter jobb, om vedkommende har barn eller lignende for å bestemme om bruker får bevilgning eller ikke. Slike beslutninger har nærliggende stor innvirkning på brukerens liv og taler for at slike behandlinger må gjennomføres med varsomhet.

3.4 Avsluttende bemerkninger til kommunikasjonsvernforordningen

Det er på det rene at Kommunal- og distriktsdepartementet vurderer forslaget som EØS-relevant.[117] En eventuell implementering av kommunikasjonsvernforordningen vil bidra til å

[115] Eva Jarbakk, norsk lovkommentar; GDPR artikkel 5 nr.1 bokstav b), c) og e), Karnov. (Lest 01.05.2023)
[116] Kommunikasjonsvernforordning av 21.feb 2021 artikkel 8 nr.1 bokstav h) nr. iii)
[117] Regjeringen, «Forslag til kommunikasjonsvernforordningen»

klargjøre ytterligere hva som skal til for at en tilbyder rettmessig kan behandle opplysninger ved bruk av informasjonskapsler, både på bakgrunn av samtykke som behandlingsgrunnlag og etter andre, alternative, behandlingsgrunnlag. Ved at cookie-bestemmelsen nedfelles i en forordning begrenses medlemsstatenes adgang til å bestemme form og midler for gjennomføringen og det gis mindre rom for nasjonale tilpasninger. Innlemmelsen av kommunikasjonsvernforordningen vil styrke harmoniseringen og en uniform tolkning av cookie-bestemmelsen. Et klarere regelverk rundt hvilke rettigheter og plikter som faktisk gjelder vil bidra til at forskjellene mellom når og hvilke rettsvirkninger som inntrer ved brudd i de ulike medlemslandene reduseres. Moderniseringsprosessen vil i større grad bidra til imøtekommelse av de nye teknologiske utviklingene, stimulere til næringsutvikling og innovasjon, og sikre et reelt og effektivt personvern på området for elektronisk kommunikasjon.

4 Avslutning

Den rettslige analysen kan tas til inntekt for at det i realiteten ikke eksisterer en tilstrekkelig harmonisering av gjennomføringen av direktiv 2002/58/EC artikkel 5 (3) i medlemsstatene. Uklarhetene i direktivet har ført til en inkonsekvent og utilstrekkelig effektiv beskyttelse av personvern og konfidensialitet i forholdet til elektronisk kommunikasjon. Området for elektronisk kommunikasjon er i rask teknisk og markedsmessig utvikling, og det er skjedd store digitale forbedringer innen kommunikasjons- og informasjonsteknologien siden direktivet først trådte i kraft.

Slik forslaget til ny ekomlov, rapporten fra arbeidsgruppen opprettet av EUs personvernråd, rettspraksis fra EU-domstolen og øvrige avgjørelser fra ulike europeiske datatilsyn viser, legger lovgiver og tilsyn en streng norm for hvordan en tilbyder rettmessig kan behandle opplysninger på bakgrunn av et samtykke gitt av brukeren ved bruk av informasjonskapsler. Dette har medført en rekke vanskeligheter rundt praktiseringen av cookie-bestemmelsen.

Samlet sett viser tilveksten av nye tilbydere, økende samtykkestrømmer, den tekniske og manipulerende utformingen av informasjonskapsler og framveksten av samtykketrøtthet, at eksisterende rettslig rammeverk ikke er tilstrekkelig.

For å sikre at brukere har kontroll over opplysninger om seg, samtidig som lovreguleringen legger til rette for verdiskapning og innovasjon for næringsvirksomheter, er det et behov for nasjonale og internasjonale endringer. Selv om EUs medlemsland enda ikke har kommet til enighet om ny kommunikasjonsvernforordning, er det satt igang en moderniseringsprosess. Fremmet kommunikasjonsvernforordning tar sikte på å sikre en mer harmonisert anvendelse av cookie-bestemmelsen, med påfølgende formål å styrke sikkerheten for bruk av elektronisk kommunikasjon. I mellomtiden er det ventet at ny ekomlov skal tre i kraft etter norsk rett. Endelig utforming av oppdatert nasjonal og internasjonal regulering imøteses. Det er å håpe at ny regulering nettopp sikrer brukerne større kontroll av opplysninger om seg samtidig som regelverket legger til rette for næringsutvikling og innovasjon.

