

Just Balstad

**DIGITALE MELLOMLEDDS ANSVAR FOR
VIDEREFORMIDLING AV YTRINGER**

E-HANDELSDIREKTIVET ART. 12-14

Henvendelser om denne bok kan gjøres til:

Institutt for rettsinformatikk
Postboks 6706 St. Olavs plass
0130 Oslo
Tlf. 22 85 01 01
www.jus.uio.no/iri/

ISBN 82-7226-052-2
ISSN 0806-1912

unipubskriftserier

Utgitt i samarbeid med Unipub Forlag
Denne boken går inn i universitets- og høyskolerådets skriftserie
Trykk: GCSM AS
Omslagsdesign Kitty Ensby

Institutt for rettsinformatikks utgivelser i sekriftserien Complex er støttet av:
Advokatfirmaet Selmer DA
Wikborg Rein & Co

FORORD

Arbeidet med spesialoppgaven begynte tidlig på høsten 2000. Grunnen til at jeg valgte å skrive om rettsregler som regulerer virksomheten til digitale mellomledd¹ på Internett er todelt. For det første oppdaget jeg i et engasjement som bestod i å kartlegge det juridiske landskapet for en internettaktør at det var et stort behov for å få klarlagt regelverket om lagring og videreformidling av informasjon for andre – et problem som særlig har aktualitet i forbindelse med særlig det siste tiårets fremvekst av elektronisk handel og forretningsdrift.²

For det annet var jeg klar over at EU-direktivet om elektronisk handel, som ble vedtatt 8. juni 2000, i art. 12-14, oppstiller regler om ansvar for videreformidling av informasjon. Disse reguleringene har til formål å løse mange av de spørsmål som dukker opp i forbindelse med virksomhet som videreformidler av informasjon over Internett.

På grunn av behovet for en rettslig kartlegging og klargjøring falt det hensiktsmessig å analysere direktivets regler fra en hovedsakelig praktisk synsvinkel. Som følge av denne tilnærmingsmåten er et hovedpoeng i oppgaven å prøve hvorvidt en rekke konkrete virksomheter, som så langt mulig har både praktisk og prinsipiell interesse, faller inn under anvendelsesområdet for e-handelsdirektivets art. 12-14. Et annet hovedpoeng er å undersøke hvorvidt disse virksomhetene faller inn under bestemmelsenes hovedregel om ansvarsfrihet.

Fordelen med tilnærmingsmåten er at den gir anledning til en oppsplitting og en nærmere analyse av de vanlige rollene som mellomledd på Internett innehar i markedet. Mitt håp er at dette kan tjene til nødvendige rettslige avklaringer for aktører som driver virksomhet som digitalt mellomledd på Internett. Jeg håper også at sontringene mellom de forskjellige rollene som mellomleddene påtar seg kan bidra til enkelte prinsipielle avklaringer i forhold til det ansvarsregimet som oppstilles i art. 12-14.

¹ Begrepet er hentet fra boken *elektronisk handel*, Hellebust mfl. (2000 s. 33 flg.). Når jeg i det følgende alternerer mellom ordene «mellomledd» og «digitale mellomledd» legger jeg ingen meningsforskjell i dette.

² Definisjon av elektronisk handel og forretningsdrift er i følge St. meld nr. 41, boks 1.2 under punkt 1.3.2 «...alle former for kommersielle transaksjoner og forretningsvirksomhet over elektroniske nett. Transaksjonene må være knyttet til bestilling, betaling og levering av fysiske varer og tjenester, men kan også omfatte overføring av digitaliserte varer og tilgang til tjenester».

Ulempen med en slik tilnærmingssmåte er at fremstillingen kan virke noe repeterende. Dette er fordi en rekke av vilkårene man må drøfte i art. 12-14 er like uansett hvilken type virksomhet man vurderer dem opp imot. Hver gang man vurderer hvorvidt e-handelsdirektivets regler er anvendelige på en bestemt virksomhet må man derfor drøfte seg gjennom likelydende vilkår. F.eks. må man ved tolkningen av både art. 12, 13 og 14 drøfte seg gjennom hvorvidt den aktuelle virksomhet utgjør en informasjonssamfunnstjeneste i e-handelsdirektivets forstand.

På den annen side kan den fremstillingsmåten jeg har valgt være å foretrekke for en rettsanvender som bruker avhandlingen som et praktisk oppslagsverk når hans skal analysere reglene i e-handelsdirektivet art. 12-14. Av denne grunn kan jeg ikke se at noen av drøftelsene til tross for gjentakelsene er overflødige.

Jeg har under enhver omstendighet forsøkt å avhjelpe det fremstillingsmessige problemet ved felles tolkninger av visse nøkkelbegreper i art. 12-14. På denne måten holdes gjentakelsene på et minimalt nivå.

Spørsmålet om ansvar for digitale mellomledd er en del av et rettsområde i rivende utvikling. På noen områder er det derfor nødvendig med en løpende oppdatering av fremstillingen. Mot slutten av skrivingen har det imidlertid vært nødvendig å bruke tiden til ferdigstilling av oppgaven. Fremstillingen er derfor rettslig àjourført frem til onsdag 11. april 2001. Etter denne datoen er tiden hovedsakelig brukt til korrekturlesning og innarbeiding av formelle krav.

Jeg ønsker å takke alle personene i miljøet på Institutt for Rettsinformatick for faglige og sosiale innspill. Jeg retter særlig en takk til min veileder, Professor dr. juris Jon Bing, for den mottagelsen jeg har fått på Instituttet, og for den inspirerende faglige dialogen han har deltatt i under arbeidet med oppgaven.

INNHOOLD

Forord.....	3
-------------	---

Innhold	5
---------------	---

1. Introduksjon	11
1.1 Innledning og hensyn	11
1.2 Tema og problemstillinger i oppgaven	12
1.3 Hvordan oppgaven er bygget opp	13
1.4 Presisering og avgrensning av oppgaven	14
1.5 Forklaring av noen begreper	18
1.6 Hvilke roller digitale mellomledd påtar seg	19
1.6.1 Innledning	19
1.6.2 Aksessleverandør	19
1.6.3 Nettverksoperatør	20
1.6.4 Proxy serving, proxy caching, mirror caching	21
1.6.5 Host service provider	22
1.6.6 Bulletin board operatør	22
1.6.7 Søkemotorer	23
1.6.8 Portaler	24
1.7 Hvilke regler kan tenkes krenket ved de forskjellige typer mellommannsvirksomhet?	24
1.7.1 Opphavsrettslige regler	25
1.7.2 Personvernrettslige regler	25
1.7.3 Strafferettslige regler	25
1.7.4 Varemerkerettslige regler	26
1.7.5 Kjøpsrettslige regler	26
1.7.6 Forbrukervernregler	26
1.7.7 Kan reglene på andre rettsområder krenkes?	27
1.8 Rettskildesituasjonen	27
1.9 Metoden som brukes i oppgaven	28
1.10 Finnes det norsk lovregulering av digitale mellomledds ansvar for videreformidling av medkontrahentens ytringer?	29
2. Ansvarsreglene i e-handelsdirektivets art. 12-14	33
2.1 Innledning	33
2.2 En oversikt over ansvarsregimet som oppstilles i e- handelsdirektivets art. 12-14	33

2.2.1	Presisering og avgrensning av ansvarsreglene i art. 12-14	33
2.2.2	For hvilke av tjenestemottagerens handlinger er digitale mellomledd ansvarsfrie etter e-handelsdirektivets art. 12-14?...	36
2.2.3	Andre retningslinjer for gjennomføringen av e-handelsdirektivet i norsk rett.....	37
2.3	Fellesfortolkninger av begrep i art. 12-14	37
2.3.1	Innledning	37
2.3.2	Tolkning av begrepet «Information Society service»?	37
2.3.3	Tolkning av begrepet «recipient of the service»	42
2.3.4	Tolkning av e-handelsdirektivets begrep «service provider»?	42
2.3.5	Tolkning av e-handelsdirektivets begrep «communication network»	43
2.4	Spørsmål om ansvarsfrihet for den virksomhet som i punkt 1.6.2 er beskrevet som aksessleverandør	43
2.4.1	Hjemmel	43
2.4.2	Omfattes levering av aksess, slik den er beskrevet i punkt 1.6.2, av e-handelsdirektivets art. 12?	44
2.4.3	Oppfyller aksessleverandøren kravene til å være en «mere conduit» i forhold til den informasjonen som er skaffet til veie av hans medkontrahent dersom han forhåndsprogrammerer slik at hans hjemmeside automatisk blir gjort til tjenestemottagerens startside, jfr. punkt 1.6.2?	45
2.4.4	Oppfyller aksessleverandøren kravene til å være en «mere conduit» dersom han forhåndsprogrammerer slik at reklamebannere/linker til hans samarbeidspartnere/annonsører blir en del av grensesnittet mot Internett for brukerne av tjenesten, jfr. punkt 1.6.2?	46
2.4.5	Oppfyller aksessleverandøren kravene til å være en «mere conduit» dersom han installerer et teknologisk filter som siler ut ulovlig eller krenkende informasjon som passerer gjennom hans server?	49
2.5	Spørsmål om ansvarsfrihet for den virksomhet som det i punkt 1.6.3 er beskrevet at nettverksoperatøren driver	50
2.5.1	Hjemmel	50
2.5.2	Er nettverksoperatørens virksomhet, slik den er beskrevet i punkt 1.6.3, omfattet av e-handelsdirektivets art. 12?	51

2.5.3	<i>Oppfyller nettverksleverandøren kravene til å være «mere conduit» der det under overføring av opphavsrettslig beskyttet materiale skjer eksemplarframstillinger som er egnet til å krenke en opphavsmanns rett?.....</i>	<i>52</i>
2.6	<i>Spørsmål om ansvarsfrihet for det som i punkt 1.6.4 er beskrevet som proxy serving/proxy caching og mirror caching.....</i>	<i>55</i>
2.6.1	<i>Hjemmel</i>	<i>55</i>
2.6.2	<i>Er den virksomhet som i punkt 1.6.4 er beskrevet som proxy caching omfattet av art 13 i e-handelsdirektivet?</i>	<i>56</i>
2.6.3	<i>Er den virksomhet som i punkt 1.6.4 er beskrevet som mirror caching omfattet av anvendelsesområdet for art 13?</i>	<i>57</i>
2.6.4	<i>Er kravene for ansvarsfrihet oppfylt dersom tilbyderer av proxy caching-tjenester installerer et teknologisk filter som siler ut innhold som er ulovlig eller krenkende?.....</i>	<i>58</i>
2.6.5	<i>Er kravene til ansvarsfrihet i art. 13, nr. 1 oppfylt dersom tilbyderer av proxy caching-tjenester ikke fjerner eller stenger tilgangen til en nettside som han vet inneholder ulovlig eller krenkende informasjon?</i>	<i>61</i>
2.7	<i>Spørsmål om ansvarsfrihet for den virksomhet som i punkt 1.6.5 beskrives som host service provider</i>	<i>63</i>
2.7.1	<i>Hjemmel</i>	<i>63</i>
2.7.2	<i>Er den virksomhet som i punkt 1.6.5 er beskrevet som host service provider omfattet av art 14 i e-handelsdirektivet?</i>	<i>64</i>
2.7.3	<i>Er vilkårene i art. 14, nr. 1, litra (a) for frihet fra strafferettslig ansvar oppfylt dersom host service provideren får en uspesifisert melding om at det er lagret ulovlig eller krenkende informasjon på hans servere og han ikke omgående fjerner eller stenger tilgang til denne?</i>	<i>66</i>
2.7.4	<i>Er vilkårene for frihet fra sivilrettslig ansvar i art. 14, nr. 1, litra (a) oppfylt dersom host service provideren får en uspesifisert melding om at det er lagret ulovlig eller krenkende informasjon på hans servere og han ikke omgående fjerner eller hindrer tilgang til denne?</i>	<i>68</i>

2.7.5	Er vilkårene for frihet fra strafferettslig ansvar i art. 14, nr. 1, litra (a) oppfylt for en host service provider som også utvikler de programapplikasjoner som lagres på hans server dersom han videreformidler krenkende eller ulovlig informasjon eller aktivitet som ligger implementert i den applikasjon som han har utviklet, etter at rettighetene til programapplikasjonen er overdratt til tjenestemottageren for hostingtjenestene, og han ikke fjerner eller stenger tilgangen til informasjonen?	70
2.7.6	Er kravene for ansvarsfrihet i e-handelsdirektivets art. 14 oppfylt for en host service provider som innfører rutiner for overvåkning og kontroll av det materialet som blir tilveieskaffet av tjenestemottageren for hostingtjenestene? ...	72
2.7.7	Er vilkårene for ansvarsfrihet i henhold til art. 14, nr. 1, litra (a) oppfylt dersom en host service provider ikke stenger tilgangen til informasjon, hvis lovlighet er omtvistet, og som han lagrer, etter at han har fått en melding som angir hvor informasjonen er å finne og på hvilket grunnlag den angivelig er ulovlig, og det senere viser seg at det var riktig å bygge på meldingsavgiverens rettsoppfatning?.....	75
2.8	Spørsmål om ansvarsfrihet for den virksomhet som i punkt 1.6.6 er beskrevet som bulletin board operator	76
2.8.1	Hjemmel	76
2.8.2	Er den virksomhet som i punkt 1.6.6 er beskrevet som bulletin board operator omfattet av e-handelsdirektivets art. 14 når tjenesteyteren eier serveren som tjenestemottageren bruker?	76
2.8.3	Er den virksomhet som i punkt 1.6.6 er beskrevet som bulletin board operator omfattet av e-handelsdirektivets art. 14 når tjenesteyteren ikke selv besitter serveren han bruker for å lagre informasjon og tilgjengeliggjøre sine tjenester?	80
2.8.4	Er vilkårene for ansvarsfrihet i art. 14 oppfylt dersom en bulletin board operatør videreformidler en av sine arbeidstakers ulovlige eller krenkende ytringer når disse er fremsatt i arbeidstiden, men ikke har noen sammenheng med de oppgaver arbeidstakeren er satt til å gjøre, og arbeidstakeren er tjenestemottaker for arbeidsgiverens bulletin board-tjenester?.....	82

2.9 Spørsmål om ansvarsfrihet for de andre typer digitale mellomledd som er beskrevet i punkt 1.6	85
2.9.1 <i>Er virksomheten som det i punkt 1.6.7 er beskrevet at en operatør av en søkemotor driver omfattet av anvendelsesområdet for art. 12-14 i e-handelsdirektivet?</i>	85
2.9.2 <i>Er virksomheten som i punkt 1.6.8 er beskrevet som portalvirksomhet omfattet av anvendelsesområdet for art. 12-14 i e-handelsdirektivet?</i>	86
3. Rettspolitiske vurderinger på bakgrunn av ansvarsregimet i e-handelsdirektivets art. 12-14	87
3.1 Innledning	87
3.2 I hvilken grad bør digitale mellomledd risikere ansvar for formidling av informasjon sett på bakgrunn av samfunnsinteresser som åpne kommunikasjonskanaler og ytringsfrihet?	88
3.2.1 Innledning	88
3.2.2 «Den dype lomme»	88
3.2.3 Muligheten for teknologisk kontroll av informasjon	89
3.2.4 Den krenkedes interesser	91
3.2.5 Medvirkningsbetraktninger	91
3.2.6 Aktsomhetsbetraktninger	92
3.2.7 Ytringsfriheten	93
3.2.8 Økonomisk vekst	94
3.2.9 Avveining og konklusjon	95
3.3 Horisontal eller vertikal regulering av ansvarsfrihet for digitale mellomledd?	95
3.4 E-handelsdirektivets risikofordeling mellom digitale mellomledd omfattet av art. 14, rettighetshaverne til den informasjon som lagres og mellomleddenes tjenestemottagere	97
3.4.1 Innledning	97
3.4.2 Kravet til kunnskap om ulovlig eller krenkende innhold i art. 14 nr. 1, litra (a) kontra fraværet av en generell undersøkelsesplikt i art. 15	98
3.4.3 Kravet til kunnskap om ulovlig eller krenkende innhold i art. 14 nr. 1, litra (a) kontra implementeringen av teknologiske kontroll-, og utsilingsfunksjoner	99
3.4.4 Kravet til kunnskap om ulovlig eller krenkende innhold i art. 14 nr. 1, litra (a) kontra underrettelser fra tredjemann	101
3.4.5 Kravet til kunnskap i art. 14 nr. 1, litra (a) kontra underretning fra et ytre, uavhengig organ	104

3.5 Forholdet til digitale mellomledd som ikke er omfattet av e-handelsdirektivets art. 12-14	105
4. Oppsummering og konklusjon	107
Litteraturliste.....	109
Elektroniske dokumenter	109
Bøker	109
Artikler	110
Offentlige publikasjoner	110
Internasjonal lovgivning, traktater og avtaler.....	111
Rettsavgjørelser	111
Vedlegg 1 Enkel oversikt over de internettvirksomheter som er beskrevet i oppgaven.....	113

1. INTRODUKSJON

1.1 Innledning og hensyn

Et uttalt satsningsområde for norske myndigheter er å gjøre Norge til en aktiv del av det globale informasjonssamfunnet. I en av fem hovedstrategier som Regjeringen Bondevik foreslo i Stortingsmelding nr. 41³ fremgår det at en videre avklaring av ansvarsforhold ved elektronisk formidling av informasjon samt avveininger i forhold til bl.a. ytringsfriheten kan være egnet til å ivareta både sosiale og samfunnsmessige hensyn i denne utviklingen.

Min erfaring er at det er stor usikkerhet i IT-bransjen mht. hvilke regler som gjelder for ulike aspekter ved virksomhet på Internett. Samtidig er det mitt inntrykk at det er en betydelig vilje til å innrette seg etter det som er rettstilstanden når denne lar seg fastlegge. En klargjøring av hvilke ansvarsregler som gjelder for aktører som driver virksomhet som digitalt mellomledd har derfor interesse for internettbransjens aktører i sin alminnelighet.

Jeg kan nevne flere grunner til at en slik klargjøring er ønskelig. For det første bærer IT-bransjen fremdeles preg av å være nyskapende på mange felt, og mange av prosjektene har et utviklingspreg som grenser opp mot forskningsprosjekter. Mange av de løsninger som utvikles har verken blitt vurdert av lovgivende organer, eller vært oppe for domstolene. Utviklingen har derfor utløst et behov hos digitale aktører for å kunne forutberegne sin rettsstilling utover de problemområder som man på forhånd kan regulere i kontrakt. Dessuten er det en avgjørende forutsetning for de digitale mellomledd å ha publikums, det vil si internettbrukernes, tillit når det gjelder f.eks. handel over nettet. I bransjen hersker det en felles forståelse av at den aktør som skulle bli dømt for brudd på aktsomhetsnormer som følger av gjeldende rett, raskt vil tape tillit i markedet, og av den grunn viktige markedsandeler. En slik forståelse blir betydelig styrket av det faktum at internettbransjen er en svært transparent bransje der massemedia daglig vier nyheter fra de som driver virksomhet på nettet anselig oppmerksomhet.

Et aspekt som ytterligere understreker de digitale mellomledds avhengighet av tillit i markedet er at mange mellomledd ikke kan regne med driftsoverskudd den første tiden de eksisterer og derfor er avhengige av kapitalinnsats fra investorer. Det er nærliggende å anta at investorenes vur-

³ Se Stortingsmelding nr. 41 (1998-99), punkt 1.3.1 nr. 5.

dering av hvorvidt det skal ytes kapitalinnsats i internettsselskap i stor grad vil basere seg på hvilken tillit digitale mellomledd har blant internettbrukere i sin alminnelighet.

Behovet for rettslig klargjøring og tillit i markedet kan også ses på bakgrunn av en mer generell usikkerhet som mange, både private internettbrukere og aktører i konvensjonelt næringsliv føler i forhold til IT-bransjen. Denne usikkerheten baserer seg på forhold som har med tiltro til virksomheter i verdipapirmarkedet å gjøre, men overføringsverdien er trolig ikke ubetydelig. Den knytter seg til de sedvanlige spekulasjoner rundt verdien av ulike internettsselskap. Ofte har høye kurser på aksjene i forskjellige internettsselskap vært fundert i luftige visjoner, og ikke i selskapets substans eller realistiske fremtidsvyer. Blant annet ved at personer som er involvert i driften av forskjellige internettsselskaper har solgt sine aksjer ved bindingstidens utløp har uavhengige aksjonærer tapt store penger som følge av kursfall.

1.2 Tema og problemstillinger i oppgaven

I oppgaven skal jeg gjøre rede for regler om ansvarsfrihet for ulike typer virksomhet som de digitale mellomleddene driver på Internett. Reglene jeg skal konsentrere meg om fremgår av EU-direktivet om visse rettslige aspekter informasjonssamfunnstjenester, spesielt elektronisk handel, i det indre marked.⁴

Hovedformålet med direktivet er å sikre samordning av, og gjennomføring i medlemslandenes interne rett av hensiktsmessige reguleringer av elektronisk handel.⁵ Ansvarsreglene fremgår av direktivets art. 12-14. Hovedformålet med disse er både å sikre rettslig forutberegnelighet for digitale aktører, samt å legge en basis for forbrukeres tillit til disse aktørenes virksomhet.⁶ Dessuten er det klart at e-handelsdirektivet har som målsetning å danne et rettslig grunnlag for ytringsfrihet⁷ på Internett og et funksjonelt

⁴ EU-dir. 2000/31/EF – alle referanser heretter til «direktivet», «EU-direktivet», eller «e-handelsdirektivet» refererer seg til dette. Direktivet ble godkjent av EU-parlamentet 4. mars 2000. Godkjenningen skjedde etter at direktivet hadde vært til annen lesning i parlamentet som følge av at det ble oppnådd politisk enighet i Rådet 7. des. 1999.

⁵ Det fremgår av EU-direktivets fortale, heretter også preambel, se punkt 3 jfr. punkt 5 at det er de divergerende rettslige reguleringer, og den rettsusikkerhet, som omfatter utviklingen av informasjonstjenester i medlemsstatenes nasjonale lovgivning som skaper det rettslige grunnlaget for fellesskapsinitiativet.

⁶ Se preambelens punkt (7)

⁷ I hht. preambelens punkt (9) skal e-handelsdirektivets begrep «freedom of expression», eller ytringsfrihet, forstås på samme måte som det er nedsatt i EMK art. 10(1). I henhold til NOU 1999:27 (Særskilt vedlegg nr. 1), s. 173, punkt 1.2.1, omfatter EMKs bruk av begre-

Internett som sikrer den frie bevegelse av informasjonssamfunnstjenester mellom medlemslandene.⁸

En hovedproblemstilling i oppgaven er hvorvidt de virksomheter som ulike mellomledd på Internett driver er omfattet av hovedregelen om ansvarsfrihet i e-handelsdirektivet. Dette spørsmålet kan deles inn i to underspørsmål. For det første kan det reises spørsmål om en virksomhet faller innunder anvendelsesområdet for art. 12-14. For det annet kan det reises spørsmål om hvert enkelt av disse bestemmelsenes vilkår for ansvarsfrihet er oppfylt for de mellomledd som faller innenfor anvendelsesområdet.

En annen hovedproblemstilling som drøftes i oppgaven er hvorvidt e-handelsdirektivets reguleringer er hensiktsmessige i den forstand at de byr på løsninger som er heldige i forhold til utviklingen av et konkurransedyktig marked for elektronisk handel.

1.3 Hvordan oppgaven er bygget opp

Oppgaven faller naturlig i fire hoveddeler. I innledningsdelen (oppgavens punkt 1) presiserer og begrunner jeg valg av tema, avgrenser oppgaven og kommer med begrepsavklaringer i forhold til tekniske og bransjespesifikke ord og uttrykk som jeg gjør bruk av. Herunder skal jeg forklare hva virksomhet som digitalt mellomledd på Internett, i følge min begrepsbruk, faktisk går ut på, samt redegjøre for hvilke regler som kan krenkes ved de ulike typer virksomhet. Videre skal jeg gi en oversikt over rettskildesituasjonen på området og metoden jeg bruker for å komme frem til mine konklusjoner.

I hoveddelen (oppgavens punkt 2) foretar jeg en tolkning av artiklene 12-14 i EU-direktivet om elektronisk handel. Disse bestemmelsene regulerer spørsmålet om ansvar for såkalte Intermediary Service Providers.⁹ Dertil gir jeg en fremstilling av noen av de problemstillinger som i praksis kan oppstå i forhold til det ansvarsregimet som artiklene oppstiller. I denne sammenheng

pet ytringsfrihet både meddelelse av ytringer og mottagelse av ytringer. Hensikten med å beskytte både meddelelse og mottagelse av ytringer er å beskytte hele kommunikasjonsprosessen og derved fri kommunikasjon av ytringer. I NOUens punkt 1.2.2, litra (b) sies det at meddelelsesfriheten ikke omfatter retten til å ytre seg gjennom andres kommunikasjonsfasiliteter. På bakgrunn av e-handelsdirektivets formål, som blant annet er å medvirke til at ytringsfriheten til de som benytter seg av Internett som kommunikasjonskanal blir ivarettatt, forutsetter jeg imidlertid at begrepet ytringsfrihet, slik jeg bruker det i denne oppgaven, også omfatter retten til å ytre seg gjennom andres kommunikasjonsfasiliteter.

⁸ Dette følger av preambelens punkt (8), jfr. punkt (9).

⁹ Jfr. overskriften til e-handelsdirektivets 4. seksjon.

skal jeg drøfte hvorvidt de, i innledningsdelen beskrevne mellomleddsvirksomheter, faller inn under anvendelsesområdet for ansvarsreglene, samt om mellomleddene oppfyller vilkårene for å komme innunder hovedregelen om ansvarsfrihet. Fordi min måte å fremstille ansvarsreglene på innebærer at jeg konsentrerer meg om utvalgte problemstillinger, er det ikke mulig å få belyst alle de rettslige aspekter ved art. 12-14. Imidlertid er mitt utvalg foretatt med intensjon om å få belyst viktige, praktiske problemer som reiser prinsipielle spørsmål i forhold til de ansvarsregler som e-handelsdirektivet oppstiller.

I de vurderingsdelen (oppgavens punkt 3) skal jeg evaluere de reglene jeg har beskrevet. I denne sammenheng skal jeg drøfte i hvilken grad det er rimelig at digitale mellomledd gjøres ansvarlig for krenkelser som er begått av deres medkontrahenter/kunder. I denne sammenheng skal jeg blant annet konsentrere meg om de rettspolitiske spørsmål som følger av de teknologiske muligheter til å kontrollere informasjon ved elektroniske agenter (filter), samt underrettelses- og slettingsregimer for antatt krenkende eller ulovlig informasjon, kontra hensynet til ytringsfrihet og fri informasjonsflyt.

I oppgavens fjerde del (punkt 4) skal jeg gi en kort oppsummering av noen av oppgavens hovedpoenger. Jeg skal videre formulere en overordnet konklusjon mht. ansvarsregimet som oppstilles i art. 12-14.

1.4 Presisering og avgrensning av oppgaven

Det første som karakteriserer virksomheten til de digitale mellomledd er at den nesten utelukkende er av informasjonsformidlende natur. Med andre ord er det normalt andre enn mellomleddet selv som skaffer til veie den informasjon som formidles. Oppgaven dreier seg derfor ikke om rettslige problemer knyttet til ansvaret for direkte å publisere ulovlig eller krenkende innhold på internettsider. Eksempel på et slik ansvar har den reiseoperatør som tilbyr og selger flybilletter på Internett. Denne vil ha samme ansvar som en operatør som selger billetter fra butikk.¹⁰

Jeg skal konsentrere meg om mellomleddets ansvar for videreformidling av informasjon representert gjennom tilgjengeliggjøring og spredning av eventuelt krenkende eller ulovlig materiale ved hjelp av dettes teknologiske infrastruktur. Spørsmålet er i denne sammenheng hvorvidt mellomleddet skal risikere ansvar for krenkende eller ulovlige handlinger begått av den tjenestetottager som opplagrer materiale på mellomleddets server, noe som kan skje ved at han deltar i en sanntids diskusjonsgruppe som drives fra mellom-

¹⁰ jfr. tillegg V, nr. 1, litra (c) til EU-dir. 98/48/EC

leddets tjenermaskin. Et annet spørsmål er hvorvidt mellomledet skal risikere ansvar for handlinger som er begått av den som leier tilgang til mellomledets aksesserver eller nettverksfasiliteter. For sivilrettens del kan dette omformuleres og presiseres til et spørsmål om hvem som skal ha risikoen for krenkende eller ulovlig handlinger som er begått av en tjenestemottager som benytter seg av mellomledets teknologiske infrastruktur. Denne risikoavveiningen har mange aspekter og er sentral i forhold til de overordnede styringsformål man kan utlede av e-handelsdirektivet. For strafferettens del blir spørsmålet i hvilken grad forskjellige reguleringer vil virke preventivt på de digitale mellomleds innstilling til å bryte mot retten. Også dette aspektet er viktig i forhold til direktivets overordnede styringsformål.¹¹

Ettersom den som ønsker å benytte seg av de digitale mellomleds teknologiske infrastruktur vanligvis må inngå en rekke kontrakter med mellomledene for å få tilgang til disse tjenester, kan det reises spørsmål om hvilken betydning en eventuelt kontraktsregulering av ansvaret spiller i denne sammenhengen. Umiddelbart kan det virke som om mellomledene skulle kunne begrense sitt ansvar i kontrakt. Imidlertid er det klart at den person hvis rettigheter er krenket, i langt de fleste tilfeller, ikke er den person som står i et avtalerettslig forhold til det digitale mellomledet. Det ansvaret denne oppgaven skal dreie seg om er da også ansvaret utad, det vil si i forhold til tredjemann hvis plikter og rettigheter i forhold til mellomledet ikke er regulert i kontrakt. Jeg nevner for fullstendighetens skyld at mellomledet, om det skulle bli kjent ansvarlig overfor tredjemann som følge av krenkende eller ulovlige forhold fra sin medkontrahent eller kundes side, i de fleste tilfeller vil sitte igjen med et regresskrav mot sin tjenestemottager. Dette ansvaret skal ikke behandles i oppgaven.

Hovedskiller i det elektroniske markedet går for det første ved hvem som er målgruppe for den virksomheten som de digitale aktørene driver. I målgruppene finner vi de tredjemenn som er mottagere av tjenester i den forstand at de søker og finner informasjon, tjenester eller varer på Internett. For det andre skiller man mellom hvem som er tjenesteyter i forhold til den aktuelle virksomhet. Populært kategoriserer man gjerne de forskjellige typene forretningsdrift i BtB-, BtC-, BtG- og etter hvert også og PtP-virksomhet. Bokstaven B betyr at virksomheten drives av en profesjonell part (Business to-). Den siste bokstaven indikerer hvem som er målgruppen for virksomheten. B står her for Business, C for Consumer og G for Government¹² (det vil si sentrale

¹¹ Jeg gjør nærmere rede for direktivets styringsformål i oppgavens punkt 2.2.1.

¹² I Stortingsmelding nr. 41 (1998-99), punkt 1.3.1 fremgår det at «Offentlig sektor skal satse på elektronisk handel for å effektivisere egne innkjøp og vil derved bli en pådriver for ut-

og lokale myndigheter). Virksomhet opp mot hver av disse målgruppene styres av tildels forskjellige regler. Ved BtC-virksomhet må det særlig tas hensyn til forbrukerlovgivningen, mens det ved BtG-virksomhet må tas hensyn til lovgivningen om offentlige anskaffelser, mv. Ofte vil hensiktsmessigheten og lønnsomheten av forskjellige typer mellomleddsvirksomhet avhenge av hvem som er målgruppen. F.eks. vil mellomledd som «host service providers»¹³ være særlig viktige innen BtB-handel. Når det gjelder PtP-virksomhet, så står forkortelsen for «peer to peer», det vil si likemann til likemann. Som ordene innebærer omfatter dette forretningsmodeller der tjenesteyter og tjenestemottager formelt står på likefot. Et typisk tilfelle er, fordi PtP i hovedsak er en betegnelse som brukes der forbrukere handler med forbrukere over Internett (CtC-virksomhet), der musikk formidles gjennom Napster-tjenesten.¹⁴ Ved PtP-virksomhet oppstår det særlig problemer i forhold til håndheving av det regelverk som gjelder for de aktuelle virksomheter. Grunnen til dette er at det er vanskelig for myndighetene å undergi de involverte partene noen effektiv kontroll, slik både offentlige og private bedrifter er. Denne oppgaven skal ikke ta opp de spesielle problemer som knytter seg til PtP-, BtC-, og BtG-virksomhet.

I mange tilfeller har virksomhet på Internett et grenseoverskridende preg. Den person hvis rettigheter påstås krenket kan f.eks. være hjemmehørende i et annet land enn der det digitale mellomleddet driver sin virksomhet. Noen ganger står den serveren som mellomleddet benytter til å videreformidle eventuelt ulovlig eller krenkende informasjon i et tredje land. Dessuten kan den person som står for den underliggende krenkelsen være hjemmehørende i et fjerde land. I disse tilfellene kan det for det første oppstå et spørsmål om hvilket lands jurisdiksjon en sak om ansvar skal høre inn under. For det andre kan det reise seg spørsmål om hvilket lands lov som skal anvendes for å løse problemet. Disse spørsmålene er del av problemkomplekset som tradisjonelt behandles i interlegalretten¹⁵, og skal ikke behandles nærmere i denne oppgaven.

I oppgavens punkt 3 skal jeg drøfte visse rettspolitiske aspekter som knytter seg til reglene e-handelsdirektivet oppstiller i art. 12-14. Meningen med

viklingen.» Arbeidet med å utvikle en egen portal for offentlige innkjøp er allerede i gang og informasjon kan finnes under domenet www.handel.no.

¹³ Jfr. punkt 1.6.5.

¹⁴ Napster-tjenesten (tilgjengelig www.napster.com) tillater brukerne vederlagsfritt å laste ned musikkfiler fra andre brukeres harddisk. Den tjenesten Napster yter består i å kartlegge musikkutvalget til, og formidle kontakt mellom de forskjellige brukere som til enhver tid er logget på systemet.

¹⁵ Se blant annet Bing (1999) og Lenda (1999).

drøftelsene er hovedsakelig å peke på en del betenkeligheter som direktivets reguleringer kan skape i forhold til blant annet yringsfriheten og ønsket om å beholde Internett som en åpen kommunikasjonskanal. Det kan i denne sammenheng oppstå konflikter mellom de løsninger jeg argumenterer for og forholdet til yringsfriheten i Grunnlovens § 100, samt i de internasjonale konvensjoner som Norge har ratifisert.¹⁶ Det ligger utenfor oppgaven å vurdere nærmere spørsmålet hvorvidt de løsningene jeg argumenterer for faktisk forårsaker grunnlovs-, eller konvensjonsstrid.

I henhold til §1-1 i teleloven¹⁷ omfattes all telekommunikasjonsvirksomhet, herunder «...overføring av lyd, tekst, bilder eller andre data ved hjelp av radiosignaler eller andre elektromagnetiske signaler i et kommunikasjonsnettverk for signalbefordring...», noe som medfører at i alle fall nettverksoperatørens virksomhet faller innunder anvendelsesområdet. Fordi det ville ligge utenfor oppgavens område å diskutere de problemstillinger som ligger innenfor teleloven avgrenser jeg mot disse.

Avslutningsvis vil jeg presisere at reguleringene som fremgår av e-handelsdirektivet i stor grad er teknologinøytrale. Dette innebærer at teknologiske forhold, som valg av stasjonære eller trådløse kommunikasjonsformer, i utgangspunktet ikke legger føringer på hvorledes man skal anvende bestemmelsene i direktivet.¹⁸ Eksempelvis er det mulig å koble seg opp til Internett via mobile terminaler som f.eks. WAP-telefoner.¹⁹ Den informasjon som kan nedlastes på en WAP-telefon blir oversendt trådløst, men er lagret på de samme serverne som vanlige internettsider. På samme måte som gjennom stasjonære terminaler vil man derfor gjennom WAP-telefonen få online tilgang til Internett. Jeg skiller i oppgaven ikke mellom hvorvidt digitale mellomledd benytter stasjonære eller trådløse teknologiske plattformer for å yte sine tjenester²⁰.

¹⁶ Av de internasjonale bestemmelsene som det her kan bli snakk om nevner jeg særlig forholdet til EMK art. 10 og til SP art. 19.

¹⁷ Se Lov om telekommunikasjon av 23.06.95, nr. 39 (teleloven)

¹⁸ Det viktigste avgrensningskriteriet er at tjenesten som ytes er en informasjonssamfunnstjeneste i e-handelsdirektivets forstand. Vilkårene for at en tjeneste er en informasjonssamfunnstjeneste skal jeg ta for meg i punkt 2.3.2.

¹⁹ WAP er en forkortelse for «Wireless Application Protocol», eller trådløs applikasjonsprotokoll.

²⁰ På en rekke punkter skiller likevel WAP-tjenestene seg fra de ordinære internetttjenestene. Internettsider benytter seg et såkalt HTML-format (format basert på HyperText Markup Language), mens formidling av WAP-sider forutsetter et såkalt WML-format (format basert på Wireless Markup Language), noe som gir seg utslag i enkelte praktiske forskjeller. Den mest iøynefallende er det begrensede brukergrensesnittet. Juridisk kan det oppstå

1.5 Forklaring av noen begreper²¹

Begrepet digitale mellomledd deles i boken *elektronisk handel* av Hellebust mfl. (2000 s. 33 flg.) inn i tre hovedkategorier: Produktintegratorer, portaler og digitale koblere. Begrepet er etter min mening godt, og det har ikke noe festnet innhold. I denne fremstillingen bruker jeg begrepet i en noe annen betydning. Jeg lar begrepet omfatte de tjenesteytere på Internett som sørger for den teknologiske infrastrukturen, herunder både kabler, rutere, servere og programvare, som muliggjør effektiv internettbruk. Jeg kan ikke se at ordlyden strider mot denne bruken.

Oppgavetittelens begrep ytringer bruker jeg i sin videste betydning. Dette vil si at så vel enkeltuttalelser av personlig art, redaksjonelt innhold som restaurantanmeldelser og musikkritikker, markedsføring gjennom bannere eller gjennom interaktive konkurranser og publisering av opphavsrettslig beskyttet materiale i form av programvare og musikk er omfattet. I tillegg omfattes også ytringer som har mye til felles med faktiske handlinger, f.eks. dersom den som benytter mellomleddets tjenester ved å gjøre tilgjengelig hackede filer på en internettside, legger til rette for piratkopiering av forskjellige typer opphavsrettslig beskyttet materiale.

I drøftelsen av enkelte problemstillinger i oppgavens hoveddel (oppgavens punkt 2) vurderer jeg den teknologiske filtrering av informasjon som enkelte digitale mellomledd foretar, opp mot vilkårene for ansvarsfrihet i e-handelsdirektivet. Jeg skal derfor gjøre klart hva jeg mener med filtreringsbegrepet. Et teknologisk filter er en type programvare som i prinsippet kan installeres på enhver datamaskin. Den vanlige bruken innebærer at hver enkelt oversendelse av informasjon blir gjennomgått av et program som reagerer på forhåndsbestemte kvalifikasjonskriterier, som f.eks. ord med rasistisk eller seksuell betydning. Dersom ordene forekommer i den informasjonen som er undergitt filtrering, vil én hovedtype filtreringsprogrammer stanse hele oversendelsen, mens en annen hovedtype sladder de ordene som er forhåndsvalgt for så slippe informasjonen igjennom. Den vanligste formen for filtrering er den førstnevnte. I praksis medfører denne metoden at dersom ord eller uttrykk i den informasjonen som inngår i en oversendelse oppfyller kvalifikasjonskriteriene, så vil hele oversendelsen bli stanset. Fordi det særlig er ved bruk av førstnevnte metode det oppstår tvilstilfeller i forhold til e-

opphavsrettslige spørsmål ved denne omformateringen. F.eks. kan overføring av grafikk-bilder til WAP-formatet medføre at kvaliteten forringes vesentlig.

²¹ Begrepsforklaringen er utarbeidet på grunnlag av Hellebust mfl. (2000 s. 33 flg.) og med støtte i Øien (2000 s. 8 flg.).

handelsdirektivets ansvarsregler er det denne som skal være gjenstand for vurdering i oppgaven.

1.6 Hvilke roller digitale mellomledd påtar seg

1.6.1 Innledning

Jeg skal nedenfor gjøre nærmere rede for de vanligste funksjonene digitale mellomledd tar på seg.²² I denne sammenheng skal jeg beskrive en rekke måter å yte tjenestene på som har utviklet seg som følge av forretningsmessig eller teknologisk hensiktsmessighet. Beskrivelsene skal tjene til en generell innføring i digitale mellomledds virksomhet samtidig som de skal danne faktiske forutsetninger for enkelte av drøftelsene i oppgavens hoveddel.

Det må presiseres at digitale mellomledd ofte opptrer i flere roller samtidig. Dette viser seg særlig i forhold til digitale aktører som står for både tilveieskaffelse av internettaksess, nettverksutleie og utleie av serverplass samtidig som de utvikler programvare for virtuelle aktiviteter, f.eks. ved programmering og design av moduler for e-handel.²³ Det er imidlertid viktig å understreke at de forskjellige rollene, og kombinasjonen av roller, er under konstant utvikling. Alle de rollene som digitale mellomledd spiller er undertiden viktige når internettbrukeren ønsker å bruke Internett på alminnelig måte, f.eks. til å «surfe» nettet eller til å laste ned digitalt materiale. I praksis må internettbrukeren først ta kontakt med en aksessleverandør for bli koblet opp til Internett. Dernest må han ved hjelp av en nettleser, og eventuelt ved hjelp av en søkemotor, identifisere og knytte seg opp til en server, operert av en host service provider, som lagrer det etterspurte materialet.

1.6.2 Aksessleverandør

Aksessleverandøren er det mellomledd som skaffer kunden tilgang til Internett. Tilgangen skjer ved at kunden kobles opp til nettverket gjennom aksess-

²² Forklaringene er utarbeidet blant annet med utgangspunkt i Julia-Barceló, Rosa (1999b s. 10-18), Draft Brochure (2000 s. 98) og opplysninger fra internettjenesten whatis?com, URL: <http://www.whatis.com>

²³ Det har i noen tid vært tale om såkalte ASP-leverandører. Betegnelsen gir uttrykk for en sammensmelting av funksjonene som programvareleverandør og som ren teknologileverandør (ASP I og ASP II). ASP I –leverandører står gjerne for programmering av det som kalles Active Server Pages. Dette er dynamiske nettsider som tillater en viss interaktivitet mellom internettbrukeren og den som driver nettstedet. ASP II-leverandører står for utleie av serverplass til forskjellige nettapplikasjoner (Application Service Provider).

leverandørens server. Derpå bruker kunden aksessleverandørens server til å søke eller legge ut informasjon på Internett. Det er vanlig at aksessleverandøren også skaffer kunden en e-postkonto. Blant aksessleverandørene finnes både de som yter sine tjenester mot et månedlig leiebeløp, men også, i den senere tid, de som tilbyr gratis aksess til Internett.²⁴

Når man skaffer seg tilgang til Internett er det vanlig at aksessleverandørens hjemmeside er forhåndsinnstilt som tjenestemottagerens startside. Dette kan gjøres ved at URL-en²⁵ til leverandørens hjemmeside automatisk installeres i nettverksinnstillingene til brukerens datamaskin. For operatører som leverer gratis aksess er det ikke uvanlig at linker til aksessleverandørens samarbeidspartnere/annonsører blir gjort til en obligatorisk del av brukerens skjermbilde.²⁶ En slik forhåndsprogrammering av linker i brukerens grensesnitt mot Internett er i de fleste tilfeller vanskelig å fjerne, og må etter min mening betraktes som en del av den tjenesten som aksessleverandøren yter.

1.6.3 Nettversoperatør²⁷

Nettversoperatøren er den aktør som skaffer de teknologiske fasiliteter som er nødvendig for å kunne sende data over et nettverk, f.eks. Internett. Praktisk sørger nettversoperatøren for kabling og ruting²⁸, enten ved at kunden kobles til nettverket gjennom en telefonlinje, eller ved at det opprettes en fastlinje. Når det gjelder nettversleveranse til private legges ofte linjene helt inn i kundens bolig. Dersom det dreier seg om nettversutleie til næringsdrivende hender det ofte at nettversoperatøren stiller til disposisjon lokaler der

²⁴ Blant annet blir de som får aksess til Telenors internettservere belastet med et månedlig leiebeløp (med unntak av Telenor Frisurf). Dersom man velger seg aksess gjennom for eksempel Liberty Surf, er denne tjenesten pt. gratis.

²⁵ Begrepet URL (Uniform Resource Locator) brukes isteden for begrepet «adresse». En URL gir en komplett angivelse av hvor informasjon er å finne på Internett.

²⁶ Jfr. f.eks. det grensesnitt som tilbys dersom man velger Liberty Surf som aksessleverandør. Her ligger linker til Liberty Surf's samarbeidspartnere/annonsører som et banner som strekker seg over hele skjermens bredde og ca. 2 cm ned i skjermbildet.

²⁷ Med de krav om økt overføringshastighet, eller båndbredde, som utviklingen har ført med seg ser man at nettversleverandørens rolle blir tiltagende mer viktig. Nettverskapasiteten er ofte en betydelig flaskehals for overføring av informasjon og den nettversoperatør som kan tilby den infrastruktur som tillater størst overføringshastighet kan gå fremtiden lyst i møte.

²⁸ Ruting skjer i rutere. Ruterer er maskinvare med spesiell programvare som fungerer som knutepunkter for forskjellige nettverk ved at de tar imot og videresender signaler. Først lagrer ruterer de mottatte signaler. Deretter sender den signalene videre til neste mottakermaskin. Dette kan være en ny ruter eller en endestasjon. Oppnår ikke ruterer kontakt med neste mottakerstasjon sendes signalene tilbake igjen. Dette gjentar seg helt til signalene ender i et lokalt nettverk eller i en endebrukerstasjon.

kundens servere kan kobles opp til nettverkslinjene, slik at de kan få stå uforstyrret og trygt.