Kilder:

Juridiske kilder:

Datatilsynet	Datatilsynet, «Datatilsynet sender brev til statsråden om cookie-regelverket». Publisert 14.02.2022. https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/datatilsynet-sender-brev-til-statsraden-om-cookie-regelverket/
Datatilsynet	Datatilsynet, «Vedrørende forslag til ny ekomlov § 3-7 – Bruk av informasjonskapsler mv.» Sendt 08.02.2022. https://www.datatilsynet.no/contentassets/c03cd5c5026547e7b8d7230759de222b/vedrorende-forslag-til-ny-ekomlov--3-7---bruk-av-informasjonskapsler-mv.pdf
EDPB	European Data Protection Board, «Letters». Sendt 18.01.2022. https://edpb.europa.eu/system/files/2022-01/edpb_letter_on_cookie_consent_out2022-0003.pdf
EDPB, Cookie Banner Taskforce (Arbeidsgruppen)	European Data Protection Board, «Report of the work undertaken by the Cookie Banner Taskforce Adopted on 17 January 2023", 18.01.2023. https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf
Ekomloven	Lov av 4.Juli 2003 nr.83 om elektronisk kommunikasjon (ekomloven)
EMK	Convention for the Protection of Human Rights and Fundamental Freedoms, Roma, 4. November

	1950. (Den europeiske menneskerettighetskonvensjonen, EMK)
Elektronisk Kommunikasjonskodedirektiv	Directive of the European Parliament and of the Council (EU) 2018/1972 of 18 December 2018 establishing the European Electronic Communcations Code
EØS-avtalen	EØS-avtalen av 02.mai 1992 nr.1 Protokoll 1 om gjennomgående tilpasning
EØS-loven	Lov av 27.november 1992 nr.109 om gjennomføring i norsk rett av hoveddel i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven)
ePrivacy-direktivet (ePD)	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, ePrivacy-direktivet)
European Commission	European Commission, «Proposal for an ePrivacy Regulation». Sist oppdatert 7.Juni 2022. https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation
European Parliament	European Parliament, «Proposal for a regulation on privacy and electronic communication». Sist oppdatert 20.02.2023. https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform
Forslag ny ekomlov	Kommunal- og distriktsdepartementet, Høringsnotat; *Forslag til ny lov om elektronisk*

	kommunikasjon, § 3-7, regjeringen.no. https://www.regjeringen.no/no/dokumenter/horing-forslag-til-ny-ekomlov-ny-ekomforskrift-og-endringer-i-nummerforskriften/id2864853/?expand=horingsnotater
Grunnloven	Lov av 17.Mai 1814 Kongeriket Norges Grunnlov (Grl.)
Kommunikasjonsvernforordningen (ePR)	Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58(EC (Regulation on Privacy and Electronic Communication). https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf
Mediebedriftenes Landsforening	Øgrey, Randi S, «Høringsuttalelse om forslag til ny ekomlov». Mediebedriftenes Landsforening. Datert 15.10.2021. https://www.regjeringen.no/no/dokumenter/horing-forslag-til-ny-ekomlov-ny-ekomforskrift-og-endringer-i-nummerforskriften/id2864853/?uid=ef370710-421c-4907-a7c5-97518f158029
Merknader ny ekomlov	Kommunal- og distriktsdepartementet, Høringsnotat; *Forslag til merknader til ny lov om elektronisk kommunikasjon*, § 3-7, regjeringen.no. https://www.regjeringen.no/no/dokumenter/horing-forslag-til-ny-ekomlov-ny-ekomforskrift-og-endringer-i-nummerforskriften/id2864853/?expand=horingsnotater

ODA	Avtale av 2. Mai 1992 nr.2 mellom EFTA-statene om opprettelse av et overvåkningsorgan og en domstol, med protokollene 1 – 7 (ODA)
Personvernforordningen (GDPR)	Europaparlaments- og rådsfordning (EU) 2016/679 av 27.April 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt oppheving av direktiv 95/46/EF (GDPR)
Prop.69 L (2012-2013)	Endringer i ekomloven
Regjeringen	Regjeringen, «Forslag til kommunikasjonsvernforordning». https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2017/juni/forslag-til-kommunikasjonsvernforordning/id2555751/
Schibsted	Næss, Ingrid og Breen, Simen, «Høringsuttalelse – Forslag til ny ekomlov, ny ekomforskrift og endringer i nummerforskriften». Schibsted. Datert 15.10.2021. https://www.regjeringen.no/no/dokumenter/horing-forslag-til-ny-ekomlov-ny-ekomforskrift-og-endringer-i-nummerforskriften/id2864853/?uid=51091328-777d-4be7-b60e-dc613e12697b
TEU	Treaty on European Union (TEU), OJ C 202. (EU-traktaten)
TEUV	Treaty on the Functioning of the European Union (TEUV), OJ C 202. (Romatraktaten)