Under oversendelsen av informasjon i et nettverk skjer det rent teknisk utallige reproduksjoner av den oversendte informasjon. Denne reproduksjonen skjer i en prosess som kalles «packet switching transmission». Prosessen består i at data som blir oversendt i nettverket blir splittet opp i små deler kalt packets. Datapakkene blir lest av datamaskiner i nettverkets knutepunkter, kjent som rutere, og blir deretter dirigert i riktig retning. Under den prosessen som skjer i ruterer kan det forekomme at et opphavsrettslig beskyttet verk oppstår i en midlertidig eksemplarframstilling. Dette forutsetter imidlertid at verket er lite nok til å inngå i én datapakke.²⁹ Noen sammensetning av de enkelte datapakkene skjer ikke før pakkene når sitt destinasjonspunkt.

1.6.4 Proxy serving, proxy caching, mirror caching

Begrepene proxy serving og proxy caching brukes om hverandre, men de beskriver hovedsakelig samme funksjon. Jeg skal i det følgende holde meg til uttrykkene proxy caching/caching om den virksomheten som jeg tar for meg i oppgaven.

Proxy caching innebærer at etterspurt informasjon som er hentet fra en fjernere server (kildeserveren) mellomlagres på en server som er lokalisert i nærheten av den som mottar videreformidlingstjenestene. Når sluttbrukeren etterspør spesiell informasjon, blir denne hentet fra kopien som er lagret på en lokal server istedenfor fra den opprinnelige kildeserveren. Som et resultat av dette sørger proxy cacheren for at etterspurt informasjon blir raskere overført over en kortere distanse, og tid spares.³⁰ Den lokale lagringen av data kan skje for kortere eller lengre perioder avhengig av etterspørsel.

Med de overføringshastigheter for data som er tilgjengelig for det store antall internettbrukere i skrivende tidspunkt ville fraværet av proxy caching-tjenestene føre til overbelastning av internettinfrastrukturen som helhet, og Internett ville slutte å fungere ordentlig.

Proxy caching kan også skje ved at tilbyderer av fjerntliggende, etterspurt informasjon selv tar initiativ til å legge denne på servere som er lokalisert i

²⁹ I praksis medfører dette at de verk som kan oppstå midlertidig i «packet switching»-prosessen kun utgjør små tekstfiler som f.eks. dikt eller sangtekster.

³⁰ Andre formål med å drive proxy caching kan være ønsket om anonymisering av internettbrukere (ved at pseudonymisering skjer i proxy serveren), ivaretagelse av informasjonssikkerheten (ved at brannvegger installeres hos proxy cacheren) eller tilpasning av dataoverføringsformat (ved at omkodning skjer i proxy serveren).

nærheten av brukerne. Denne formen for proxy caching kalles gjerne *mirror caching*.³¹

Det er viktig å være oppmerksom på at det jeg beskriver om proxy caching skiller seg fra det som i teknologikretser tradisjonelt er oppfattet som *caching*. Den sistnevnte funksjonen innebærer en midlertidig lagring av informasjon som skjer i internminnet til en datamaskin, det vil si i RAM-minnet. Denne midlertidige lagringen omfattes ikke av bestemmelsene i e-handelsdirektivet, og jeg skal ikke gå nærmere inn på denne i oppgaven. Imidlertid gjør e-handelsdirektivet i overskriften til art. 13 bruk av begrepet caching på en slik måte at det er naturlig å forstå det som proxy caching. Der hvor jeg av hensynet til tekstflyten finner det nødvendig å bruke begrepet *caching* gjør jeg det derfor i betydningen proxy caching.

1.6.5 Host service provider

Tjenesten en host service provider yter innebærer at mellomledet skaffer til veie en server (tjenermaskin) der lagringsplass for nettsider, e-handelsløsninger og lignende blir leiet ut til private brukere, eller vare-, og tjenesteytere på Internett (hosting). De nettsidene som tilbys ved hjelp av host service providerens tjenester kan inneholde all slags digitalt materiale som f.eks. programvare, tekst, grafikk, lyd, musikk, internettradio³² mm. Som regel omfatter også tjenesten utleie av serverplass til en e-postkonto.

1.6.6 Bulletin board operatør³³

I kategorien for bulletin board operatører finner vi tjenester som innebærer at mellomledet skaffer til veie serverplass for både identifiserte og uidentifiserte brukere, det vil si både innenfor og utenfor noe formalisert kundeforhold. Ved bruk av disse tjenestene kan man poste egne meldinger og lese informa-

³¹ Det er i teorien noe delte oppfatninger om hva virksomheten «mirror caching» egentlig skal omfatte. Blant annet gir Julià-Barceló (1999b s. 12) uttrykk for at «mirror caching» omfatter langvarig lagring av hele websteder og som ikke er automatisk eller mellomliggende. En slik definisjon av «mirror caching» kan imidlertid ikke være holdbar ettersom den virksomheten hun beskriver tilsvarer det som etter tradisjonell oppfatning er kjent som hosting.

³² Formidling av internettradio er pt. en relativt ressurskrevende aktivitet i den forstand at det kreves mye serverplass og spesiell programvare som tillater såkalt «streaming» av digitale signaler. Implikasjonene av å formidle nettradio er at radiostasjoner verden rundt kan bli gjort lokalt tilgjengelig gjennom Internett.

³³ Disse tjenestene faller innunder det som i bransjen ofte kalles community-tjenester.

sjon som er postet av andre.³⁴ Vanligvis er de aktuelle tjenester knyttet opp til spesielle emner.

Det finnes to hovedkategorier bulletin board tjenester, nemlig de som har en host master, det vil si en interaktiv gruppeleder, og de som ikke har det. Funksjonene til en interaktiv gruppeleder består for det første ofte i å overvåke den enkelte tjeneste slik at mellomledet gis en mulighet til å stanse ytringer som kan virke krenkende, og som derfor kan true brukernes oppslutning rundt tjenesten. For det andre kan gruppelederen bistå i debattledelse ved at han kommer med nyttige spørsmål og innspill til de emner som diskuteres. Bulletin board tjenesten tillater også direktekommunikasjon mellom mennesker i sanntid i såkalte chat rooms.

Tilbudet av bulletin board tjenester kan omfatte både utleie/utlån av plass på egen eiet server og (vederlagsfri) fremleie av andre aktørers serverplass. I sistnevnte tilfelle består bulletin board tjenesten hovedsakelig av en tilretteleggelse for utøvelse av forskjellige typer interaktiv virksomhet, ved at bulletin board operatøren tilbyr den programapplikasjonen som er nødvendig for å drive den aktuelle tjenesten.

1.6.7 Søkemotorer³⁵

Formålet med å drive søkemotortjenester er å skaffe internettbrukere et verktøy som er nødvendig for å finne nettsider der etterspurt informasjon er lokalisert. Det finnes flere kategorier av søkemotorer, avhengig av hvordan de fungerer. Enkelte av søkemotorene er helautomatiserte mens andre i større grad er avhengige av menneskelig initiativ for å lokalisere informasjon. Det er også forskjeller mht. hvilke kriterier søkemotorene baserer søkene sine på. Enkelte store søkemotorer som Yahoo og Alta Vista opererer med en metode som har til mål å indeksere og klassifisere et representativt innhold av all informasjon på Internett. Deretter bruker de forskjellige kriterier for å ordne sidene hierarkisk ved hvert enkeltøk. Andre søkemotorer, som f.eks. norske Kvasir, baserer seg hovedsakelig på tekstsøk, det vil si at motoren utfører søk i ord og uttrykk som

³⁴ Eksempler på slike bulletin board tjenester finner man hos mange av de kjente internettaktørene i Norge. Blant annet er nettvenntjenesten til Scandinavia Online AS (www.sol.no), som består i en tilretteleggelse for å poste og søke i kontaktannonser på Internett, en slik bulletin board tjeneste.

³⁵ Vi har flere eksempler på søkemotorer. Blant de største er Yahoo og Alta Vista. I Norge har vi blant annet søkemotoren Kvasir. En hjelp til å finne forskjellige søkemotorer er å finne på adressen www.easysearcher.com/ez2.html

nettsidene inneholder, og deretter, basert på blant annet relevanskriterier, danner et hierarki av de sider der søkeordene er representert.³⁶

1.6.8 Portaler

Portalen utgjør et virtuelt samlingspunkt (i praksis en nettside) som inneholder pekere til forskjellige internettadresser. Portalene har til formål å tilgjengeliggjøre og segmentere informasjon fra en spesiell bransje eller for en spesiell gruppe nettsteder. Det er ikke nødvendig at den server som portalsidene ligger på inneholder informasjon utover de nevnte internettadresser. Portaltjenestene gjør det enklere for internetbrukeren å finne og få videreformidlet etterspurt informasjon.

1.7 Hvilke regler kan tenkes krenket ved de forskjellige typer mellommannsvirksomhet?

Det er ikke noe nytt problem at massemedia og andre kommunikasjonskanaler misbrukes til illegal aktivitet. Internett er imidlertid forskjellig fra eldre teknologi når det gjelder visse nøkkelaspekter for kommunikasjon. Det er særlig muligheten for alle til alle kommunikasjon og interaksjon mellom tjenesteyter og tjenestebruker som skiller Internett fra de tidligere kommunikasjonskanalene. Gjennom utviklingen har man sett at dette kan føre til nesten anarkistiske tilstander der respekten for gjeldende regelverk blir satt på prøve. Som vi skal se under beror det imidlertid på en misforståelse dersom man tror at lovverket ikke gjelder fordi man har en teknologi som er ny og ukjent.

Oversikten som følger er ment å gi eksempler på noen av de rettsområder som særlig berøres av den teknologiske utviklingen mot informasjonssamfunnet. De materiellrettslige regler som særlig kan tenkes krenket ved virksomhet på Internett er de følgende:³⁷

³⁶ For en nærmere beskrivelse av søkemotorenes funksjon se under S i den meget nyttige netttjenesten whatis.com, tilgjengelig på www.whatis.com

³⁷ Det ser ut til å være en enighet mellom juridiske forfattere om at det er rettsreglene på de herunder nevnte rettsområdene som oftest vil bli krenket. Se Loundy (1993 s. 102-173), Lloyd (1996 s. 273-299), Angel (1996 s. 150-157) og Hagstrøm (1989 s. 196-220).

1.7.1 Opphavsrettslige regler³⁸

Opphavsretten er kanskje det viktigste området der man etter fremveksten av det digitale samfunn ser at lovgivningen står i fare for å bli krenket. Grunnen til at aktørene på dette rettsområdet har vist seg å være særlig utsatt for krenkende og ulovlige handlinger ligger i de vernede rettigheters natur. Med utviklingen av digitaliseringen har muligheten til å overføre store mengder materiale som omfattes av immaterielle rettigheter økt i revolusjonerende grad. Kopiering av opphavsrettslig vernet materiale kan skje med meget enkle håndgrep og med en kostnad som er nesten lik null. I tillegg fører ikke kopiering med digitale midler til at kopien forringes i forhold til originalen. Fra ett originaleksemplar er det dermed mulig å fremstille et tilnærmet ubegrenset antall (pirat)kopier.

Konkret kan de opphavsrettslige reglene krenkes ved at materiale som eks. tekst, bilder, musikk, og til og med spillefilmer blir gjort tilgjengelig på nettsider der de ukontrollert kan bli nedlastet til brukermaskiner over hele verden.

1.7.2 Personvernrettslige regler

Personvernrettens område er et annet viktig område der man ser gjeldende rett utfordret av aktørene i det nye informasjonssamfunnet. Med den økning i mulighetene til å registrere personopplysninger, samt å utarbeide personregister til bruk i markedsføringsformål og lignende, ser man at lovgivningen ikke lenger fungerer tilfredsstillende. Problemet er for det første at personvernreglene ofte ikke blir respektert av de mange nye aktørene på e-handelsmarkedet. For det annet har det vist seg vanskelig for Datatilsynet³⁹ å sette av de nødvendige ressurser for å kontrollere innsamlingen og behandlingen av personopplysninger i alle enkelttilfeller.⁴⁰

1.7.3 Strafferettslige regler

Strafferettslige regler kan krenkes ved at pornografisk, rasistisk eller ærekrenkende materiale gjøres tilgjengelig via en nettside.

³⁸ Når det gjelder enklere opphavsrettslige spørsmål, så kan man benytte seg av veiledningen som tilbys gjennom internettjenesten Clara. Tjenesten er utviklet av en rekke forvaltningsorganer for opphavsrettslig beskyttet materiale, URL: <http://www.clara.no/>

³⁹ Datatilsynet er den nasjonale kontrollinstansen når det gjelder personvernsspørsmål, jfr. personopplysningslovens §§ 42 flg.

⁴⁰ Ny lov på personvernområdet trådte i kraft 01.01.2001, se Lov om personopplysninger av 14.04.2000 nr. 31. Denne loven er basert på EU-direktiv 95/46/EC (personverndirektivet).

1.7.4 Varemerkerettslige regler

Varemerkerettslige regler kan krenkes ved at rettighetshaveres navn eller logo blir misbrukt, enten ved at navnet eller logoen plasseres i en kontekst som er med på å forringe merkenavnet, eller ved at det oppstår konflikt om retten til et varemerke som følge av at det brukes på en nettside, eksempelvis der et nasjonalt varemerke kommer i konflikt med et internasjonalt varemerke. I forhold til søkemotorer kan det oppstå særlige problemer i forhold til bruk av såkalte meta tags.⁴¹ Dersom noen søker etter et særlig nøkkelord ved hjelp av en søkemotor vil denne også liste opp de nettstedene som kun inneholder nøkkelordet i en meta taggingen. Dersom et firma f.eks. bruker varemerket til en konkurrent i meta taggingen på egne nettsider, vil søkemotoren liste opp disse nettsidene når det blir søkt etter konkurrentens varemerke. Resultatet av slik meta tagging kan være at det firma som på slik måte misbruker et varemerke får høyere prioritet i søket enn nettsiden til rettighetshaveren. Det er den alminnelige oppfatningen i norsk og internasjonal juridisk litteratur at denne virksomheten representerer en misbruk av tredjemanns varemerkerettigheter.⁴²

1.7.5 Kjøpsrettslige regler

Kjøpsloven dekker et rettsområde som er viktig når det gjelder handel med varer over Internett. Mange av både kjøperens og selgerens rettigheter og plikter ved kjøp av varer i nettbutikker er regulert i denne lovgivningen. Som eksempel kan jeg nevne at reglene om både mangler, forsinkelse og risikoovergang ved levering av varer kommer til anvendelse. Selv om en vare er bestilt gjennom en nettbutikk må levering nødvendigvis skje utenom nettet. Rettslig må dette behandles på samme måte som levering av produkter som er bestilt på «vanlig» måte. Når det gjelder levering gjennom nettet, typisk av elektronisk informasjon som dataprogrammer mv., reiser dette, på samme måte som ved fysisk overlevering, spørsmål om dokumentasjon av hva som er levert og på hvilket tidspunkt.

1.7.6 Forbrukervernregler

Ved salg av varer og tjenester til forbruker over Internett eksisterer det et omfattende regelverk som tar sikte på å beskytte forbrukere når de handler med næringsdrivende. Det er også under utarbeidelse nye regler i forhold til hvilke

⁴¹ Meta tags er nøkkelord som bli innskutt i kildekoden til nettsider og som ikke er synlige på det aktuelle nettstedet.

⁴² Spørsmål kan imidlertid også reises om hvorvidt slik virksomhet strider mot konkurranserettslige prinsipper.

rettigheter og plikter som skal pålegge de enkelte partene.⁴³ Disse reguleringen er meget sentrale i forhold til den virksomhet som mange næringsdrivende bedriver på Internett. Som eksempel på rettslige krav kan jeg nevne at forbrukeren alltid skal ha vedlagt et angrefristformular, jfr. ved den leverte vare når han handler på nettet, samt at avtalevilkårene skal være klare og uttømmende.

1.7.7 Kan reglene på andre rettsområder krenkes?

Av andre regler som kan tenkes krenket ved virksomhet på Internett er blant annet regler om patentrettigheter og konkurranserettlige regler. Jeg går ikke nærmere inn på disse da de viktigste rettsområdene der tredjemanns rettigheter er truet allerede er nevnt ovenfor.

1.8 Rettskildesituasjonen

Den 8. juni 2000 trådte EU-direktivet om elektronisk handel i kraft. Direktivet regulerer i art. 12-14 spørsmålene om ansvar for digitale mellomledd. En forutsetning for min oppgave er at direktivet gjennom EØS-avtalen implementeres i norsk rett.⁴⁴ I denne sammenheng skal direktivet etter Romatraktatens art. 189, 3. ledd være bindende for medlemsstatene mht. sin målsetning, men overlater til de nasjonale myndigheter å bestemme form og midler for gjennomføringen. Direktivets ordlyd er av denne grunn den viktigste rettskildefaktor for tolkning av direktivet. Det er imidlertid knyttet en del usikkerhetsmomenter til ordlyden. Direktivet er f.eks. utferdiget på en rekke offisielle språk og ordlyden i de forskjellige språk kan ha forskjellige nyanser. E-handelsdirektivets bestemmelser inneholder dessuten forholdsvis mange vage og skjønsmessige uttrykk som kan ordlydsfortolkningen vanskelig.

Ordlyden må tolkes i lys av direktivets preambel, også kalt fortale. Denne gir etter Romatraktatens art. 190 uttrykk for begrunnelsen for direktivet. Preambelen fyller noen av de samme funksjonene som lovers forarbeider gjør etter norsk rett. Imidlertid er den i enda større grad vag og skjønsmessig. Preambelen har imidlertid i seg selv ikke særlig rettskildemessig vekt.

⁴³ Se Ot.prp. nr. 36 (1999-2000) som inneholder forarbeider til ny lov om angrerett og forslag til ny lovtekst.

⁴⁴ Medlemsstatene er etter e-handelsdirektivets art. 22 nr. 1 gitt tiden frem til 17. jan. 2002 for å implementere direktivets bestemmelser i nasjonal rett. Dette innebærer en 18 måneders frist fra vedtagelsesdatoen. Forslag om samtykke ble fremmet 16.3.2001 i St. prp. nr. 55 (2000-2001), og i skrivende stund (primo april 2001) var innstillingen planlagt behandlet av Stortinget 26.4.2001.

Som en ytterligere rettskildefaktor kan nevnes direktivets formålsbestemmelse i art. 1 der det i grove trekk fremgår hvilke interesser direktivet er ment å ivareta.

Noe juridisk litteratur har det vært mulig å oppdrive når det gjelder å få et generelt overblikk over artiklene 12-14, og de hensyn som disse skal ivareta. Imidlertid er det svært sparsomt med kommentarer til hvile virksomheter som konkret omfattes av bestemmelsene i direktivet, og hvilke omstendigheter som avgjør hvorvidt en virksomhet i praksis skal nyte godt av hovedregelen om ansvarsfrihet.

Det er ellers beskjedent med internasjonale rettskilder når det gjelder forståelsen av artiklene 12-14 i e-handelsdirektivet. F.eks. har EU-domstolen ennå ikke tolket direktivet. De vurderinger som foretas i oppgavens hoveddel er derfor i relativt stor grad basert på reelle hensyn og mine egne kvalifiserte antagelser om hvorledes gjeldende rett er, basert på det som utover selve e-handelsdirektivet med dets preambel er et sparsommelig rettskildemateriale. Avsnittene nedenfor må leses med den reservasjon som ligger i ovennevnte.

1.9 Metoden som brukes i oppgaven

I oppgaven bruker jeg juridisk metode. Spørsmålene som drøftes vil derfor bli avgjort etter en prosess styrt av normer for de forskjellige rettskildefaktorens relevans, slutning og vekt. Ettersom de bestemmelsene som skal tolkes følger av et EU-direktiv vil EU-rettslige rettskildeprinsipper legge føringer på hvordan de enkelte rettskildefaktorens relevans og vekt vil bli vurdert i drøftelsene.⁴⁵ Som følge av EU-lovgivningens overnasjonale og autonome karakter blir det ved EU-domstolens tolkning særlig lagt vekt på integrasjonsformål. Dessuten er tolkningslæren mer åpent rettspolitisk enn i de fleste nasjonale retts-systemer. En del andre særtrekk ved tolkningslæren er oppsummert av EU-domstolen i CILFIT-saken⁴⁶ fra 1982. Her er det blant annet de metodemessige problemene mht. EU-rettens flerspråklighet som blir adressert. For tolkningslærens del medfører en slik flerspråklighet at man i tvilstilfeller må sammenligne de ulike språkversjonene. Videre medfører dette at det normalt legges mindre vekt på den eksakte ordlyden enn hva vi er vant til. Ved variasjon i språklige nyanser i de enkelte språkversjoner medfører dette ofte en formålsrettet tolkning fremfor en fintolkning av det enkelte uttrykk. I tillegg til dette fokuserer også redegjørelser i CILFIT-saken på EU-rettens dynamiske

⁴⁵ Se nærmere Sejersted mfl. (1995 kap. 3.1).

⁴⁶ EF-domstolens sak 283/81.

karakter. Denne medfører at eksisterende lovtekster fortrinnsvis skal tolkes dynamisk over tid fremfor å erstattes av ny lovgivning. At enkelte bestemmelser på denne måten får et annet innhold enn det opprinnelige når de blir fortolket over tid er ansett som helt legitimt. Det er nødvendig også å legge merke til at EU-retten ofte opererer med sine egne begreper som nærmest kan sammenlignes med de nasjonale legaldefinisjoner. Disse begrepene har ofte en avvikende betydning fra de tilsvarende nasjonale, og man må se hen til hvordan EU-domstolen har tolket det for å kunne være sikker på hvordan det skal forstås. Denne tolkningsmetoden kalles gjerne for autonom tolkning.

1.10 Finnes det norsk lovregulering av digitale mellomledds ansvar for videreformidling av medkontrahentens ytringer?

Man kan reise spørsmål om det finnes norske regler om informasjonsformidling som kan være anvendelige i forhold til den virksomhet som de digitale mellomledd driver. Spørsmålet faller, som jeg tidligere har nevnt, strengt tatt utenfor oppgaven. For å skape et komplett bilde av e-handelsdirektivets ansvarsregime ser jeg det likevel hensiktsmessig å gi kort redegjørelse for hvilke norske ansvarsregler som kan tenkes å være anvendelige på de digitale mellomledds virksomhet dersom de ikke kommer innunder hovedregelen om ansvarsfrihet i art. 12-14.

På mange områder vil virksomheten til de digitale mellomledd rammes av lovens forskjellige bestemmelser om medvirkningsansvar. Eksempler i denne sammenheng er medvirkningstilleggene til strl.⁴⁷ §§246 og 247. Når det gjelder disse bestemmelsene er spørsmålet om digitale mellomledd kan bli ansvarlig fordi deres virksomhet må anses å utgjøre en medvirkning til ulovlige og krenkende handlinger ved at de besørger den infrastruktur som er nødvendig for å tilgjengeliggjøre og spre ulovlig materiale. En viktig begrensning i denne sammenheng følger av strl. §254 som unntar fra ansvar ærekrenkelse forøvd i «blad eller tidsskrift» eller i «kringkastingssending» dersom medvirkeren bare har deltatt i teknisk fremstilling eller distribusjon av det krenkende materialet. Sistnevnte bestemmelse er en straffrihetsregel, hvilket reduserer betenkelighetene ved en situasjonsbestemt, vid fortolkning av blant annet begrepet «kringkastingssending», slik at det også omfatter informasjonssamfunnstjenester. For sivilrettens område gjøres i skl.⁴⁸ §3-6, 4. ledd samme unntak for krenkelser

⁴⁷ Almindelig borgerlig Straffelov av 22.05.1902 nr. 10 (strl.)