Rettspraksis:

C-61/19 (Orange Romania) Dom av 11.November 2020 [SC], *Orange Romania*, C-61/19, ECLI:EU:C:2020:901

C-673/17 (Planet49) Dom av 1. Oktober 2019 [GC], *Planet49*, C-673/17, ECLI:EU:C:2019:801

Rt.2000 s.1811 P (Finanger I)

SAN-2021-023 Franske Datatilsynet (CNIL). 2021. Engelsk versjon, Hentet fra: https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_the_restricted_committee_no._san-2021-023_of_31_december_2021_concerning_google_llc_and_google_ireland_limited.pdf

SAN-2021-024 Franske Datatilsynet (CNIL). Engelsk versjon, hentet fra: https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_the_restricted_committee_no._san-2021-024_of_31_december_2021_concerning_facebook_ireland_limited.pdf

Litteratur:

Adjust Adjust, «What is over-the-top (OTT)?». https://www.adjust.com/glossary/ott-over-the-top#what-does-ott-mean

Annonse Store norske leksikon. «Annonse». Roger Phil. 30.11.2020. https://snl.no/annonse

Annual Report 2022 Data Protection Commision, «Annual Report 2022», Hentet 17.04.2023. https://www.dataprotection.ie/sites/default/files/u

ploads/2023-03/DPC%20AR%20English_web.pdf

Anonymisering og pseudonymisering — Svensson, Anders og Skogheim, Jan Ove, «anonymisering og pseudonymisering», GDPRControl.no. Publisert 08.01.2023. https://gdprcontrol.no/anonymisering_og_pseudonymisering/

Anonymisering av personopplysninger — Datatilsynet, «Anonymisering av personopplysninger». 2015. https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/veiledere/anonymisering-veileder-041115.pdf

Berettiget interesse — Eva Jarbakk, Karnov lovkommentar, personopplysningsloven artikkel 6 nr.1 bokstav f). 02.09.2021. Lovdata.no. https://lovdata.no/pro/#document/NL/lov/2018-06-15-38/gdpr/a6

Bergseng mfl — Bergsen, Åste Marie, Rønnevik, Cecilie, Skorstad, Jørgen og Pellerud, Marius Engh. Lovkommentar; personvernforordningen. Artikkel 5. «Prinsipper for behandling av personopplysninger». Juridika.no. Lest 28.03.2023. https://juridika.no/no/lov/2016-04-27-679/§5/kommentar?q=GDPR&fbclid=IwAR2_H_Wzunjpl1tiZLc-aV115xYhhSZAWHXT92iUkG6OZBb0aYDrMUOg73w

CMS — CMS, «Tracking under the e-privacy regulation». Lest 20.03.2023. Hentet fra:

https://cms.law/en/deu/insight/e-privacy/tracking-under-the-e-privacy-regulation

CookieInformation — CookieInformation, «what are dark patterns in cookie banners?» Publisert 22.08.2022. https://cookieinformation.com/resources/blog/what-are-dark-patterns-in-cookie-banners/

CookieInformation — CookieInformation, Nordic Report-April 2023; «Cookie Compliance in the Nordics». Frigitt April 2023.