⁴⁸ Lov om skadeserstatning av 13.06.1969 nr. 26 (skl.)

forøvd i blad eller tidsskrift, samt, i annet punktum, for kringkastingssending. Også i dette tilfellet er det gjort unntak for den som bare har deltatt ved teknisk framstilling eller distribusjon av skriftet.

Av de reguleringer som knytter seg til ansvar for videreformidling av informasjon gjennom spesifikke medier, er særlig det såkalte «redaktøransvaret» i strl. §431 fremtredende i norsk rett. I bestemmelsens første ledd reguleres redaktørens ansvar for offentliggjøring gjennom «blad eller tidsskrift», mens tredje ledd utvider anvendelsesområdet til «offentliggjøring gjennom kringkastingssending». Spørsmålet er i vårt tilfelle om regelverket kommer til anvendelse på informasjonssamfunnstjenester slik disse er definert i e-handelsdirektivet, herunder særlig om informasjonssamfunnstjenester er omfattet av begrepet «kringkastingssending». Problemet er komplisert og har ikke funnet noen løsning i norsk rettspraksis. I den juridiske litteraturen er meningene delte på dette punktet.⁴⁹ Som det fremgår av drøftelsen i pkt 2.3.2 trekkes skillet mest hensiktsmessig opp på grunnlag av de reelle hensyn i hvert konkrete tilfelle. Det er derfor klart at resultatet ikke sikkert lar seg forutsi etter gjeldende rett.

For de aktører hvis virksomhet på Internett særlig er å videreformidle informasjon⁵⁰ kan det reises spørsmål om utbredelsen av et eget informasjonsansvar.⁵¹ Læren om dette ansvaret omhandler skader som har fått spesiell aktualitet i informasjonssamfunnet. I henhold til juridisk teori⁵² er vilkårene for å bli kjent ansvarlig i henhold til dette ansvaret, for det første, at den som formidler informasjon gjennom almene kommunikasjonskanaler, som f.eks. en nettside, må ha utvist uaktsomhet. Innlysende er det imidlertid at et ansvar for enhver uaktsom villedning ville være uholdbart fordi det ville favne for vidt. Skadesituasjonen må derfor vurderes som helhet for å se om den skadelidte hadde et særlig grunnlag for tillit til den aktuelle informasjonen. På den ene side kan vi tenke oss tilfeller der det eksisterer kontraktsliknende relasjoner mellom informasjonsformidleren og den skadelidte, slik at det er rimelig å oppstille et krav om lojalitet, og derigjennom en aktsomhetsplikt. I et slikt tilfelle er det lett å argumentere for et ansvar dersom den informasjon som skadelidte måtte stole på var gal, og dette skyldtes uaktsomhet fra informa-

⁴⁹ Se drøftelsene til Einstabland (1992 s. 105-113)

⁵⁰ Eksempel på dette kan være den virksomhet som jeg har beskrevet at leverandøren av proxy caching-tjenester (se pkt 1.6.4) driver. Her kan informasjon om faktiske forhold som værmeldinger, trafikkmeldinger, prissammenlikninger, karttjenester, etc. ligge midlertidig tilgjengelig for tredjemenn på proxy serveren.

⁵¹ Læren om informasjonsansvaret, eller ansvar for villedning av annen enn kontraktspart, er beskrevet av Hagstrøm (1989 s. 196-220)

⁵² Se Hagstrøm (1989 s. 200 flg.).

sjonsformidlerens side. På den annen side kan vi tenke oss tilfeller der skadelidte har fått nyss om den aktuelle informasjonen, uten at det var meningen at han skulle kjenne til den. Her er et ansvar utvilsomt mindre fordøyd, selv om informasjonsformidleren har vært uaktsom. Eksempel på et tilfelle der informasjonsansvaret er anvendelig kan vi tenke oss i tilfellet der en leverandør av proxy caching-tjenester, som pga. mangelfulle oppdateringsrutiner fortsatt tilbyr en nettside som han vet er blitt fjernet fra nettverket fordi den inneholder skadelig informasjon, kan bli ansvarlig i henhold til informasjonsansvaret dersom skadelidte hadde tilstrekkelig grunn til å stole på den formidlede informasjonen.⁵³

Som et eksempel på at bransjenormer for internettaktører er under utvikling i norsk rett nevner jeg særlig ett eksempel der forskjellige bransjeorganisasjoner⁵⁴ har gått sammen og dannet et Internett-etisk råd, nemlig Nettnemda. Nemda trådte i funksjon 8. februar 01 etter stiftelsesmøte i Telenors lokaler. Det kan best sammenliknes med Pressens faglige utvalg (PFU), men i motsetning til PFU skal det ha myndighet til å stenge nettsteder som bryter norsk lovgivning. Den type myndighet som vi her ser lagt til et uavhengig organ, kommer i fremtiden trolig til å være en viktig pådriver i utviklingen av bransjestandarder og kutymer for internettbransjen i Norge. Så stor rettskildemessig vekt vil ikke rådets avgjørelser ha, men på sikt vil de likevel kunne være med på utforme sedvanerett.

⁵³ Som vi skal se nedenfor er heller ikke e-handelsdirektivets vilkår for ansvarsfrihet for leverandøren av proxy caching-tjenester oppfylt dersom han ikke stenger tilgangen til informasjon som han vet er blitt fjernet fra nettverket. I dette tilfellet er derfor ikke e-handelsdirektivets bestemmelser til hinder for at ansvar blir pålagt med hjemmel i villedningsansvaret.

⁵⁴ Disse organene er internettaktørenes interesseorganisasjon, IKT-Norge, og Statens filmtilsyn

2. ANSVARSREGLENE I E-HANDELSDIREKTIVETS ART. 12-14

2.1 Innledning

Drøftelsene som følger nedenfor har som siktemål å avgjøre hvorvidt de forskjellige aktivitetene som jeg har beskrevet i punkt 1.6 er omfattet av bestemmelsene i e-handelsdirektivets art. 12-14. Dersom det viser seg at den enkelte virksomhet er omfattet av direktivets bestemmelser, skal jeg drøfte meg gjennom en rekke relevante, praktiske problemstillinger som er egnet til å illustrere i hvilken utstrekning den funksjon som mellomledet utøver vil kunne føre til risiko for ansvarsgjennombrudd for tjenesteyteren. Et slikt opplegg gjør det vanskelig å få belyst alle aspekter ved det ansvarsregime som oppstilles i direktivet. Mitt hovedformål med fremstillingen er av denne grunn å trekke frem de problemer som det kan være praktisk nyttig å få en avklaring på sett fra både tjenestemottagernes og tjenesteyternes side.

Før jeg går nærmere inn på forholdet mellom de virksomheter som jeg har beskrevet i punkt 1.6 og bestemmelsene i direktivets art. 12-14, skal jeg i punkt 2.2 knytte noen generelle kommentarer til ansvarsregimet som oppstilles.

2.2 En oversikt over ansvarsregimet som oppstilles i e-handelsdirektivets art. 12-14

2.2.1 Presisering og avgrensning av ansvarsreglene i art. 12-14

E-handelsdirektivet oppstiller som hovedregel at de digitale mellomledd som opptrer i en av de mellommannsfunksjonene som det gjøres rede for i art. 12-14, bestemmelsenes 1. pkt., skal være ansvarsfrie for videreformidling av informasjon som er skaffet til veie av deres tjenestemottagere. Med ansvarsfrihet menes at ansvar aldri skal anses for å være inntrådt.⁵⁵ Kun de virksomheter som er omfattet av anvendelsesområdet for art. 12-14, og som oppfyller alle vilkårene i disse bestemmelsene, vil nyte godt av ansvarsfriheten. Det er ikke dermed sagt at de virksomheter som faller utenfor anvendelsesområdet automatisk blir ansvarlige. Dersom betingelsene for ansvarsfrihet ikke er oppfylt, vil

⁵⁵ Parallellen til strafferettens straffrihetsgrunner er her klar.

et eventuelt ansvar helt og holdent bero på hvorvidt det finnes et ansvarsgrunnlag i hver enkelt medlemsstats materielle rett. Dersom det etter nasjonal rett viser seg at en handling verken er ulovlig eller krenkende, eller at det finnes regler som fritar det digitale mellomleddet fra ansvar på et annet grunnlag, vil handlingen være like ansvarsfri som før e-handelsdirektivet ble vedtatt.

Det følger av ordlyden i art. 12-14, bestemmelsenes 1. pkt, sammenholdt med preambelens punkt (42) at hovedregelen om ansvarsfrihet kun skal gjelde der aktiviteten til det digitale mellomledd begrenser seg til den tekniske prosessen som består i å operere og skaffe aksess til et nettverk der den informasjon som oversendes er skaffet til veie av tjenestemottageren, og oversendelsen eller lagringen av informasjonen skjer på forespørsel fra tjenestemottageren. Denne aktiviteten må kun være av en teknisk, automatisk og passiv natur, noe som impliserer at tjenesteyteren verken har kunnskap om, eller kontroll over den informasjon som oversendes. Med andre ord unntar ikke direktivet fra ansvar noen aktivitet fra tjenesteyterens side som innebærer utvelgelse, endring eller produksjon av informasjon. En naturlig forståelse av et slikt regime er at bestemmelsene er ment for å beskytte visse, utvalgte typer virksomhet, slik disse er beskrevet i e-handelsdirektivet. Dersom en aktør forlater denne rollen, vil han ikke lenger nyte godt av ansvarsfriheten og risikerer derfor ansvar. Etableringen av et slikt ansvarsregime virker styrende på aktører i internettbransjen. Meningen er at man skal oppnå positive effekter for informasjonsflyten, både ved at ytringsfriheten sikres fordi mellomleddene ikke har noe incitament til å sensurere den informasjon som passerer gjennom deres fasiliteter og at internettinfrastrukturen sikres god funksjonalitet ved at mellomleddene ikke behøver å iverksette tids-, og kapasitetskrevenne kontrollmekanisme. Gjennom en slik samordning av de nasjonale regelverk fjernes hindringer for informasjonsflyt i EUs indre marked, og internettaktørenes konkurranseevne i forhold til f.eks. amerikanske bransjeaktører bedres.

Reguleringene i e-handelsdirektivet er, som tidligere nevnt, i utgangspunktet teknologinøytrale. Dette innebærer at ansvarsfrihet kan foreligge uavhengig av hvilken teknologiplattform som brukes for å formidle informasjonen så lenge den tjeneste som ytes er en informasjonssamfunnstjeneste i direktivets forstand, og så lenge de andre vilkårene for ansvarsfrihet i art. 12-14 er oppfylt. Hvilke tjenester som faller innunder begrepet informasjonssamfunnstjeneste, samt hvilke virksomheter som er omfattet av de nevnte artiklene, skal jeg komme tilbake til nedenfor.

Reglene i art. 12-14 krever en kommentar når det gjelder adgangen til å gripe inn med tvangsmidler mot det digitale mellomleddet. Jeg vil presisere at adgangen til å bruke tvangsmidler er et prosessuelt virkemiddel, og har derfor

ikke noe å gjøre med hvorvidt det materielt sett kan sies å foreligge et ansvar. Det fremgår av art. 12-14, siste ledd, sammenholdt med preambelens punkt (45) at e-handelsdirektivets ansvarsbegrensninger ikke skal hindre beslutninger fra en domstol eller en offentlig myndighet som er påkrevet for å få tjenesteteyteren til å stanse eller motvirke en krenkelse. Bestemmelsen retter seg særlig mot tilfeller der det er tvil rundt ansvarsfrihetsspørsmålet etter art. 12-14, eller der det ikke er tid til å vente på en avgjørelse fra rette myndighet, og der den informasjon som oversendes likevel er krenkende eller ulovlig, slik at eventuelle rettighetshavere eller skadelidte står i fare for ytterligere krenkelser. Muligheten til å gripe inn ved hjelp av prosessuelle midler er blitt klarere i det endelige, vedtatte direktivet enn det var i henhold til Kommisjonens bearbejdede forslag til e-handelsdirektiv⁵⁶, ettersom den aktuelle passusen er blitt flyttet til siste punkt i hver av artiklene 12-14. Av en omformulering fremgår videre den presiseringen at de beslutninger som i direktivforslaget omtales som «prohibitory injunctions» også skal omfatte alle de typer avgjørelser som tvisteløsningsorganer etter nasjonal rett finner nødvendige for å stanse eller motvirke en krenkelse. I e-handelsdirektivets art. 12-14, alles siste pkt., samt i preambelens punkt (45), annen passus, fremgår det nå at ikke bare de beslutninger som er fattet av retten, men også avgjørelser som er fattet av administrative myndigheter, f.eks. av den nasjonale forvaltningen, eller spesifikt opprettede kontroll-, og tvisteløsningsorganer (jfr. art. 17, nr. 2), kan tillates håndhevet i forhold til de digitale mellomledd som er omfattet av bestemmelsene om ansvarsfrihet i direktivet.

I art. 14, nr. 3, siste passus, sies det at reglene om ansvarsfrihet i artikkelen heller ikke skal påvirke medlemsstatenes muligheter til å etablere prosedyrer for fjerning av informasjon, eller stenging av tilgang til informasjon. Jeg presiserer at mulighetene til å etablere slike prosedyrer kun gjelder i forhold til den virksomhet som faller innenfor anvendelsesområdet for art. 14. En slik regel medfører, slik det er naturlig å forstå den, at skal være mulig for medlemsstatene å etablere nasjonale ordninger for å fjerne informasjon, eller stenge tilgangen til informasjon, uavhengig av om vilkårene for ansvarsfrihet i art. 14 er oppfylt.⁵⁷ Også denne regelen er uttrykk for det behov for en sikkerhetsventil som eksisterer i forbindelse med å hindre ytterligere krenkelser av tredjemanns rettigheter. Eksempel på tilfeller der behovet kommer til syne er der det tar tid å få avgjort hvorvidt den informasjon som tilbys er ulovlig

⁵⁶ Amended proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the Internal Market.

⁵⁷ En slik prosedyre for fjerning eller stenging av tilgang til informasjon er beskrevet i oppgavens del 3, der jeg redegjør for det som populært kalles et «notice-, and take down-regime».

eller krenkende og hosteren ikke selv tar initiativ for å fjerne tilgangen til den. Bestemmelsen kan ses i sammenheng med art. 17, nr. 2 som fastslår at medlemsstatene skal oppfordre til dannelsen av organer for utenrettslig konfliktløsning.

2.2.2 For hvilke av tjenestemottagerens handlinger er digitale mellomledd ansvarsfrie etter e-handelsdirektivets art. 12-14?

E-handelsdirektivet legger som vi skal se opp til en horisontal regulering i forhold til hvilke av tjenestemottagerens handlinger digitale mellomledd skal være ansvarsfri i forhold til. Dette innebærer at hovedregelen om ansvarsfrihet gjelder uavhengig av på hvilket grunnlag tjenestemottagerens atferd er krenkende eller ulovlig. Herunder omfattes tjenestemottagerens brudd på alle de regelverk som jeg har skissert i punkt 1.7. En slik horisontal regulering er ikke kommet klart til uttrykk i e-handelsdirektivet. Ansvarsregimet i art. 12-14 må imidlertid ses i sammenheng med fraværet av en generell undersøkelsesplikt i art. 15. Dersom tjenesteyterens ansvar skulle være avhengig av hvilken type krenkende eller ulovlig handling tjenestemottageren har foretatt, ville dette gjøre fraværet av en generell undersøkelsesplikt i art. 15 illusorisk. Et ansvarsregime som oppstiller forskjellig ansvarstandarder avhengig av hvilken del av den underliggende, materielle retten som er medkontrahenten har krenket vil oppfordre de digitale mellomleddene til å innføre overvåkningsregimer for den informasjon som passerer gjennom deres fasiliteter, og på denne måten effektivt true effektivitet og integritet ved oversendelse av informasjon.

Det har under lovgivningsprosessen vært reist enkelte innvendinger mot Kommisjonens kompetanse til å regulere nasjonal strafferett på den måten som e-handelsdirektivet gjør.⁵⁸ Så langt det er nødvendig for å fjerne hindringer i EUs indre marked kan det imidlertid ikke være betenkelig å overlate utarbeidelsen av regler om ansvarsfrihet til Kommisjonen. At e-handelsdirektivets formål med å regulere nasjonal strafferett ikke strekker seg lenger enn til å samordne reglene for EUs indre marked har støtte i direktivets preambel, punkt (8) som understreker at formålet med e-handelsdirektivet er å skape et rettslig rammeverk som skal sørge for fri bevegelse av informasjonssamfunnstjenester mellom medlemsstatene, og ikke for å harmonisere strafferettsområdet i seg selv. Sett fra norsk side reiser under enhver omstendighet ikke en overnasjonal regulering av strafferettens område på e-handelsdirektivets premisser så store betenkeligheter sålenge det er snakk om å implementere straffrihetsregler.

⁵⁸ Det er på det rene at en horisontal regulering av ansvarsfrihet for digitale mellomledd også vil omfatte en viss regulering av nasjonal strafferett ettersom ansvarsfriheten også skal omfatte de tilfeller der tjenestemottageren bryter mot strafferettlige regler.

Grunnen til dette er blant annet at lovskravet på strafferettens område ikke gjør seg gjeldende i dette tilfellet.

2.2.3 Andre retningslinjer for gjennomføringen av e-handelsdirektivet i norsk rett

E-handelsdirektivet er et minimumsdirektiv i den forstand at nasjonalstatene som et minstekrav må implementere regler om ansvarsfrihet som strekker seg minst like langt som etter e-handelsdirektivet, og som altså ikke gir uttrykk for et strengere ansvarsregime. Denne forståelsen underbygges av direktivets preambel, punkt (10), som gir uttrykk for at tiltakene i direktivet, i tråd med det EU-rettslige proporsjonalitetsprinsippet, er strengt begrenset til det minste som er nødvendige for å oppnå et indre marked som fungerer tilfredsstillende. I tillegg må dette også følge logisk av direktivets system, ettersom et strengere ansvarsregime, slik jeg har redegjort for over, langt på vei vil være egnet til å legge en demper på ytringsfriheten og på den teknologiske funksjonaliteten til Internett.

2.3 Fellesfortolkninger av begrep i art. 12-14

2.3.1 Innledning

E-handelsdirektivets art. 12-14 inneholder en rekke begrep som er felles for de tre bestemmelsene. Disse begrepene undergir jeg av praktiske grunner en felles fortolkning før jeg går over til å drøfte om hver enkelt av de virksomheter som jeg har beskrevet i punkt 1.6 kan subsumeres under de fortolkninger jeg kommer frem til.

Begrepene jeg skal undergi felles fortolkning er definert i e-handelsdirektivets art. 2, som sammen med preambelens punkt (17) og (18) henviser til EU-direktiv 98/34/EC som er sammenslått med og endret ved EU-direktiv 98/48/EC.⁵⁹

2.3.2 Tolkning av begrepet «Information Society service»?

I henhold til e-handelsdirektivets artikkel 2, litra (a), jfr. preambelens nr. (17) og (18) skal begrepet Information Society service, heretter informasjonssamfunnstjeneste, omfatte tjenester som ligger innenfor betydningen av art. 1, nr. 2 i definisjonsdirektivet. Etter denne bestemmelsen skal en informasjonssam-

⁵⁹ EU-dir. 98/34/EC, sammenslått og endret ved EU-dir. 98/48/EC. EFT, endret ved EU-dir. 98/48/EC. Heretter: «definisjonsdirektivet»

funnstjeneste omfatte «any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of the service».

Det første vilkår for at en tjeneste skal være en informasjonssamfunnstjeneste er etter definisjonsdirektivets art. 1 punkt 2, 1. ledd er at tjenesten normalt sett ytes mot vederlag, «normally provided for remuneration».

I den danske oversettelsen av definisjonsdirektivet brukes ordet «betaling» der det engelske utkastet bruker ordet «remuneration». Selv alle de offisielle språkversjoner av e-handelsdirektivet i utgangspunktet skal være likeverdige kan den språklige tolkningen etter min mening bli klarere dersom man søker støtte i flere av de forskjellige utgavene. På bakgrunn av en slik tankegang kan det synes som om det danske utkastet oppstiller et noe snevrere anvendelsesområde enn det engelske. Vilkåret om «betaling» synes å forutsette at det skjer en konkret overføring av verdier mellom de to involverte parter. Såvidt jeg kan forstå har det engelske uttrykket «remuneration» en noe videre betydning, slik at også et mer nøytralt begrep som kompensasjon må sies å omfattes. Sistnevnte oppfatning fører til at et bredere spekter av økonomisk aktivitet kommer innunder direktivets anvendelsesområde. Denne forståelsen er også den som er mest i overensstemmelse med uttalelsene i e-handelsdirektivets preambel (se under). Etter ordlyden skulle det derfor fremgå at det ikke er avgjørende om vederlag faktisk ytes i det individuelle tilfelle. Avgjørende må være om tjenesten er av en slik art at det vanligvis ytes en kompensasjon for den.

I e-handelsdirektivets preambel punkt (18) fremgår det at informasjonssamfunnstjenester ikke er begrenset til tjenester som forutsetter on-line kontraktsinngåelser, men også, ihvertfall så lenge det dreier seg om utøvelse av økonomisk aktivitet, omfatter tjenester som ikke blir betalt av de som mottar dem. Av bestemmelsen fremgår verken hvilken type vederlag som må foreligge eller hvem vederlaget må komme fra for at vilkåret om økonomisk aktivitet skal være oppfylt. Dersom formidling av informasjonstjenester betinger at brukeren f.eks. aksepterer å motta direkteklame, vil dette innebære en forpliktelse som har klar økonomisk verdi på linje med en overføring av penger, og vederlag i direktivets forstand må derfor sies å foreligge. På samme måte innebærer formidling av reklamefinansierte tjenester at vederlaget for tjenesten betales av de som har økonomisk interesse i å drive markedsføring overfor brukeren. I begge disse tilfeller må vilkåret om at tjenesteformidlingen skal skje mot vederlag være oppfylt. I Romatraktatens art. 60 benyttes også definisjonen «normally provided for remuneration». Definisjonen av informasjonssamfunnstjenester kan ikke ses løsrevet fra dette. Uttrykket er i EU-

retten tolket svært vidt.⁶⁰ Både tjenester som leveres gratis og salg av varer og tjenester dekkes. Eksempler i denne sammenheng er gratis e-posttjenester, søkemotortjenester mv. I motsetning til dette kan jeg nevne tjenester som utelukkende skjer off-line, slik som for eksempel levering av fysiske varer. Det skulle etter dette være klart at e-handelsdirektivets vilkår om at informasjonssamfunnstjenesten skal ytes mot vederlag ikke kan tolkes særlig strengt.

For det andre er det et vilkår at en informasjonstjeneste ytes «at a distance». I henhold til art. 2 nr. 1 innebærer dette at tjenesten blir tilskaffet uten at partene er «simultaneously present». Denne passusen reiser spørsmål om i hvilken grad det må innfortolkes en tidsmessig såvel som en stedlig begrensning i hva som skal anses som en informasjonssamfunnstjeneste. Mest mening gir vilkåret dersom det tolkes dithen at kun de tjenester som ytes mens partene er samtidig til stede på samme sted anses for å falle utenfor begrepet. Denne løsningen fremgår også av tillegg V til definisjonsdirektivet som bestemmer at nærmere bestemte tjenester som blir tilskaffet under fysisk tilstedeværelse av både tilbyder og mottager ikke regnes som en informasjonssamfunnstjeneste selv om partene gjør bruk av elektroniske midler for å kommunisere. De tjenester som på denne måten faller utenfor direktivets anvendelsesområde er: litra (a) medisinsk undersøkelse eller behandling med elektroniske midler på en operasjonssal der pasienten er fysisk til stede, (b) gjennom søkingen av en elektronisk katalog i en butikk der kunden er til stede, (c) reservasjon av flybilletter ved hjelp av et computernetttverk i et reisebyrå under fysisk tilstedeværelse av kunden, (d) elektroniske spill som blir gjort tilgjengelige der kunden er fysisk til stede. Utenom de oppregnede tilfellene vil altså tjenester som blir ytet med elektroniske midler mens partene er fysisk til stede kunne sies å være tilveiebrakt «at a distance». Et naturlig unntak fra dette gjøres imidlertid i e-handelsdirektivets preambel, punkt (18), siste passus, der det sies at aktiviteter som etter sin beskaffenhet ikke kan bli utført «at a distance» og «by electronic means» ikke utgjør en informasjonssamfunnstjeneste. Som eksempler her nevnes medisinsk rådgivning som krever undersøkelse av pasienten og lovpålagt regnskapsrevisjon.

For det tredje må en informasjonssamfunnstjeneste være tilskaffet «by electronic means». Etter art. 1 nr. 2 menes med denne passusen at tjenesten opprinnelig er sendt fra og mottatt ved sin destinasjon med elektronisk verk-tøy som er egnet til å utføre databehandlingsoperasjoner (her inkl. digital komprimering) og lagring av data. Videre må tjenesten i sin helhet avsendes, overbringes og mottas via kabel, radiosignaler, optiske fiberkanaler eller ved elektromagnetiske midler. I denne sammenheng presiseres det i direktivets

⁶⁰ Se EF-domstolens sak 109/92, domsgrunn 15 og sak C-352/85, domsgrunn 16

preambel punkt (18) at informasjonssamfunnstjeneste omfatter økonomiske aktiviteter som finner sted on-line. Som eksempel nevnes typisk salg av varer over Internett. I kontrast til dette fremgår det at off-line aktiviteter som levering av de bestilte varer, isolert sett, ikke er omfattet. I dette ligger det også en forutsetning om at den aktuelle aktivitet må være knyttet opp til bruken av elektroniske hjelpemidler.

For det fjerde må tjenesten i hht. art. 1 nr. 2 i definisjonsdirektivet være utført «at the individual request of a recipient of the services». Dette innebærer at informasjonssamfunnstjenesten må være tilskaffet etter en individuell forespørsel fra en tjenestemottager.

Etter ordlyden avgrenses det her mot de tilfeller der det oversendes data uten at det foreligger en konkret og personlig forespørsel fra en som ønsker å motta tjenesten.

I e-handelsdirektivets preambel, punkt (18) avgrenses uttrykket mot kringkastingstjenester som fjernsynskringkastingstjenester som er omfattet av art. 1, pkt (a) i EU-direktiv 89/552/EEC⁶¹ (tv-radiospredning over kabel eventuelt trådløst, også via satellitt i kodet eller ukodet form av fjernsynsprogrammer) radiokringkasting ikke er omfattet av definisjonen av informasjonssamfunnstjeneste. Avgrensningen begrunnes med at radiokringkasting og fjernsynskringkasting ikke er tjenester som blir tilskaffet på individuell forespørsel, jfr. definisjonsdirektivets art. 1, punkt 2, 2. ledd, 3. strek.

Den samme avgrensningen fremgår av definisjonsdirektivets art. 1 nr. 2 ved at direktivet unntar radiokringkastingstjenester og fjernsynskringkastingstjenester som er omfattet av EU-direktiv 89/552/EEC. I vedlegg V, punkt 3 til definisjonsdirektivet fremgår det videre at tjenester som skaffes til veie ved oversendelse av data og som mottas samtidig av et ubegrenset antall individer uten individuell forespørsel (point to multipoint transmission), ikke skal regnes for en informasjonssamfunnstjeneste. I punkt 3, litra a-c nevnes som eksempler fjernsynskringkastingstjenester, teletekst (tekst-TV) og radiokringkastingstjenester. Også dette begrunnes med at tjenesten ikke anses yet «at the individual request of a recipient of the service». Imidlertid fremgår det her at tjenester som blir oversendt «point to point» slik som formidling av videofilmer på forespørsel eller direktemarkedsføring via elektronisk post skal være å regnes for å være en informasjonssamfunnstjeneste.

Som fremhevet av Lloyd⁶² allerede i 1995, er grensen mellom on-line informasjonstjenester og kringkastingstjenester i ferd med å utviskes. Etter Lloyds mening er essensen av en on-line tjeneste at kommunikasjon mellom

⁶¹ EU-dir.89/552/EEC Sist endret ved EU-dir. av 97/36/EC

⁶² Lloyd (1995 s. 273-274).

en informasjonstjenesteyter og en bruker (eller en gruppe brukere) foregår i sanntid via et kommunikasjonsmedium. Slike on-line tjenester kan etter Lloyds mening skilles fra kringkastingstjenester ved at førstnevnte tillater brukeren å interagere med tjenesten. Av dette skulle det fremgå at nyvinninger som f.eks. tekst-TV må falle utenfor begrepet informasjonssamfunnstjeneste. Selv om brukeren har muligheten til å motta tekstsider, så har han ingen mulighet til å påvirke skjermbildet, og tilfellet er parallelt med de situasjoner der brukeren har mulighet til å velge program på fjernsynsapparatet. Imidlertid vil en slik oppfatning føre til å de ovenfor omtalte point to point-tjenestene også skulle falle innunder kringkastingsbegrepet. Heller ikke i disse tilfellene tillates det jo noen interaksjon med tjenesten. En slik løsning ville imidlertid være i strid med e-handelsdirektivets preambel nr. (18) som uttrykkelig sier at disse tjenestene skal omfattes.

I norsk juridisk teori er spørsmålet særlig drøftet av Einstabland.⁶³ Han konkluderer sin drøftelse av hvorvidt man kan betrakte teledata⁶⁴ som kringkasting med at de vilkår som oppstilles i legaldefinisjonen i kringkastingslovens⁶⁵ §1-1, 1. ledd er oppfylt. Imidlertid mener han at det å betrakte teledata som kringkasting kan synes noe fremmed i forhold til kringkastingslovgivningen generelt, og at det ikke er i takt med gjeldende praktisering av konsesjonsplikten. En klar grensdragning krever derfor etter Einstablands syn en mer inngående vurdering av de reelle hensyn som ligger bak reglene

Etter min mening synes det ut fra de foreliggende rettskilder, og da særlig med henblikk til Lloyds argumentasjon, naturlig å skille informasjonssamfunnstjenester fra kringkastingstjenester ved hjelp av to parametere. For det første må det være et krav at den aktuelle tjeneste tillater en viss interaksjon mellom tjenesteyter og brukeren. For det andre må det være et krav at tjenesten skjer «point to point» og ikke «point to multipoint», det vil si at interaksjonen må skje på et individuelt plan. Imidlertid er jeg enig med Einstabland i at en klar grensdragning ikke kan foretas uten en grundigere analyse av de reelle hensyn som ligger bak reglene. Det vil imidlertid føre for langt å gå nærmere inn på denne problemstillingen i dette dokumentet.

Som en oppsummering av denne drøftelsen kan det se ut som Kommisjonen ved å innføre begrepet informasjonssamfunnstjeneste har forsøkt å benytte et ord som dekker langt de fleste tjenester er tjenesteyteren bruker informasjons-, og kommunikasjonsteknologi som en del av sin økonomiske

⁶³ Se drøftelsene i Einstabland (1992 s. 105-113)

⁶⁴ Ut fra den definisjon som Einstabland (1992) opererer med synes det ikke tvilsomt at begrepet teledata også omfatter informasjonssamfunnstjenester i e-handelsdirektivets forstand, se særlig s. 105-106.

⁶⁵ Lov om kringkasting 14.04.1992, nr. 127 (kringkastingsloven)

virksomhet. Hvor grensen skal trekkes er vanskelig å svare konkret på, men definisjonen av en informasjonssamfunnstjeneste i e-handelsdirektivets forstand er dynamisk, og vil fort få et fastere innhold.

2.3.3 Tolkning av begrepet «recipient of the service»

I e-handelsdirektivets art. 2, litra (d) menes med «recipient of the service», heretter også tjenestemottageren, enhver fysisk eller juridisk person som i profesjonelt øyemed og ellers bruker en informasjonssamfunnstjeneste særlig med det formål å søke informasjon eller gjøre informasjon tilgjengelig. Etter denne definisjonen er det klart at så vel fysiske personer som selskap, organisasjoner og foreninger kan være mottager av tjenesten i direktivets forstand. Videre er det likegyldig om den virksomheten som mottageren av tjenesten driver er kommersiell eller ikke. I denne sammenhengen er det klart at også forbrukere vil falle innunder begrepet. Denne forståelsen finner støtte i e-handelsdirektivets preambel, punkt (20), der det fremgår at definisjonen av en tjenestemottager skal dekke alle typer bruk av informasjonssamfunnstjenester, både av personer som skaffer informasjon til åpne nettverk som Internett og av personer som søker informasjon på Internett av private eller profesjonelle grunner.

Den definisjon av begrepet «recipient of the service» som direktivet oppstiller kan virke noe forvirrende på grunn av den doble betydningen som fortolkningen gir anvisning om. Jeg finner det derfor nødvendig å klargjøre visse aspekter ved min bruk av begrepet.

Når det gjelder min omtale av de aktører som bruker mellomleddenes tjenester for å gjøre informasjon tilgjengelig skal jeg ved drøftelsen av problemstillinger i forhold til artiklene 12-14 holde meg mest mulig til direktivets begrepsbruk, nemlig «recipient of the service», eller tjenestemottager. Imidlertid alternerer jeg noen steder med begrepene medkontrahent eller kunde. I de tilfellene der jeg omtaler de aktører som bruker mellomleddenes tjenester for å søke informasjon benytter jeg hovedsakelig begrepene tredjemann eller bruker.

2.3.4 Tolkning av e-handelsdirektivets begrep «service provider»

I henhold til e-handelsdirektivets art. 2, litra (b) er en «service provider», heretter også tjenesteyter, enhver fysisk eller juridisk person som fremskaffer en informasjonssamfunnstjeneste. I denne sammenheng omfattes så vel fysiske personer som selskap, organisasjoner og foreninger. Det oppstilles ingen krav til målsetningen for tjenesteyterens virksomhet utover det som fremgår når man sammenholder begrepet tjenesteyter med definisjonen av en informasjonssamfunnstjeneste, der det stilles krav til at den aktuelle tjeneste må

ytes i sammenheng med en økonomisk aktivitet. På denne bakgrunn vil vurderingen av hvorvidt en utøver av de ovenfor beskrevne virksomheter kan sies å være en tjenesteyter i e-handelsdirektivets forstand langt på vei være avhengig av hvorvidt den virksomheten han driver lar seg karakterisere som en informasjonssamfunnstjeneste. Denne vurderingen skal jeg komme tilbake til når jeg nedenfor vurderer hver av de i punkt 1.6 beskrevne virksomheter opp mot art. 12-14 i e-handelsdirektivet.

2.3.5 Tolkning av e-handelsdirektivets begrep «communication network»

Art. 12 og 13 gir ikke særlige holdepunkter for hva som skal forstås med begrepet «communication network», heretter også kommunikasjonsnettverk eller nettverk. Imidlertid kan man slutte fra ordlyden i art. 12 og 13 sammenholdt med definisjonen av en informasjonssamfunnstjeneste at det må dreie seg om et nettverk som tillater elektronisk kommunikasjon uten at partene er til stede samtidig og som tillater at brukeren interagerer med de forskjellige tjenester. Det er på det rene at en slik definisjon omfatter både åpne nettverk, som Internett, og lukkede, interne nettverk som for eksempel bedrifters intranett.

2.4 Spørsmål om ansvarsfrihet for den virksomhet som i punkt 1.6.2 er beskrevet som aksessleverandør

2.4.1 Hjemmel

Dersom en informasjonssamfunnstjeneste som består i å skaffe tilveie aksess til et kommunikasjonsnettverk blir ytet skal tjenesteyteren etter e-handelsdirektivets art. 12, nr. 1 som utgangspunkt ikke risikere ansvar for den informasjon som er frembrakt av tjenestemottageren og som blir oversendt gjennom nettverket. Imidlertid forutsetter ansvarsfriheten at tjenesteyterens virksomhet ikke strider mot noen av vilkårene i artikkelens nr. 1, litra (a)-(c). Her fremgår det at ansvarsfriheten gjelder så lenge aksessleverandøren (a) ikke initierer oversendelsen, (b) ikke velger ut mottageren av oversendelsen og (c) ikke velger ut eller endrer den informasjonen som inngår i oversendelsen. Den aksessleverandører som oppfyller disse tre vilkårene vil oppfylle kriteriene til å være «mere conduit», og kan ikke blir gjort ansvarlig for ulovlig eller krenkende informasjon som er lagt ut på nettverket av tredjemenn. Dette betyr at tjenesteyteren kun risikere ansvar dersom han bryter mot ett av vilkårene i litra (a)-(c).

2.4.2 Omfattes levering av aksess, slik den er beskrevet i punkt 1.6.2, av e-handelsdirektivets art. 12?

For det første er det et vilkår at tilskaffelsen av aksess oppfyller kravene som e-handelsdirektivet oppstiller for at tjenesten skal være en informasjonssamfunnstjeneste. Aksessleverandøren er som tidligere nevnt det mellomledd som skaffer brukeren tilgang til Internett gjennom sin(e) server(e). Spørsmålet er om denne tjenesten faller inn under den tolkningen av begrepet informasjonssamfunnstjeneste som fremgår av punkt 2.3.2. I denne sammenheng er problemet om tilveieskaffelsen av aksess er en tjeneste som normalt sett ytes mot vederlag, på avstand, ved elektroniske midler og etter individuell forespørsel fra tjenestemottageren.

Det første man her må vurdere er hvorvidt aksess tjenestene er av en slik art at de normalt ytes mot vederlag. Når det gjelder tilveieskaffelse av aksess som forutsetter at tjenestemottageren betaler et månedlig beløp, kan det ikke være særlig tvilsomt at vilkåret om vederlag er innfridd. Spørsmålet om gratis aksess tilskaffelse omfattes av direktivets bestemmelser volder noe større problemer. Jeg er i tolkningen av vederlagsbegrepet i punkt 2.3.2 kommet til at det avgjørende ikke kan være hvorvidt vederlag faktisk ytes i et konkret tilfelle, så lenge det dreier seg om utøvelsen av en form for økonomisk aktivitet. Det er i denne sammenheng på det rene at den vederlagsfrie tilveieskaffelsen av aksess, i hvert fall i de tilfellene jeg kjenner, forutsetter at tjenestemottakerens grensesnitt mot Internett inneholder en eller flere reklamebannere tilhørende aksessleverandørens samarbeidspartnere. På denne måten er det klart at også den vederlagsfrie aksess tilskaffelsen representerer en økonomisk virksomhet fordi samtykke til mottak av reklame kan sies å utgjøre vederlag for bruk av aksess tjenesten.

Når det gjelder vilkåret om at tjenesten må være ytet på avstand er dette ment å trekke opp grensen mot de tilfeller der tjenesteyter og tjenestemottaker er på samme sted til samme tid og at det av den grunn er naturlig å snakke om personlig utførte tjenester. Det er på det rene at tilveieskaffelse av aksess, slik jeg over har beskrevet virksomheten, er en tjeneste som ytes på avstand etter som tjenesteyteren og tjenestemottageren ikke er tilstede samtidig.

Vilkåret om at en informasjonssamfunnstjeneste må skje med elektroniske midler volder ikke problemer i forhold til tilveieskaffelse av aksess fordi all kontakt mellom tjenestemottageren og aksessleverandøren skjer ved at kunden kommuniserer via en datamaskin med aksessleverandørens server gjennom de kabler og det nettverk som til enhver tid er nødvendige for å koble seg opp mot Internett.

Den vanlige fremgangsmåten som benyttes for å skaffe seg aksess til Internett skjer ved utsendelse av data fra aksessleverandørens server til aksessmot-

takerens brukermaskin, noe som er betinget av at sistnevnte aktivt har tatt initiativ til dette, samt at aksessen kun gjelder et begrenset antall personer, det vil si de som har adgang til brukermaskinen. I denne sammenheng kan det ikke være tvil om at vilkåret om at aksessstilskaffelsen skal skje på individuell forespørsel fra tjenestemottakeren er oppfylt. Det er på denne bakgrunn ikke tvilsomt at den virksomhet som jeg beskriver at aksessleverandøren driver er en informasjonssamfunnstjeneste i e-handelsdirektivets forstand.

For det annet er det et vilkår at den informasjon som oversendes i nettverket et skaffet til veie av en mottager av informasjonssamfunnstjenesten. Dette vilkåret er ment å avgrense mot de tilfeller der tjenesteyteren selv må regnes som innholdsleverandør. På bakgrunn av de faktiske forutsetningene i punkt 1.6.2 ovenfor kan det ikke være tvilsomt at det er tjenestemottageren som oversender informasjonen i nettverket.

For det tredje oppstilles det et krav om at informasjonssamfunnstjeneste må bestå av en oversendelse i et kommunikasjonsnettverk. Heller ikke i dette tilfellet er det tvilsomt at Internett konstituerer et kommunikasjonsnettverk i e-handelsdirektivets forstand.

Konklusjonen er at aksessleverandørens virksomhet er omfattet av e-handelsdirektivets art. 12.

2.4.3 Oppfyller aksessleverandøren kravene til å være en «mere conduit» i forhold til den informasjonen som er skaffet til veie av hans medkontrahent dersom han forhåndsprogrammerer slik at hans hjemmeside automatisk blir gjort til tjenestemottagerens startside, jfr. punkt 1.6.2?

I henhold til art. 12 skal den som yter en informasjonssamfunnstjeneste som består i tilveieskaffelsen av aksess til et kommunikasjonsnettverk ikke være ansvarlig for den informasjon som er skaffet til veie av en mottager av aksess-tjenesten og som blir oversendt gjennom nettverket. Denne ansvarsfriheten gjelder på en rekke vilkår som fremgår i art. 12, nr. 1, litra (a)-(c). Når det gjelder den informasjon som aksessleverandøren selv formidler gjennom sin hjemmeside er det klart at han må være ansvarlig for denne på lik linje med andre innholdsleverandører. Dette er klart fordi denne informasjonen ikke er skaffet til veie av en tjenestemottager og fordi oversendelsen under enhver omstendighet er initiert av aksessleverandøren, jfr. litra (a). I tillegg til dette har aksessleverandøren valgt ut informasjonen som inngår i oversendelsen, jfr. litra (c).

Spørsmålet som reiser seg i vårt tilfelle er hvorvidt den handlingen som aksessleverandøren foretar når han gjør sin hjemmeside til brukerens startside

gjør at han forlater rollen som «mere conduit» også i forhold til den oversendte informasjonen som er skaffet til veie av hans medkontrahent.

I denne sammenheng vil jeg presisere at den innholdsformidling som aksessleverandøren foretar gjennom kanaliseringen av tjenestemottagerne til sin hjemmeside opphører i det øyeblikk brukeren taster inn en ny URL og oppsøker et nytt internettområde.

Dersom en ser nærmere på vilkårene for ansvarsfrihet i litra (a)-(c), så synes det klart at disse må være oppfylt etter at tjenestemottageren har forlatt aksessleverandørens hjemmesider. Dette blir særlig klart ettersom bruken av bestemt form i litra (a)-(c), nemlig «the transmission» synes å understreke at aksessleverandørens rolle må vurderes separat i forhold til hver enkelt informasjonsoversendelse. Tanken må være at selv om aksessleverandøren ikke oppfyller vilkårene til å være «mere conduit» når han oversender informasjon fra sin hjemmeside, så kan han i det øyeblikk brukeren er videreformidlet til neste URL være inne i rollen. Noen nærmere forklaring på hva som inngår i én oversendelse gir verken direktivet eller preambelen, men en naturlig forståelse er likevel at hver ny nedlasting av informasjon fra aksessleverandørens server utgjør en oversendelse. Når således tjenestemottageren fortsetter sin informasjonssøken med å erstatte aksessleverandørens hjemmeside med nytt materiale fra aksessserveren, og dette materiale ikke er påvirket eller valgt ut av aksessleverandøren, må derfor aksessleverandøren kvalifisere til rollen som «mere conduit» i art. 12s forstand. En slik oppfatning har støtte i reelle hensyn ettersom en altfor vid definisjon av hva som skal inngå i én «transmission» i denne sammenheng ville føre til en uoversiktlig situasjon for aksessleverandøren og på den måten være egnet til å legge feller for hans virksomhet. Dette ville igjen virke imot e-handelsdirektivets formål om å sikre ytringsfriheten samt å fjerne hindringer for utviklingen av informasjonssamfunnet.

Konklusjonen er at aksessleverandøren oppfyller kravene til å være en «mere conduit» i forhold til den informasjon som er skaffet til veie av hans medkontrahent selv om han forhåndsprogrammerer slik at hans hjemmeside automatisk blir gjort til tjenestemottagerens startside.

2.4.4 Oppfyller aksessleverandøren kravene til å være en «mere conduit» dersom han forhåndsprogrammerer slik at reklamebannere/links til hans samarbeidspartnere/annonsører blir en del av grensesnittet mot Internett for brukerne av tjenesten, jfr. punkt 1.6.2?

I forhold til det innhold som aksessleverandøren formidler gjennom linker og reklamebannere i brukerens grensesnitt mot Internett risikerer han, på samme måte som der han forhåndsprogrammerer sin hjemmeside til å bli brukerens

startside, ansvar for eventuelt ulovlig eller krenkende innhold. Etter e-handelsdirektivet er dette utvilsomt fordi den aktuelle informasjonen ikke er skaffet til veie av tjenestemottageren og fordi han i dette henseendet både initierer oversendelsen, litra (a), og velger ut den informasjonen som inngår i oversendelsen, litra (c).

Når det gjelder spørsmålet om aksessleverandøren risikerer ansvar for den informasjon som hans medkontrahenter formidler gjennom hans fasiliteter stiller saken seg annerledes. I denne sammenheng blir spørsmålet hvorvidt den handlingen som aksessleverandøren foretar når han legger linker og reklamebannere inn i brukerens grensesnitt gjør at han forlater rollen som «mere conduit» i forhold til den oversendte informasjonen. Også dette tilfellet må vurderes opp mot vilkårene i litra (a)-(c) i art. 12.

Jeg vil presisere at i motsetning til tilfellet der aksessleverandøren formidler brukeren til sin hjemmeside, så innebærer en forhåndsprogrammering av linker og reklamebannere inn i brukerens grensesnitt mot Internett en manipulasjon som virker kontinuerlig inn på skjermbildet den tiden brukeren er logget på Internett, og som brukeren ikke kan kvitte seg med.