Datatilsynet — Datatilsynet, «Cookies og informasjonskapsler». Publisert 20.06.2018. https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/cookies/

Datatilsynet — Datatilsynet, «Hva er personvern». Publisert 17.07.2019. https://www.datatilsynet.no/rettigheter-og-plikter/hva-er-personvern/

Datatilsynet — Datatilsynet, «Sporing i det offentlige rom». Publisert 26.09.2016. https://www.datatilsynet.no/personvern-pa-ulike-omrader/overvaking-og-sporing/sporing-i-det-offentlige-rom/

Ekkokammer — Wolff-Hansen, E. S., Overland, J. (2021, 10. desember). Digitale og sosiale medier i offentligheten. NDLA. https://ndla.no/article/34509

Estudie — Sander, Kjetil. «Hvorfor trenger vi innovasjon?». Estudie. Publisert 28.11.2019. https://estudie.no/hvorfor-innovasjon/

European Parliament — European Parliament, «Interinstitutional negotiations ».

https://www.europarl.europa.eu/olp/en/interinstitutional-negotiations

European Union — European Union, «Court of Justice of the European Union (CJEU)». https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/court-justice-european-union-cjeu_en

Fredriksen mfl. — Fredriksen, Halvard Haukeland, Gjermund, Mathisen. *EØS-rett*. Bergen: Fagbokforlaget, 2022

HELP Forsikring — HELP Forsikring, «Informasjonskapsler (cookies)». https://help.no/personvern/informasjonskapsler-cookies

ICO — Information Commissioner`s Office. «Cookies and similar technologies». Lest 12.05.2023. https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/

Innflytelse — Store Norske Leksikon, «Innflytelse». Ole T. Berg.19.02.2021. https://snl.no/innflytelse

Mediebedriftenes Landsforening — Mediebedriftene, «Våre Medlemmer». Hentet 14.04.2023. https://www.mediebedriftene.no/om-mbl/vare-medlemmer/

Meta — Gjessing, Marianne, «Historisk dom: Meta får ikke bruke persondata til målrettet annonsering». Digi.no. 05.01.2023. https://www.digi.no/artikler/historisk-dom-meta-far-ikke-bruke-persondata-til-malrettet-annonsering/524798

Meta	Vågen, kjell, Dyrhovden, Sindre og Biermann, Miriam Maria. «Skyhøye gdpr-bøter til Meta for ulovlig målrettet markedsføring». Clp.no. 30.01.2023. https://clp.no/skyhoye-gdpr-boter-til-meta-for-ulovlig-malrettet-markedsforing/
Metadata	Stor Norske Leksikon, «metadata». Aud Gjersdal og Tom Heine Nätt. 10.10.2023. https://snl.no/metadata
NOYB	noyb, «Our Detailed Concept». https://noyb.eu/en/our-detailed-concept
Regjeringen	Regjeringen, «Datatilsynet». https://www.regjeringen.no/no/dep/kdd/org/etater-og-virksomheter-under-kommunal--og-distriktsdepartementet/underliggende-etater/datatilsynet/id373618/
Regjeringen	Regjeringen, «forskning og innovasjon for næringslivet». https://www.regjeringen.no/no/tema/naringsliv/forskning-og-innovasjon/id526417/
Regjeringen	Regjeringen, «Lovteknikk og lovforberedelse». https://www.regjeringen.no/globalassets/upload/kilde/jd/bro/2000/0003/ddd/pdfv/108138-lovteknikkboka.pdf?fbclid=IwAR0JLWnbWJwT0USyNtMqabaQIGrjzFkDWeGc2sBSzBpMHoIYoAadnqTveH0
Regjeringen	Regjeringen, «Nasjonal kommunikasjonsmyndighet/Nasjonal Kommunikasjonsmyndigheit (Nkom)». https://www.regjeringen.no/no/dep/kdd/org/etater-og-virksomheter-under-kommunal--og-

	distriktsdepartementet/underliggende-etater/nkom/id443414/
Reklame	Store norske leksikon. «Reklame». Birger M. Vikøren, Roger Phil og Even Ruud. 12.01.2023. https://snl.no/reklame
Strategem	Romarheim, Anders, «Digital påvirkning som eksistensiell trussel», strategem.no. https://www.stratagem.no/digital-pavirkning-som-eksistensiell-trussel/
Tilburg Law review	Naithani, Paarth, «Curtailing the Cookie Monster through Data Protection by Default», Tilburg Law review. Publisert 17.02.2023. https://tilburglawreview.com/articles/10.5334/tilr.311?fbclid=IwAR2LmVHpPTAePV9dwP_cmXLct4OD55JQYCy1xkO01l9veHM6R7Axn7OIv6I
TV 2	TV 2, «Bruk av cookies på TV 2s nettsteder». https://www.tv2.no/informasjonskapsler/