Etter art. 12, litra (a)-(c) kan det føre til ansvarsgjennombrudd for aksessleverandøren dersom han a) initierer oversendelsen av informasjon, b) velger ut mottageren av informasjon og c) velger ut eller endrer den informasjonen som inngår i oversendelsen. Også her er det klart at aksessleverandøren risikerer ansvar dersom han bryter mot ett av vilkårene i litra (a)-(c).

I vår sammenheng må det være klart at aksessleverandøren verken er den som initierer oversendelsen, litra (a), eller velger ut mottageren av den informasjon som oversendes, litra (b). Imidlertid kan det reises spørsmål i forhold til litra (c) hvorvidt den informasjonen som medkontrahenten oversender gjennom aksessserveren i og med oppdelingen av skjermbildet blir endret av aksessleverandøren.

Det kan hevdes at aksessleverandøren ikke endrer den informasjonen som blir oversendt fordi hans handlinger ikke påvirker integriteten til den informasjonen som han videreformidler for sin tjenestemottager. Dette synspunktet underbygges av at hans handlinger ikke utgjør noe direkte inngrep i den informasjonen som medkontrahenten sender. I denne sammenheng må man imidlertid vurdere aksessleverandørens virksomhet opp mot de uttalelser som fremgår av preambelens punkt (43) der det fremholdes at en tjenesteyter kun kan nyte godt av ansvarsfriheten etter art. 12 dersom han ikke under noen omstendighet er involvert i den informasjon som blir oversendt. Ordlyden favner her vidt, og skal man tolke en slik formulering bokstavelig, er det klart at den også omfatter en endring i det skjermbilde som den oversendte informasjonen fremgår i. Imidlertid åpner siste passus i punkt (43) for at ansvars-

frihet kan foreligge dersom modifikasjonene av den oversendte informasjon kun strekker seg til tekniske manipulasjoner som skjer i forbindelse med oversendelsen så lenge de ikke påvirker den informasjonen som inngår i sendingen. Det spørsmål som må stilles i denne sammenheng er hvorvidt en etablering av en rekke reklamebannere i brukerens grensesnitt mot Internett kan sies å utgjøre tekniske manipulasjoner i forbindelse med oversendelsen som ikke påvirker den informasjonen som oversendes. Med tekniske manipulasjoner må det fortrinnsvis være snakk om tekniske bearbeidelser som skjer for at oversendelsen skal kunne foregå på en hensiktsmessig måte. I preambelens punkt (42) styrkes denne oppfatningen ved at det presiseres at den tekniske prosessen som består i å skaffe aksess til et kommunikasjonsnettverk skal ha som eneste mål å gjøre oversendelsen mer effektiv. Eksempel på slike aktiviteter er komprimering av data og lignende. Slik jeg tolker e-handelsdirektivet utgjør derfor ikke etableringen av bannerbeltet i brukerens grensesnitt noen teknisk manipulasjon som har til eneste formål å gjøre oversendelsen av informasjon mer effektiv.

Det som imidlertid, etter min mening, må være avgjørende i dette tilfellet er spørsmålet om hvorvidt oppstillingen av bannerbeltet påvirker den informasjon som oversendes gjennom aksessserveren. I hvilken grad aksessleverandøren påvirker den informasjon som oversendes presiseres i preambelens punkt (42) til et spørsmål om han har hatt noen kontroll over, eller kunnskap om, innholdet i den oversendte informasjon. I de tilfeller der en rekke reklamebannere legger seg automatisk inn i brukerens skjermbilde, kan jeg ikke se at aksessleverandøren har hatt slik kontroll over, eller kunnskap om den oversendte informasjonen.

På tross av den vide fortolkningen av ordlyden i litra (c) som preambelens punkt (43) legger opp til, er jeg derfor kommet til at den oppstillingen av reklamebannere og linker til aksessleverandørens samarbeidspartnere/annonsører ikke medfører at den oversendte informasjon er endret av aksessleverandøren i art. 12, litra (c)s forstand.

Konklusjonen er at aksessleverandøren oppfyller kravene til å være en «mere conduit» selv om han forhåndsprogrammerer slik at reklamebannere/linker til hans samarbeidspartnere/annonsører blir en del av grensesnittet til Internett for brukeren av tjenesten.

2.4.5 Oppfyller aksessleverandøren kravene til å være en «mere conduit» dersom han installerer et teknologisk filter⁶⁶ som siler ut ulovlig eller krenkende informasjon som passerer gjennom hans server?

Spørsmålet om aksessleverandøren kan risikere ansvar for den informasjonen som mottageren av aksess tjenestene formidler gjennom hans fasiliteter dersom han installerer et teknologisk filter som siler informasjonen som passerer gjennom hans server må vurderes opp mot vilkårene i litra (a)-(c) i art. 12.

Det er på det rene at installasjon av et teknologisk filter verken medfører at aksessleverandøren initierer oversendelsen av informasjon, eller at han velger ut mottageren av informasjonen. Imidlertid kan det reises spørsmål om han i direktivets forstand velger ut eller modifiserer informasjonen som inngår i den oversendelsen av informasjon som hans medkontrahent foretar, jfr. litra (c).

Etter en naturlig forståelse av ordlyden i litra (c) må det være klart at filtreringen ikke innebærer noen endring av den oversendte informasjon. Det som skjer er jo at informasjonen i sin helhet avvises i filtreringsprosessen. Mer tvilsomt er det om vilkåret om at aksessleverandøren ikke må velge ut den informasjon som oversendes er oppfylt. Det å velge ut informasjon skulle etter ordlyden både omfatte de tilfeller der aksessleverandøren positivt velger ut den informasjon som han ønsker at mottageren skal ha, og at han negativt velger bort informasjon som han ikke ønsker å videreformidle.

I preambelens punkt (42) presiseres det at hovedregelen om ansvarsfritak kun skal gjelde ved tekniske manipulasjoner av oversendt informasjon som innebærer at tjenesteyteren ikke har kontroll over den informasjonen som blir oversendt, jfr. siste passus. Dertil fremgår det av punkt (43) at han kun skal nyte godt av ansvarsfriheten når han overhodet ikke er involvert i den informasjon som oversendes. Sistnevnte omfatter ikke tekniske manipulasjoner i forbindelse med oversendelsen, men som jeg nevnte ovenfor, må disse manipulasjonene ha som eneste formål å gjøre oversendelsen mer effektiv. Det er ikke tilfellet ved filtreringen. Uttalelsene fra preambelen taler, slik jeg ser det, klart for at filtreringen må medføre at tjenesteyteren faller utenfor direktivets hovedregel om ansvarsfrihet.

Reelle hensyn tilsier at installasjonen av et teknologisk filter for siling av informasjon må føre til at aksessleverandøren trår ut over rammene for passiv videreformidling. Dette er fordi han i dette tilfellet trer inn i en rolle som medfører et redaksjonelt utvalg av den oversendte informasjonen. Han har med andre ord forlatt rollen som passiv videreformidler til fordel for rollen som en aktør som med viten og vilje innvirker på det oversendte innholdet.

⁶⁶ Se begrepsforklaringen foran i pkt 1.5.

På bakgrunn av det entydige rettskildematerialet kan det ikke være tvil om at vilkåret om ansvarsgjennombrudd i art. 12, 1.ledd, litra (c) er oppfylt når tjenesteyteren undergir det videreformidlede innholdet teknologisk filtrering.

Konklusjonen er at aksessleverandøren ikke oppfyller kravene til å være en «mere conduit» dersom han installerer et teknologisk filter som å siler ut ulovlig eller krenkende informasjon som passerer gjennom hans server.

2.5 Spørsmål om ansvarsfrihet for den virksomhet som det i punkt 1.6.3 er beskrevet at nettverksoperatøren driver

2.5.1 Hjemmel

Dersom en informasjonssamfunnstjeneste som består i oversendelse av informasjon tilskaffet av en mottager av tjenesten i et kommunikasjonsnettverk blir ytet, skal tjenesteyteren etter e-handelsdirektivets art. 12, nr. 1 ikke være ansvarlig for den informasjonen som blir oversendt gjennom nettverket. Dette gjelder imidlertid kun dersom vilkårene i artikkelens nr. 1, litra (a)-(c) er oppfylt. Her fremgår det at ansvarsfriheten gjelder så lenge nettverksoperatøren (a) ikke initierer oversendelsen, (b) ikke velger ut mottageren av oversendelsen og (c) ikke velger ut eller endrer den informasjonen som inngår i oversendelsen. Den nettverksoperatør som oppfyller disse tre vilkårene vil oppfylle kriteriene til å være «mere conduit». Med andre ord kan ansvar kun inntre dersom tjenesteyteren bryter mot ett av vilkårene i litra (a)-(c).

Tjenesteyteren nyter også godt av ansvarsfriheten i forhold til direkte, selvstendig krenkelse av tredjemanns opphavsrettigheter dersom vilkårene for å være en «mere conduit» i art. 12, nr. 2 er oppfylt.

Når det gjelder vilkårene i art. 12, nr. 1, litra a-c, reiser ikke disse prinsipielle spørsmål for virksomhet som nettverksoperatør utover de som jeg har drøftet i forhold til aksessleverandøren i punktet ovenfor. Nok en gjennomgang av disse vilkårene vil derfor ikke bringe nytt materiale av interesse inn i oppgaven.

I forhold til nettverksoperatørens virksomhet finner jeg det mer hensiktsmessig å konsentrere meg om problemer knyttet til den eksemplarframstilling som kan skje under oversendelse av informasjon i nettverket. Under dette punktet vil jeg derfor legge hovedvekten på forholdet mellom nettverksoperatørens virksomhet og e-handelsdirektivets art. 12, nr. 2.

2.5.2 Er nettverksoperatørens virksomhet, slik den er beskrevet i punkt 1.6.3, omfattet av e-handelsdirektivets art. 12?

For det første er det et vilkår at den virksomhet som er beskrevet i punkt 1.6.3 innfrir vilkårene til å være en informasjonssamfunnstjeneste. Jeg vil nok en gang gjøre det klart at en nettverksoperatør er den aktør som skaffer de nødvendige kabler og rutere for å kunne sende data over et nettverk.

Spørsmålet er om nettverksoperatørens tjenester faller inn under e-handelsdirektivets begrep informasjonssamfunnstjeneste, slik det er fortolket i punkt 2.3.2. I denne sammenheng må det spørres om operasjonen av et nettverk er en tjeneste som normalt sett ytes mot vederlag, på avstand, ved elektroniske midler og etter individuell forespørsel fra tjenestemottageren.

Det første spørsmål er hvorvidt nettverksoperatørens tjenester er av en slik art at de normalt ytes mot vederlag.

Næringsdrivende eller private som ønsker å opprette en fastlinje for overføring av data, eventuelt som ønsker å opprette høyhastighetsforbindelse til en server som enten står i egne eller i nettverksoperatørens lokaler, må i langt de fleste tilfeller inngå et kontraktrettslig forhold med nettverksleverandøren. I forhold mellom næringsdrivende fremgår ofte ytelse og motytelse i forbindelse med nettverksleie av egne avtaler. For private, som ofte velger å koble seg opp mot Internett ved hjelp av et modem og en telefonlinje, ytes vederlaget ved at tjenestemottageren belastes for tellerskritt over telefonregningen. Den motytelse som den næringsdrivende eller den private i de beskrevne tilfellene vedtar å yte, må sies å oppfylle de lempelige kravene til vederlag som fremgår av tolkningen av begrepet informasjonssamfunnstjeneste.

Det neste vilkåret er at tjenesten må ytes på avstand. Ettersom nettverksoperatørens ytelse består i å stille til disposisjon kabler og rutere for tjenestemottageren er det klart at tjenesteyteren og tjenestemottageren ikke er på samme sted til samme tid når tjenesten foregår som avtalt. Vilåret om at tjenesten skal ytes på avstand er derfor oppfylt.

Det er videre et krav at tjenesten må ytes ved elektroniske midler. I dette ligger det for nettverksoperatørens virksomhet et krav om at informasjonen i sin helhet avsendes, overbringes og mottas via kabel, optiske fiberkanaler eller ved elektromagnetiske midler. I de tilfeller jeg har skissert under punkt 1.6.3, altså både der nettverksoperatøren stiller til disposisjon en alminnelig telefonlinje, for bruk med modem, og der han stiller til disposisjon en fastlinje som er koblet direkte opp mot en server, forutsetter virksomheten at informasjonen i sin helhet avsendes, overbringes og mottas via kabel, optiske fiberkanaler eller ved elektromagnetiske midler. Vilåret om at tjenesten må ytes med elektroniske midler volder med andre ord ikke problemer i dette tilfellet.

Det siste kravet for at nettverksoperatørens virksomhet skal være å anse som en informasjonssamfunnstjeneste er at tjenesten må være utført etter en individuell forespørsel fra en tjenestemottager. Det er i denne sammenheng på det rene at nettverksoperatørens virksomhet ikke er tilgjengelig for mottageren uten at denne har inngått et avtalerettslig forhold til operatøren, det være seg enten det gjelder tilkobling til Internett via telefonlinje eller via en fastlinje. Vilkåret om individuell forespørsel er derfor oppfylt.

Det er på grunnlag av den ovenstående drøftelse ikke tvilsomt at vilkåret om at nettverksoperatørens virksomhet må være en informasjonssamfunnstjeneste er oppfylt i dette tilfellet.

For det annet er det et vilkår at den som skaffer informasjon til oversendelse gjennom nettverket er tjenestemottager i art. 12's forstand.

I henhold til tolkningen av hvem som skal være å oppfatte som tjenestemottager i art. 12's forstand er det på det rene at enhver fysisk og juridisk person, altså både private og profesjonelle parter som jeg har beskrevet i punkt 1.6.3, og som mottar tjenester fra nettverksoperatøren skal omfattes av begrepet. Vilkåret er svært vidt og det må derfor anses for sikkert at en person som skaffer til veie informasjon til oversendelse gjennom nettverksoperatørens fasiliteter er tjenestemottager i art. 12's forstand.

For det tredje er det et vilkår at oversendelsen av informasjon skjer i det som e-handelsdirektivet omtaler som et «communication network». Etter det jeg har ovenfor har kommet til ved tolkningen av begrepet er det ikke tvilsomt at Internett er et slikt kommunikasjonsnettverk.

Konklusjonen er at nettverksleverandørens virksomhet, som beskrevet i punkt 1.6.3, er omfattet av e-handelsdirektivets art. 12.

2.5.3 Oppfyller nettverksleverandøren kravene til å være «mere conduit» der det under overføring av opphavsrettslig beskyttet materiale skjer eksemplarframstillinger som er egnet til å krenke en opphavsmanns rett?

Forutsetningen for denne drøftelsen er at den eksemplarframstillingen som foregår i ruten under oversendelsen av informasjon i nettverket er egnet til å krenke opphavsmannens rettigheter.

Ingen av bestemmelsene i art. 12, nr. 1 litra a-c vil føre til risiko for ansvarsgjennombrudd for nettverksoperatøren i dette tilfellet. Dette er fordi nettverksleverandøren verken initierer oversendelsen av informasjon, velger

ut mottageren av informasjonen eller velger ut eller endrer den informasjonen som inngår i oversendelsen ved den prosessen som kalles packet switching.⁶⁷

Spørsmålet er om den eksemplarfremstilling i ruterne som jeg har beskrevet i punkt 1.6.3 kan medføre risiko for ansvarsgjennombrudd for nettverksoperatøren etter art. 12, nr. 2.

Dersom ansvar skal være aktuelt som følge av en krenkelse av opphavsrett ved midlertidige eksemplarfremstillinger må det dreie seg om mellomleddets ansvar for den direkte, selvstendige overtredelsen av opphavsrettslovgivningen. Problemet ligger, fordi det dreier seg om regulering av en selvstendig krenkelse av lovverket, utenfor de avgrensningene som ligger til grunn for oppgaven⁶⁸, men ettersom direktivet tydelig tar høyde for spørsmålet finner jeg det likevel naturlig å inkludere drøftelsen i dette punktet. Mye kan nemlig tyde på at Kommisjonen har ønsket å sikre ansvarsfrihet også for den midlertidige lagringen som skjer under oversendelsen av informasjon i nettverk. Art. 12, punkt 2 oppstiller i denne sammenheng en rekke betingelser til den midlertidige lagringen for at den skal omfattes av hovedreglen om ansvarsfrihet.

E-handelsdirektivet gjør i art. 12, nr. 2⁶⁹ det klart at ordene «transmission in a communication network» skal omfatte også den automatiske, mellomliggende og kortvarige lagringen av oversendt informasjon, forutsatt at denne lagringen utelukkende tjener til utførelse av oversendelsen i kommunikasjonsnettverket, og dens varighet ikke overstiger den tid som med rimelighet må antas være nødvendig for oversendelsen. Den mellomlagring som innfrir de vilkårene som blir oppstilt i art. 12, nr. 2 vil oppfylle vilkårene for å være en mere conduit-virksomhet, og vil derfor nyte godt av ansvarsfriheten i art. 12.

Når det gjelder vilkåret om at lagringen av det beskyttede verket i ruterne må være automatisk volder dette ikke problemer ettersom hele prosessen er styrt gjennom de tekniske funksjoner som danner forutsetningene for kommunikasjon over Internett. Når det gjelder vilkåret om at lagringen må være mellomliggende må dette anses for å trekke opp grensen mot de tilfeller der lagringen skjer i en endestasjon på Internett, for eksempel en maskin som er tilgjengelig for alminnelige brukere. Den lagringen som skjer i ruterne kjenetegnes nettopp ved sin mellomliggende karakter ettersom ruterne kun danner knutepunkter i nettet. Vilkåret om at lagringen skal være kortvarig må ses på bakgrunn av varigheten ikke må overstige den tid som med rimelighet må antas å være nødvendig for oversendelsen. Det er på det rene at en mellomlagring i

⁶⁷ Jfr. punkt 1.6.3

⁶⁸ Jfr. punkt 1.4.

⁶⁹ Det er verdt å merke seg at den amerikanske DMCA §512, litra (a) etablerer et tilsvarende ansvarsfritak når det gjelder nettverksleveranse og aksessstilskaffelse.

en ruter tidsmessig kan strekke seg ut over rent øyeblikkelige eksemplarframstillinger, f.eks. der det er stor trafikk og kø i nettverket. I denne sammenheng må det være klart at art. 12, nr. 2 også må omfatte de tilfeller der eksemplaret blir liggende i noen tid mens videre oversendelse avvantes. Vilkåret om at lagringen i ruterne utelukkende må tjene til utførelsen av oversendelsen i nettverket må oppfattes dithen at art. 12, nr. 2 ikke skal omfatte tilfeller der mellomlagringen også tjener andre formål enn ren videreformidling av informasjonen. Som eksempel på slike tilfeller kan nevnes at under lagringen gjøres handlinger for å nyttegjøre seg den informasjon som fremgår av det beskyttede verket eller fremstille varige eksemplarer av det. I de prosesser som jeg har beskrevet er det en forutsetning at rutingen kun omfatter ren videreformidling av informasjon. Dette vilkåret volder derfor ikke problemer i vårt tilfelle.

Til slutt oppstiller art. 12, nr. 2 et vilkår om at en mellomlagring av informasjon i ruterne ikke må strekke seg utover en periode som er lengre enn det som er rimelig nødvendig for oversendelsen. Etter ordlyden gir dette vilkåret bud om en objektiv vurdering av hvorvidt den periode informasjon lagres i ruterne er rimelig nødvendig ut fra normale forhold. Med andre ord skal det i denne vurderingen ses hen til hva som er objektivt rimelig å forvente ut fra omstendigheter som stor trafikk på nettet og liten overføringskapasitet som kan være med på å forlenge mellomlagringen. Det avgjørende vil være om den mellomlagringen som skjer strekker seg ut over den tid som alle forhold tatt i betraktning burde være tilstrekkelig etter en objektiv faglig vurdering. Vilkåret er på denne måten med på å legge grunnlaget for fremvekst av bransjestandarder for hvor lenge mellomlagring i en ruter skal kunne foregå samtidig som tjenesteyteren holder seg innenfor en tidsramme som er akseptabel uavhengig av de konkrete omstendigheter.⁷⁰

I det tilfelle jeg drøfter er det ingen holdepunkter for at mellomlagringen av informasjon strekker seg ut over den tid som må anses for rimelig nødvendig for å gjennomføre oversendelsen.

På bakgrunn av det jeg har kommet frem til ovenfor må det være klart at den mellomlagringen som skjer i ruterne under overføringen av opphavsrettslig beskyttede verk på Internett i dette tilfellet er omfattet av ansvarsfrihetsbestemmelsen i art. 12, nr. 2.

Konklusjonen er at nettverksleverandøren nyter godt av hovedregelen om ansvarsfrihet i art. 12 der det under overføring av opphavsrettslig beskyttet

⁷⁰ I preambelen til e-handelsdirektivet, punkt (41), fremholdes det at direktivet skal skape en balanse mellom de forskjellige, involverte parter interesser og danne grunnlaget for prinsipper som industrielle avtaler og standarder kan bli basert på.

materiale skjer eksemplarframstillinger i ruterne som er egnet til å krenke opphavsmannens rett.

2.6 Spørsmål om ansvarsfrihet for det som i punkt 1.6.4 er beskrevet som proxy serving/proxy caching og mirror caching

2.6.1 Hjemmel

Den som skaffer til veie en informasjonssamfunnstjeneste som går ut på oversendelse i et kommunikasjonsnettverk av informasjon som er skaffet til veie av en mottager av tjenesten til andre mottagere av tjenesten på disses oppfordring, oppfyller kravene til det som i e-handelsdirektivets art. 13, nr. 1 er beskrevet som caching. Aktører som oppfyller disse kravene skal ikke risikere ansvar for den automatiske, mellomliggende og midlertidige lagringen av informasjonen så lenge oversendelsen er utført etter forespørsel fra andre mottagere av tjenesten med eneste formål å gjøre informasjonsoversendelsen til disse mer effektiv.

Ansvarsfriheten gjelder imidlertid kun så lenge vilkårene i art. 13, nr. 1, litra (a)-(e) er oppfylt. Dette innebærer, som jeg også gjorde klart i forhold til direktivets art. 12, at vilkårene er negativt kumulative i den forstand at ansvarsgjennombrudd kan forekomme når tilbyderen av cachingtjenestene bryter mot ett av disse vilkårene.

I art. 13 litra (a)-(e) fremgår det at tjenesteyteren ikke (a) må endre informasjonen, (b) at han må overholde betingelsene for adgang til informasjonen, (c) at tjenesteyteren overholder reglene om ajourføring av informasjonen, (d) at tjenesteyteren ikke foretar inngrep i den lovlige anvendelse av teknologi, som er alminnelig anerkjent og anvendt av industrien, med det formål å skaffe seg data om anvendelse av informasjonen og (e) at tjenesteyteren straks tar skritt for å fjerne den informasjon som han har lagret, eller hindrer adgangen til den når han får konkret kunnskap om at informasjonen er blitt fjernet fra nettet eller adgangen til den er hindret, eller at en domstol eller en administrativ myndighet har krevd informasjonen fjernet eller adgangen til den hindret.

De første spørsmål som jeg skal ta stilling til er om de virksomhetene som i punkt 1.6.4 er beskrevet som proxy caching og mirror caching er omfattet av art. 13 i e-handelsdirektivet.

2.6.2 Er den virksomhet som i punkt 1.6.4 er beskrevet som proxy caching omfattet av art 13 i e-handelsdirektivet?

For det første er det i henhold til art. 13, 1. pkt et vilkår at proxy cachingen er en informasjonssamfunnstjeneste i e-handelsdirektivets forstand. En informasjonssamfunnstjeneste er i e-handelsdirektivets forstand «any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of the services».

Når det gjelder kravet om vederlag er det, etter det som fremgår av tolkningen ovenfor, og da særlig av preambelens punkt (18), tilstrekkelig at cachingtjenesten inngår i en virksomhet av økonomisk karakter. Terskelen for hva som skal omfattes av en slik virksomhet kan på bakgrunn av de lempelige krav som stilles til vilkåret om vederlag, ikke være særlig høy. Ettersom cachingtjenester i de fleste tilfeller inngår i en eller annen form for næringsvirksomhet regner jeg det som klart at dette vilkåret er oppfylt for den beskrevne funksjonen.

Når det gjelder kravet om at cachingtjenesten skal ytes på avstand og med elektroniske midler volder heller ikke dette problemer da det ligger i cachingtjenestens natur at den skjer mens partene ikke er til stede på samme tid samt at den skjer gjennom bruk av elektronisk verktøy.

Vilkåret om at proxy cachingen må ytes på individuell forespørsel fra den som mottar tjenesten er, som nevnt i tolkningen i punkt 2.3.2 ovenfor, ment for å trekke opp grensen mot blant annet kringkastingstjenester, og andre tjenester som er tilgjengelige uten noen konkret kontakt mellom tjenesteyter og tjenestemottager. Fordi informasjon fra en fjerntliggende server kun er tilgjengelig etter at den aktør som ønsker å yte proxy caching-tjenester aktivt tar kontakt med kildeserveren for å innhente den, må vilkåret om at tjenesten skal være tilveieskaffet på individuell forespørsel fra den som mottar tjenesten anses for oppfylt.

For det andre er det et vilkår etter 1. punkt at informasjonssamfunnstjenesten består i oversendelse i et kommunikasjonsnettverk av informasjon som er tilveieskaffet av den som mottar cachingtjenesten. Som det fremgår av tolkningen over er det ikke tvilsomt at Internett er et kommunikasjonsnettverk og at oversendelsen av informasjon derfor skjer i et kommunikasjonsnettverk i e-handelsdirektivets forstand.

Når det gjelder vilkåret om at den informasjon som oversendes må være tilskaffet av en som mottar cachingtjenesten, eller en «recipient of the service», viser jeg til den forklaringen som jeg har gitt i punkt 1.6.4 der det fremgår at den informasjonen som tilbys gjennom proxy cachingen er tilveieskaffet av innehaveren av kildeserveren. Som det fremgår av tolkningen av begrepet «recipient of the service», jfr. punkt 2.3.3, skal dette omfatte

enhver fysisk eller juridisk person som, i profesjonelt øyemed og ellers, bruker en informasjonssamfunnstjeneste særlig med det formål å søke informasjon, men også for å gjøre informasjon tilgjengelig. Som jeg har forklart benytter innehaveren av en kildeserver seg av proxy caching-tjenestene nettopp for å gjøre informasjon lettere tilgjengelig for andre som mottar proxy caching-tjenestene. Vilkåret for å være tjenestemottager i e-handelsdirektivets forstand er derfor oppfylt for den som innehar kildeserveren for den informasjon som tilbys gjennom proxy caching-tjenester.

For det tredje er det et vilkår at den automatiske, mellomliggende og midlertidige lagringen som skjer i proxy cacherens server utføres med eneste formål å gjøre oversendelsen av informasjon til «other recipients of the service», det vil si til andre enn innehaveren av kildeserveren, mer effektiv. Det er på det rene at også disse andre tjenestemottagerne må oppfylle kravene til e-handelsdirektivets definisjon av «recipient of the service». På bakgrunn av den vide fortolkningen av begrepet som direktivet oppstiller, jfr. punkt 2.3.3, er det klart at også de aktørene som bruker Internett for å skaffe seg informasjon gjennom bruk av proxy caching-tjenestene er omfattet.

For det fjerde er det et krav at oversendelsen skjer på forespørsel fra andre tjenestemottagere enn innehaveren av kildeserveren. I denne sammenheng viser jeg til min forklaring i punkt 1.6.4 som fremholder at proxy caching i praksis innebærer en oversendelse av informasjon i de tilfeller der sluttbrukeren etterspør spesiell informasjon. På bakgrunn av dette er det klart at informasjonsoversendelsen i disse tilfellene skjer på forespørsel fra andre tjenestemottagere enn innehaveren av kildeserveren.

Etter dette må det være klart at vilkårene for komme innunder anvendelsesområdet for art. 13, 1. ledd er oppfylt når det gjelder proxy caching-tjenester.

Konklusjonen er at den virksomhet som jeg har beskrevet som proxy caching i punkt 1.6.4 er omfattet av anvendelsesområdet for art 13 i e-handelsdirektivet.

2.6.3 Er den virksomhet som i punkt 1.6.4 er beskrevet som mirror caching omfattet av anvendelsesområdet for art 13?

For at mirror caching-virksomheten skal være omfattet av anvendelsesområdet for art. 13, er det for det første et krav at den er en informasjonssamfunnstjeneste i e-handelsdirektivets forstand. I denne sammenheng må den utgjøre en tjeneste «normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of the service». Når det gjelder dette spørsmålet skiller ikke mirror caching-virksomheten seg

fra proxy caching-virksomhet. I denne sammenheng henviser jeg derfor til drøftelsene i punktet ovenfor.

I forhold til vilkåret om at den mellomlagrede informasjonen må overføres til «other recipients of the service» kan det imidlertid være grunn til å skille mellom proxy caching og mirror caching. Dette er fordi den som i mirror caching-tilfellet må regnes som en «recipient of the service» verken bruker cachingtjenestene aktivt for å søke informasjon, eller for å gjøre informasjon tilgjengelig. Han mottar jo gjennom mirror caching-prosessen informasjon passivt ved at innehaveren av cachingserveren oversender ham denne. Der- som vi ser hen til drøftelsen av begrepet «recipient of the service» i punkt 2.3.3 forutsetter den at personer som skal være tjenestemottagere må utvise en minste grad av aktivitet for enten å søke informasjon, eller gjøre informa- sjon tilgjengelig på Internett. Med andre ord utelukkes de tilfeller der aktører mottar informasjon gjennom å forholde seg passive. Etter min mening tyder dette på at den som mottar informasjon gjennom mirror caching-tjenester ikke er tjenestemottager i e-handelsdirektivets forstand.

I samme retning som drøftelsen i avsnittet over går vurderingen av et an- net vilkår i art. 13 nr. 1. Som nevnt innebærer mirror caching-tjenesten at det er tjenesteyteren som på eget initiativ sørger for informasjonens videre over- sendelse til andre tjenestemottagere. Dette er i strid med vilkåret i art. 13 nr. 1 in fine om at informasjonens videresendelse til andre tjenestemottagere må skje «upon their request».

På bakgrunn av at mirror caching på disse punktene klart skiller seg fra den virksomheten som er beskrevet i art. 13 nr. 1 kan det ikke være tvilsomt at virksomheten faller utenfor de tilfellene som artikkel 13 er ment å regulere. Aktører som driver denne typen virksomhet nyter derfor ikke godt av hoved- regelen om ansvarsfrihet.

Konklusjonen er at den virksomhet som jeg har beskrevet som mirror caching ikke er omfattet av anvendelsesområdet for art. 13. Mirror caching vil derfor ikke bli behandlet nærmere i det følgende.

2.6.4 Er kravene for ansvarsfrihet oppfylt dersom tilbyderer av proxy caching-tjenester installerer et teknologisk filter som siler ut innhold som er ulovlig eller krenkende?

Når det gjelder spørsmålet om hvordan et teknologisk filter fungerer i praksis henviser jeg til redegjørelsen foran i punkt 1.5.

I henhold til art. 13 nr. 1 fremgår det at tjenesteyteren ikke skal være ansvarlig for den automatiske, mellomliggende og midlertidige lagringen av informasjon som utføres med eneste formål å gjøre informasjonens oversendelse

til andre tjenestemottagere mer effektiv sålenge informasjonen er oversendt etter forespørsel fra andre tjenestemottagere. Ansvarsfriheten er imidlertid undergitt en rekke vilkår som fremgår av bestemmelsens nr. 1, litra (a)-(e).

I forhold til den aktuelle problemstillingen er det, i tillegg til vilkåret om at lagringen og videresendelsen av informasjon må være automatisk, mellomliggende og midlertidig, særlig et vilkår at tilbyderer av proxy caching-tjenester ikke endrer den informasjonen som blir lagret og videresendt gjennom hans server, jfr. litra (a).

Første spørsmålet er om tjenesteyteren ved å installere et teknologisk utslingsfilter endrer den lagrede og oversendte informasjonen, jfr. litra (a), og på denne måten unngår å oppfylle vilkårene for ansvarsfrihet.

Etter en språklig forståelse av direktivets begrep «modify» må det omfatte de tilfeller der den lagrede eller videresendte informasjonen, som følge av proxy cacherens handlinger, undergår en forandring som tilsidesetter informasjonens integritet. Dette innebærer at en del av den lagrede informasjonen fjernes eller legges til, eller eventuelt at det gjøres endringer i den rekkefølge og den orden som informasjonen opprinnelig kommer i.

I preambelen er det enkeltuttalelser som kan trekke i retning av en utvidende tolkning av begrepet «modify», se f.eks. uttalelsen i punkt (43), første passus, som sier at ansvarsfrihet forutsetter at proxy cacheren ikke på noen måte må være involvert i den informasjonen som oversendes. Fortalen sett i en mer helhetlig sammenheng gir, etter min mening, likevel ikke tilstrekkelig grunnlag for en så vid fortolkning. En tolkning av preambelens punkt (43), andre passus, medfører nemlig en presisering vilkåret av «modify» dithen at det skal gjelde kun i de tilfeller der informasjonen endres under oversendelsen. Denne presiseringen får støtte i punkt (43), tredje passus, som fremholder at dersom informasjonen undergis tekniske manipulasjoner, og her regner jeg filtrering som en teknisk manipulasjon, så skal ikke disse utgjøre endringer i direktivets forstand dersom de ikke faktisk tilsidesetter informasjonens integritet. Det avgjørende for hvorvidt filtreringen skal falle innenfor begrepet «modify» i art. 13 må derfor være om det faktisk er skjedd materielle endringer i den oversendte informasjonen. Man må i denne sammenheng se hen til hvordan teknologiske filter praktisk fungerer. Filtrene er nemlig innrettet slik at informasjon som inneholder forhåndsbestemte kvalifikasjonskriterier i sin helhet nektes overført gjennom proxy cacherens server. Det synes derfor mer naturlig å si at den oversendte informasjonen velges bort eller stanses fremfor at den endres når proxy cacheren benytter et teknologisk filter. Etter min mening omfattes ikke slik bortvelgelse eller stansing av informasjon av begrepet «modify» i art. 13.

En praksis der man benytter seg av teknologiske filter for å velge bort eller stanse informasjon er ikke mindre betenkelig i forhold til ytringsfriheten og funksjonaliteten i Internett enn en eventuell manuell oppstykking og utvelgelse av den informasjon som skal videreformidles gjennom proxy cachingen. Reelle hensyn taler derfor isolert sett for at filtreringen skal omfattes av direktivets begrep «modify».

På tross av de reelle hensyn og med særlig vekt på ordlyden i direktivet, samt uttalelsene fra preambelen, finner jeg det klart at installasjonen av et teknologisk filter som har til intensjon om å sile ut ulovlig eller krenkende innhold ikke faller inn under det som etter direktivet skal være å forstå med å «modify the information». Vilkårene for ansvarsfrihet etter e-handelsdirektivet er derfor oppfylt etter dette vilkåret.

Det andre spørsmålet jeg skal undersøke er om videresendelsen, eventuelt mellomlagringen av informasjonen kan sies å være automatisk i e-handelsdirektivets forstand når teknologiske filter benyttes. Dersom mellomlagringen eller oversendelsen av informasjon ikke er automatisk vil etter art. 13s system heller ikke virksomheten falle inn under hovedregelen om ansvarsfrihet.

Etter en språklig fortolkning av ordlyden i art. 13, nr. 1 er det naturlig å oppfatte vilkåret om at lagringen skal være automatisk dithen at videresendelsen må være av en passiv og teknisk art, det vil si at den foregår uten noen manuell innblanding fra proxy cacheren. I preambelens punkt (42) annen passus presiseres dette ved utsagnet om at de ansvarsfrie aktiviteter skal være av kun «technical, automatic and passive nature, which implies that.. [proxy cacheren] ..has neither knowledge of nor control over the information which is transmitted or stored.» Når tilbyderer av proxy caching-tjenester installerer et teknologisk filter utøver han etter min mening kontroll over den materialet som lagres og oversendes fordi han på denne måten sørger for at informasjon som oppfyller filterets kvalifikasjonskriteriene velges bort. I punkt (43), første passus, sies det videre at en tjenesteyter kan nyte godt av ansvarsfriheten for blant annet caching «when he is in no way involved in the information transmitted.» Ordlyden i denne bestemmelsen er så vidt at den under enhver omstendighet må omfatte den påvirkningen som installasjonen av et teknologisk filter medfører. I de to følgende passusene innsnevres imidlertid denne oppfatningen noe i det vurderingen av hvorvidt han har vært involvert i den oversendte informasjon skal være avhengig av om informasjonen er blitt endret. Noe krav om endring er det imidlertid ikke rimelig å oppstille for at oversendelsen av informasjon ikke skal kunne sies å være automatisk. Jeg tillegger derfor ikke punkt (43) første passus noen vekt i denne sammenheng.

Dersom man ser hen til styringsformålet som fremgår av reguleringsene i art. 13, som enkelt sagt er å sørge for at mellomleddene ikke legger hindring-

er i veien for ytringsfriheten, samt at de ikke hindrer funksjonaliteten av Internett, så understøtter også dette at proxy cacheren, når han installerer et teknologisk filter, opererer utenfor de roller som er omfattet av ansvarsfriheten i art. 13.

Særlig på bakgrunn av direktivets ordlyd sett i lys av uttalelsene i preambelen og reelle hensyn finner jeg det rimelig å si at den tilbyder av proxy caching-tjenester som installerer et teknologisk filter for å stanse ulovlig eller krenkende informasjon ikke kvalifiserer til å drive virksomhet som innebærer automatisk videreformidling og mellomlagring i art. 13 nr. 1s forstand. I denne sammenheng er altså direktivets vilkår for ansvarsfrihet for proxy cacheren ikke oppfylt, og han må risikere ansvar på linje med andre aktører i markedet.

Konklusjonen er, på bakgrunn av den siste drøftelsen, at kravene til ansvarsfrihet ikke er oppfylt dersom tilbyderer av proxy caching-tjenester installerer et teknologisk filter som har til intensjon å sile ut innhold som er ulovlig eller krenkende.

2.6.5 Er kravene til ansvarsfrihet i art. 13, nr. 1 oppfylt dersom tilbyderer av proxy caching-tjenester ikke fjerner eller stenger tilgangen til en nettside som han vet inneholder ulovlig eller krenkende informasjon?⁷¹

Jeg forutsetter at tjenesteyteren driver proxy caching-virksomhet på en slik måte at den er omfattet av anvendelsesområdet for art. 13 nr. 1. Dette innebærer at virksomheten kvalifiserer til å være en informasjonssamfunnstjeneste, at den lagrede informasjonen er tilskaffet av en aktør som oppfyller kravene til å være en «recipient of the service», at lagringen er automatisk, mellomliggende og midlertidig, at lagringen er utført med eneste formål å gjøre den videre oversendelsen til andre som oppfyller kravene til å være en «recipient of the service» samt at informasjonen kun oversendes på forespørsel fra disse andre tjenestemottagerne.

Under disse forutsetningene er mitt spørsmål om tilbyderer av proxy caching-tjenester oppfyller kravene til ansvarsfrihet i art. 13 nr. 1 dersom han vet at den informasjon som han mellomlagrer i forbindelse med proxy cachingen er ulovlig eller krenkende, og han ikke foretar seg noe for å fjerne den eller stenge tilgangen til den.

⁷¹ Slik kunnskap kan proxy cacheren få for eksempel ved rene tilfeldigheter eller ved spesifiserte underretninger fra andre aktører i markedet.

Det er naturlig å vurdere dette spørsmålet opp i mot vilkårene i art. 13 nr. 1, litra (e). I henhold til denne bestemmelsen er det et vilkår for ansvarsfrihet for den som driver proxy caching at han handler «expeditiously» for å fjerne eller stenge tilgangen til den informasjon som han har lagret dersom han får «actual knowledge» om at informasjonen i kildeserveren har blitt fjernet fra nettverket, at tilgangen til den har blitt stanset, eller at en domstol eller en administrativ myndighet har besluttet slik fjerning eller sperring.

Det er i det aktuelle tilfellet på det rene at tilbyderer av proxy caching-tjenestene har «actual knowledge», eller faktisk kunnskap om det ulovlige eller krenkende innholdet, og det er også klart at han ikke foretar seg noe «expeditiously», eller omgående, for å fjerne eller stenge tilgangen til den. Problemet er imidlertid at litra (e) ikke oppstiller noen handleplikt i de tilfeller der proxy cacheren vet at den informasjon som han mellomlagrer er ulovlig eller krenkende. Det er imidlertid, ut fra de tilfellene som faktisk reguleres i litra (e), klart at det har vært lovgiverens intensjon å ta høyde for de situasjoner der den informasjonen som ligger hos proxy cacheren har uønsket innhold. Mitt spørsmål er derfor, om det i denne sammenheng, er forsvarlig å innfortolke en plikt til å fjerne ulovlig eller krenkende informasjon i de tilfeller der proxy cacheren vet om denne. En slik tolkning kan f.eks. begrunnes i en analogi fra e-handelsdirektivets art. 14.

Det hensyn som særlig begrunner er slik analogi er den urimelighet det innebærer at proxy cacheren skal nyte godt av reglene om ansvarsfrihet selv om han faktisk vet at den informasjon han lagrer og formidler er ulovlig. I denne sammenheng er det særlig ønsket om å unngå ytterligere krenkelser av tredjemanns rettigheter som gjør seg gjeldene.

I art. 14 er det tatt høyde for problemet i nr. 1, litra (b), der det uttrykkelig sies at tjenesteyteren må handle «expeditiously» for å fjerne eller stanse tilgang til (den ulovlige, jfr. litra (a)) informasjonen, for å kunne nyte godt av ansvarsfriheten etter art. 14 nr. 1.

Proxy cacherens plikter må ses på bakgrunn av den rolle han besitter. Proxy caching innebærer utøvelse av en funksjon som særlig har til formål å lette trafikk over Internett ved at informasjon gjøres tilgjengelig over kortere distanser og gjennom færre mellomledd. Det er i denne sammenheng et krav i art. 13 at all lagring av informasjon som skjer ved proxy caching skal være automatisk, mellomliggende og midlertidig. Situasjonen er med andre ord på mange måter lik nettverksoperatørens. En viktig forutsetning for at ytringsfriheten skal kunne sikres og at Internett skal kunne fungere hensiktsmessig, er at nettopp de som opererer nettverket skal slippe å involvere seg i den informasjonen som oversendes. Regler som gir risiko for ansvarsgjennombrudd der proxy cacheren har kunnskap om at han formidler ulovlig eller krenkende informasjon ville

effektivt true funksjonaliteten i nettverket. Så stor vekt kan likevel ikke slike betraktninger ha sålenge det er snakk om faktisk kunnskap om den ulovlige informasjonen. Den interesse som er begrunnet i muligheten til å formidle ulovlig informasjon effektivt er ikke akkurat beskyttelsesverdig.

En betraktning som bør tillegges større vekt er at dersom ansvarsfrihet gjøres avhengig at proxy cacheren fjerner eller stenger tilgangen til eventuelt ulovlig innhold, så vil risikoen for den rettslige vurderingen av om informasjonen faktisk medfører rettsbrudd i for stor grad bli lagt på dette mellomleddet. Det er verken tilfellet i praksis eller meningen i teorien at de digitale mellomleddene skal besitte den kompetanse som er nødvendig for å foreta vurderinger av hvorvidt informasjon er ulovlig eller ikke.

Det må under enhver omstendighet være klart at en analogi fra art. 14 vil medføre store betenkeligheter i forhold til reglene om innføring av de aktuelle bestemmelsene i nasjonal rett. Som jeg har nevnt ovenfor er e-handelsdirektivet er minimumsdirektiv. Dette innebærer at man ved anvendelsen av bestemmelsene i nasjonal rett godt kan komme frem til et ansvarsregime som er mildere enn det som fremgår i art. 13, men aldri til et strengere. Å innfortolke et vilkår som fører til ansvarsgjennombrudd i det tilfelle som jeg diskuterer ovenfor vil derfor føre til at løsningen kommer i strid med e-handelsdirektivet. Således må det være klart at en analogi fra art. 14 ikke er mulig. Dette medfører at ansvarsfriheten etter art. 13 nr. 1, litra (e) ikke kan gjøres avhengig av at proxy cacheren fjerner eller stanser tilgangen til ulovlig eller krenkende informasjon som han vet at han lagrer på sin server.

Konklusjonen er at kravene til ansvarsfrihet er oppfylt selv om tilbyderer av proxy caching-tjenester ikke fjerner eller stenger tilgangen til en nettside som han vet inneholder ulovlig eller krenkende informasjon.

2.7 Spørsmål om ansvarsfrihet for den virksomhet som i punkt 1.6.5 beskrives som host service provider

2.7.1 Hjemmel

I henhold til e-handelsdirektivets art. 14, nr. 1 skal tjenesteyteren, så lenge vilkårene i artikkelens litra (a)-(b) er oppfylt, være ansvarsfri dersom han skaffer til veie en informasjonssamfunnstjeneste som består i lagring av informasjon som er skaffet til veie av en mottaker av tjenesten og informasjonen er lagret etter forespørsel fra en mottaker av tjenesten.

EU-direktivet skiller i art. 14, nr. 1, litra (a) mellom sivil-, og strafferettslig krenkelser foretatt av mellomleddets tjenestemottager idet det etablerer forskjellige kriterier for frihet fra hver av disse typene ansvar. Når det gjelder et strafferettslig ansvar bestemmes det at en host service provider ikke skal kunne gjøres ansvarlig for tjenestemottagerens brudd på straffelovgivningen med mindre han har faktisk kunnskap om at innholdet er ulovlig. Når det gjelder et sivilrettslig erstatningsansvar skal en host service provider ikke risikere ansvar for ulovlig innhold som er skaffet til veie av tjenestemottageren med mindre han er klar over de fakta og omstendigheter som gjør den ulovlige aktivitet synlig.

Videre skal host service provideren, selv om han for strafferettslige krenkelsers del har faktisk kunnskap om det ulovlige innholdet eller for sivilrettslige krenkelsers del er klar over de fakta og omstendigheter som gjør krenkelsen synlig, være ansvarsfri dersom han, i det han får slik kunnskap, handler «expeditiously» for å fjerne eller hindre tilgang til det krenkende eller ulovlige materialet, jfr. litra (b).

2.7.2 Er den virksomhet som i punkt 1.6.5 er beskrevet som host service provider omfattet av art 14 i e-handelsdirektivet?

For at hosting skal være omfattet at art. 14 er det for det første et vilkår at virksomheten er en informasjonssamfunnstjeneste i e-handelsdirektivets forstand. I denne sammenheng er kravet at virksomheten utgjør en tjeneste som normalt sett ytes mot vederlag, på avstand, med elektroniske midler og på individuell forespørsel fra en som er mottager av tjenestene.

Som det fremgår av punkt 2.3.1 er de krav som stilles for at virksomheten skal være av en karakter som normal sett skjer mot vederlag ikke særlig omfattende. Det avgjørende må være at host service provideren yter sine tjenester i en eller annen form for næringsvirksomhet. De typer hosting som jeg konsentrerer meg om i denne oppgaven ytes alle i profesjonelle forhold der meningen er å sørge for verdiskapning. Vilkåret om at virksomheten normalt sett ytes mot vederlag er derfor oppfylt for host service providerens del.

Neste vilkår er at virksomheten må utøves på avstand og med elektroniske midler. Ettersom det ligger i hostingens natur at den skjer mens partene ikke er tilstede sammen og ved bruk av datamaskiner, finner jeg det ikke tvilsomt at dette vilkåret er oppfylt.

Det siste vilkåret for at hosting skal være en informasjonssamfunnstjeneste i e-handelsdirektivets forstand er at hostingtjenesten må skje «at the request of a recipient of the service». Betingelsen om at tjenestemottageren må være en «recipient of the service» volder ikke problemer i dette tilfeller ettersom

direktivets definisjon av dette omfatter alle som gjør bruk av en informasjonssamfunnstjeneste både for å søke og gjøre informasjon tilgjengelig over Internett, jfr. punkt 2.3.3. Vilåret om individuell forespørsel er, som jeg tidligere har nevnt, ment for å trekke opp grensen mot blant annet kringkastings tjenester, som jo ytes uten at tjenestemottageren har vært i kontakt med kringkasteren. Hostingtjenestene ytes kun i de tilfeller der det har vært en konkret kontakt mellom tjenesteyter og tjenestemottager, enten ved at de har personlig avtale, eller ved at tjenestemottageren, før bruken av tjenesten kan begynne, har oppsøkt host service leverandørenes tjenester på Internett. Jeg regner det derfor som sikkert at hostingtjenesten ytes på individuell forespørsel fra tjenestemottageren.

I tillegg til dette er det et vilkår at virksomheten som host service leverandøren driver innebærer «storage», eller lagring av den informasjonen som er skaffet til veie av tjenestemottageren. Verken e-handelsdirektivets ordlyd eller preambelen gir noen nærmere forklaring av ordet «storage». Imidlertid må den virksomhet som host service leverandøren driver, nemlig å sørge for plass og tilgjengelighet til forskjellige typer programvare på sine servere, være innenfor den naturlige forståelse av ordet lagring. Kravet om at informasjonen må være tilveieskaffet av tjenestemottageren er særlig ment for å trekke opp grensen mot de tilfeller der host service leverandøren selv må karakteriseres som innholdsleverandør. Det er nemlig bare i de tilfeller der hans virksomhet omfatter videreformidling av informasjon som er skaffet til veie av andre at han kommer inn under ansvarsfriheten i e-handelsdirektivet. I den type virksomhet som jeg har gjort rede for i punkt 1.6.5 er det klart at host service leverandøren kun lagrer informasjon som er skaffet til veie av de som mottar tjenestene.

Til slutt er det et vilkår for å komme innunder anvendelsesområdet for art. 14 at lagringen av informasjon skjer «at the request of a recipient of the service». Denne passusen avgrenser mot de tilfeller der lagringen av den informasjonen som andre enn host service leverandøren har skaffet til veie, skjer etter hostens eget initiativ, og ikke etter initiativ fra en som er tjenestemottager i e-handelsdirektivets forstand. I de tilfeller som jeg har beskrevet i punkt 1.6.5, skjer lagringen av informasjon utelukkende etter initiativ fra en som er tjenestemottager i e-handelsdirektivets forstand.

Ut fra det foreliggende rettskildematerialet kan det, slik jeg ser det, ikke reises tvil om at virksomheten som er beskrevet som host service leverandør faller innunder de vilkår som oppstilles i art. 14.

Konklusjonen er at den virksomheten som det i punkt 1.6.5 er beskrevet at en host service leverandør driver er omfattet av ansvarsfrihetsreglene i art. 14 i e-handelsdirektivet.

2.7.3 Er vilkårene i art. 14, nr. 1, litra (a) for frihet fra strafferettslig ansvar oppfylt dersom host service provideren får en uspesifisert melding om at det er lagret ulovlig eller krenkende informasjon på hans servere og han ikke omgående fjerner eller stenger tilgang til denne?

Med uspesifisert melding mener jeg en anonym melding som angir at host service providerens server inneholder ulovlig eller krenkende informasjon, men som ikke gjør rede for hvilken URL informasjonen er tilgjengelig på, og som ikke nevner noe om hvilken type rettsbrudd den ulovlige informasjonen medfører.

I henhold til art. 14 nr. 1, litra (a), første passus, er det et vilkår for frihet fra strafferettslig ansvar at host service provideren ikke har «actual knowledge», eller faktisk kunnskap, om den ulovlige aktiviteten eller informasjonen.

I e-handelsdirektivet gis det, utover ordlyden i litra (a), ingen veiledning mht. hvordan kravet om faktisk kunnskap skal fortolkes. Problemet må derfor løses på grunnlag av ordlyden og en vurdering av de reelle hensyn som gjør seg gjeldende. I denne sammenheng må kravet om faktisk kunnskap særlig ses i sammenheng med fraværet av en generell undersøkelsesplikt i art. 15 nr. 1.

Det er viktig å merke seg at det å lokalisere ulovlig innhold på en av serverne til host service provideren, etter at denne har fått en uspesifisert melding om tilstedeværelsen av dette, vil innebære at han må søke igjennom all den informasjonen han lagrer.⁷² Derpå må han sørge for omgående å få fjernet eller hindret tilgangen til eventuelt ulovlig eller krenkende materiale dersom han ønsker å fortsatt være ansvarsfri, jfr. litra (b).

Det kan reises spørsmål om en slik plikt til gjennomgang av innholdet vil kunne være strid med e-handelsdirektivets art. 15 nr. 1 som oppstiller et forbud mot å pålegge de virksomheter som er omfattet av blant annet art. 14 en generell undersøkelsesplikt i forhold til den informasjon de lagrer. Det kan imidlertid hevdes at en uspesifisert melding, slik jeg har beskrevet den ovenfor, ikke pålegger host service provideren en generell, men heller en spesiell undersøkelsesplikt fordi det dreier seg om én konkret angivelse av ulovlig innhold. I preambelens punkt (47) presiseres art. 15 nr. 1 dithen at forbudet mot å pålegge overvåkingsplikter kun skal gjelde plikter av en generell natur, noe som ikke forhindrer at det oppstilles overvåkingskrav i en spesiell

⁷² Det er på det rene at enhver host service provider som driver en virksomhet av en viss størrelse normalt vil ha informasjon på sine servere som tilsvarer millioner på millioner av boksider. Selv ved bruk av teknologiske lokaliseringsmidler vil det by på en enorm oppgave å finne en bestemt bit med informasjon blant all den andre.

sak. På bakgrunn av disse uttalelsene kan jeg ikke se at forbudet mot å innføre en generell undersøkelsesplikt legger begrensninger på host service providers plikt til å undersøke servernes innhold i denne konkrete saken.

En språklig fortolkning av direktivets begrep faktisk kunnskap medfører at host service provideren må ha en uomtvistelig visshet om den ulovlige aktiviteten eller det ulovlige innholdet på serveren sin. Dette betyr at host service provideren må kjenne til innholdet av de data som han lagrer og som er krenkende eller ulovlige. Dertil må det etter min mening, på bakgrunn av den enorme informasjonsmengden som i de fleste tilfellene lagres hos host service provideren, innfortolkes et krav til faktisk kunnskap om hvor materialet er lokalisert på serverne slik at det er fysisk mulig å finne det igjen.

Det er på det rene at host service provideren etter en slik uspesifisert melding som jeg beskriver ovenfor ikke besitter den informasjon som er nødvendig for på en enkel måte verken å kunne identifisere eller lokalisere den ulovlige informasjonen eller aktiviteten.

Reelle hensyn tilsier at dersom kravet til faktisk kunnskap anses å være oppfylt i et tilfelle som dette, vil dette kunne virke urimelig ovenfor host service provideren på flere måter. For det første kan hans muligheter for å kunne oppfylle vilkårene for ansvarsfrihet i e-handelsdirektivet være avskåret allerede i utgangspunktet fordi ressursituasjonen i bedriften ikke tillater den belastning som det ville være å finne frem til én ulovlig side med informasjon blant millioner på millioner av andre. For det andre ville slike uspesifiserte meldinger lett kunne misbrukes av host service providers konkurrenter for å sette ham ut av spill for en tid. For det tredje er det under enhver omstendighet overveidende sannsynlig at serverne til host service provideren til enhver tid inneholder materiale som på et eller annet grunnlag er i strid med loven. En for streng tolkning av vilkåret faktisk kunnskap vil i sin ytterste konsekvens kunne lede til at denne vissheten avskjærer digitale mellomledds muligheter til å noensinne å oppfylle vilkårene for ansvarsfrihet.

På bakgrunn av e-handelsdirektivets formål, som blant annet er å sørge for informasjonsflyt og ytringsfrihet, jfr. preambelens punkt (8)-(10), kan det ikke være tvil om at en så vid fortolkning av begrepet faktisk kunnskap at også uspesifiserte meldinger skal omfattes vil føre for langt i forhold til de aktører som opererer som host service providere. Dette er fordi en slik tolkning av begrepet lett ville kunne gjøre forbudet mot en generell undersøkelsesplikt i art. 15 illusorisk, samtidig som det ville medføre tunge belastninger i forhold til ressursituasjonen til de digitale mellomledd, noe som igjen vil føre til at informasjonsflyten og ytringsfriheten på Internett blir truet.

På bakgrunn av et relativt entydig rettskildemateriale der både ordlyden, reelle hensyn og formålsbetraktninger taler for en restriktiv tolkning av

begrepet faktisk kunnskap finner jeg det klart at vilkåret ikke er oppfylt i dette tilfellet.

Konklusjonen er at vilkårene i art. 14, nr. 1, litra (a) for frihet fra straffetrettslig ansvar er oppfylt dersom host service provideren får en uspesifisert melding om at det er lagret ulovlig eller krenkende informasjon på hans servere selv om han ikke omgående fjerner eller hindrer tilgang til denne.

2.7.4 Er vilkårene for frihet fra sivilrettslig ansvar i art. 14, nr. 1, litra (a) oppfylt dersom host service provideren får en uspesifisert melding om at det er lagret ulovlig eller krenkende informasjon på hans servere og han ikke omgående fjerner eller hindrer tilgang til denne?

Når det gjelder hva som skal forstås med uspesifisert melding henviser jeg til forklaringen i punktet ovenfor.

Etter art. 14 nr. 1, litra (a), andre passus, er det et vilkår for frihet fra sivilrettslig ansvar at host service provideren ikke er «aware of the facts or circumstances from which the illegal activity or information is apparent». Dette kan omskrives til et krav om at tjenesteyteren ikke skal ha muligheter til konstruktiv kunnskap om den ulovlige informasjonen. Spørsmålet som reiser seg i denne sammenheng er hvorvidt man skal si at host service provideren, etter å ha fått en uspesifisert melding om at hans server(e) inneholder ulovlig materiale, er klar over fakta eller omstendigheter som gjør at den ulovlige aktivitet eller informasjon blir synlig. Ettersom kravet til kunnskap her utvides også til forhold som kan peke på den ulovlige informasjon er det klart at dette er et vilkår som innsnevrer området for ansvarsfriheten og som derfor er strengere i forhold til host service provideren enn kravet til faktisk kunnskap.

I e-handelsdirektivet gis det utover ordlyden i litra (a) ingen veiledning mht. hvordan kravet om mulighet til konstruktiv kunnskap skal fortolkes. Problemet må derfor også her løses på grunnlag av en språklig fortolkning av ordlyden i direktivet, en vurdering av uttalelser i preambelen, samt de reelle hensyn som gjør seg gjeldende. På samme måte som i drøftelsen over kan ikke forbudet mot en generell undersøkelsesplikt i art. 15, nr. 1 legge noen begrensninger på hvorvidt host service provideren, i ett konkret tilfelle, skal sies å ha en plikt til å gjennomføre en undersøkelse av den informasjonen som han lagrer. Heller ikke forbudet mot pålegge tjenesteytere en generell plikt til aktivt å søke fakta eller omstendigheter som indikerer ulovlig aktivitet, jfr. art. 15 nr. 1, siste komma, oppstiller noen begrensninger i dette tilfellet ettersom slike fakta eller omstendigheter allerede må sies å foreligge i og med den uspesifiserte meldingen.

Vilkåret etter nr. 1, litra (a) er at den uspesifiserte meldingen må gjøre den ulovlige aktivitet eller informasjon «apparent», eller synlig. I denne sammenhengen kan det ikke være tvil om at den uspesifiserte meldingen gjør tjenesteyteren oppmerksom på at han lagrer ulovlig informasjon. Hvorvidt den er synlig i direktivets forstand er mer tvilsomt. I denne sammenheng kan det spørres om host service provideren har noen plikt til å undersøke innholdet nærmere, slik at den ulovlige informasjonen eller aktiviteten blir synlig.

I henhold til preambelens punkt (48) legger ikke e-handelsdirektivet hindringer i veien for at mellomledd som lagrer informasjon for andre pålegges aktsomhetsplikter, «duties of care», som man med rimelighet kan forvente at de gjør for å oppdage og motvirke bestemte typer ulovlige aktiviteter. Dersom mellomleddet mottar en uspesifisert melding om at deres server(e) inneholder ulovlig innhold er det ut fra en tolkning av punkt (48) nærliggende å anta at de har en plikt til å undersøke innholdet nærmere. Imidlertid er det på bakgrunn av formuleringene i punkt (48), jfr. passusen «...med rimelighet kan forvente...», rimelig å hevde at undersøkelsesplikten må være relativ i forhold til hvilken type ulovlig innhold det er snakk om. En aktsomhetsplikt må for eksempel strekke seg vesentlig lenger der det er snakk om at mellomleddet lagrer barnepornografisk materiale enn der det lagrer programapplikasjoner som bryter mot forbrukervernlovgivningen. Fordi det i dette tilfellet ikke er mulig å fastslå hvilken type krenkende materiale host service providere lagrer kan man etter min mening ikke fra preambelens punkt (48) utlede noe avgjørende argument for at host service provideren skal anses for å ha en spesiell plikt til å undersøke serverne sine nærmere.

Det er under enhver omstendighet klar at det også i dette tilfellet vil innebære en omfattende innsats for host service provideren å lokalisere det ulovlige innholdet. Som tidligere nevnt må han iverksette undersøkelser av en informasjonsmengde som kan tilsvare millioner på millioner av boksider dersom han skal finne den ulovlige informasjonen. På denne bakgrunn finner jeg det ikke rimelig å si at den ulovlige eller krenkende informasjon eller aktivitet er synlig for host service provideren i tilfellet der han får en uspesifisert melding.

De reelle hensyn som jeg nevnte i drøftelsen i punktet ovenfor vil komme inn med samme vekt i denne drøftelsen. Urimeligheten av å pålegge en spesiell undersøkelsesplikt eller en aktsomhetsplikt etter preambelens punkt (48) i et tilfelle som dette, viser seg for det første ved at host service leverandørenes muligheter til å kunne oppfylle vilkårene for ansvarsfrihet i e-handelsdirektivet kan være avskåret allerede i utgangspunktet pga. ressursituasjonen i bedriften. For det andre kommer hensynet til å skjerme tjenestetilbyderen mot sine konkurrenter inn med samme vekt som i punktet over, og for det tredje taler hensynet for overhodet å kunne innfri vilkårene om ansvarsfrihet, når man som tjeneste-

ytter i de fleste tilfeller må regne det som overveidende sannsynlig at serverne til enhver tid inneholder ulovlig eller krenkende materiale, for at vilkåret om konstruktiv kunnskap her ikke er oppfylt.

Hvis man ser hen til e-handelsdirektivet formål, som er å sørge for informasjonsflyt og ytringsfrihet, jfr. preambelens punkt (8)-(10), kan det ikke være tvil om at en vid fortolkning av kravet til når den ulovlige informasjonen skal sies å være synlig for tjenesteyteren, vil føre for langt i forhold til de aktører som opererer som host service providere. Dette er fordi en vid fortolkning både kan gjøre fraværet av en generell undersøkelsesplikt illusorisk, og fordi det ville legge for stramme bånd på ressursituasjonen i de digitale mellomleddene, noe som igjen er egnet til å true både informasjonsflyt og ytringsfrihet på Internett.

Oppsummeringsmessig taler etter min mening et relativt entydig rettskildemateriale for en restriktiv fortolkning av kravet til når ulovlig informasjon eller aktivitet skal anses for å være synlig for host service provideren. Vilkaåret om konstruktiv kunnskap kan derfor ikke være oppfylt i dette tilfellet.

Konklusjonen er at vilkårene i for frihet fra sivilrettslig ansvar i art. 14, nr. 1, litra (a) er oppfylt dersom host service provideren får en uspesifisert melding om at det er lagret ulovlig eller krenkende informasjon på hans servere selv om han ikke omgående fjerner eller hindrer tilgang til denne.

2.7.5 Er vilkårene for frihet fra strafferettslig ansvar i art. 14, nr. 1, litra (a) oppfylt for en host service provider som også utvikler de programapplikasjoner som lagres på hans server dersom han videreformidler krenkende eller ulovlig informasjon eller aktivitet som ligger implementert i den applikasjon som han har utviklet, etter at rettighetene til programapplikasjonen er overdratt til tjenestemottageren for hostingtjenestene, og han ikke fjerner eller stenger tilgangen til informasjonen?⁷³

Spørsmålet er om den host service provider som utvikler egne programapplikasjoner, og som senere opptrer som host service provider for de samme app-

⁷³ Grunnen til at jeg stiller dette spørsmålet er at det er meget viktig for de mellomledd som jeg ovenfor, i fotnote nr. 22, kaller for ASP-leverandører å vite at kravet til faktisk kunnskap om ulovlig eller krenkende innhold kan være oppfylt allerede fordi de har utviklet plattformen for f.eks. en e-handelsløsning. I denne sammenheng kan det f.eks. stilles spørsmål om kravet til kunnskap om ulovlig eller krenkede informasjon eller aktivitet er oppfylt ved at modulen for avtaleinngåelse ikke tar høyde for næringsdrivendes plikter i forbrukervernlovgivningen, f.eks. selgers opplysningsplikt før avtaleinngåelsen i forhold til forbrukeren, jfr. angrerettloven kap. 2, kan være misligholdt fordi de nødvendige opplysninger ikke er implementert i handelsmodulen.

likasjonene, etter at disse er overdratt til den som mottar hostingtjenestene, må sies å oppfylle kravet til faktisk kunnskap, jfr. art. 14, nr. 1 litra (a), om den ulovlige eller krenkende informasjonen eller aktiviteten som ligger implementert i den applikasjon han har utviklet. Jeg vil presisere at jeg i denne drøftelsen ikke tar stilling til hvorvidt host service provideren skal risikere ansvar for informasjon som tjenestemottageren legger inn i de utviklede programapplikasjoner etter at den er ferdig utviklet og overdratt.

Som jeg har nevnt ovenfor gir verken direktivet selv eller preambelen noen veiledning mht. hvordan vilkåret om faktisk kunnskap her skal fortolkes. Spørsmålet må derfor løses ut fra en språklig fortolkning av ordlyden, samt de reelle hensyn som gjør seg gjeldene i dette tilfellet.

En språklig fortolkning av direktivets begrep faktisk kunnskap medfører også i denne sammenhengen at host service provideren må ha en uomtvistelig visshet om den ulovlige aktiviteten eller det ulovlige innholdet på serveren sin. Dette betyr at host service provideren må kjenne til innholdet av de data som han lagrer og som er krenkende eller ulovlige. Også her må det innfortolkes et krav til faktisk kunnskap om hvor det ulovlige materialet er lokalisert på serverne, slik at host service provideren har en rimelig mulighet til å finne det.

I det tilfelle jeg har skissert i problemstillingen ovenfor er spørsmålet om den ulovlige informasjon eller aktivitet kan sies å ha kommet til host service providerens kunnskap ettersom han selv har utviklet de programapplikasjoner som inneholder den ulovlige informasjon eller aktivitet. I denne sammenheng kan det være tvilsomt om hosteren har kunnskap om de reglene som gjør informasjonen eller aktiviteten ulovlig. Det kan også reises spørsmål om han har kunnskap om at den aktuelle informasjonen eller aktiviteten faller inn under de regler som gjør virksomheten ulovlig. Villfarelse i forhold til hvilke rettsregler som eksisterer og hvilke tilfeller de omfatter kan imidlertid ikke gjøre host service provideren ansvarsfri. Dette er i tråd med et alminnelig prinsipp i blant annet norsk strafferett, som sier at rettsvillfarelse, for de fleste praktiske formål, ikke frifinner tiltalte. Det avgjørende må derfor være hvorvidt hosteren har faktisk kunnskap om de deler av eller aspekter ved de programapplikasjoner som han utvikler og som gir objektive holdepunkter for å fastslå at loven er brutt. En slik kunnskap må det, etter min mening, utvilsomt sies at host service provideren har når han selv har forestått utviklingen av programapplikasjonen i hver minste detalj.

Reelle hensyn tilsier at den profesjonelle aktør som begir seg inn på profesjonell utvikling og hosting av programapplikasjoner selv bør bære den risikoen som markedet medfører i forhold til hans virksomhet. Dette underbygges av at han, i og med at han gjør valget om å drive næringsvirksomhet på dette området, må sies å gjøre et valg med hensyn til den risiko han er villig

til å ta i forhold til den virksomheten han driver. Det faktum at området er komplisert og uoversiktlig både praktisk/teknologisk og juridisk kan ikke moderere dette synspunktet.

Det kan imidlertid hevdes at et ansvarsgjennombrudd i dette tilfellet vil ramme enkelte host service providere unødig hardt. Mange av disse aktørene kan være relativt nystartede gründerbedrifter der ressursituasjonen, kanskje særlig med hensyn til juridisk kompetanse, er knapp. Et slikt argument kan ikke la seg høre all den tid utviklingen mot et godt fungerende marked for digitale aktører forutsetter at de nødvendige tilpasninger til lovens krav blir gjort.

På bakgrunn av en språklig fortolkning av direktivets ordlyd og en vurdering av de reelle hensyn som er aktuelle i dette tilfelle, er jeg kommet til at vilkåret om faktisk kunnskap må være oppfylt i dette tilfellet.

Konklusjonen er at vilkårene for frihet fra strafferettslig ansvar i art. 14, nr. 1, litra (a) ikke er oppfylt for en host service provider som også utvikler de programapplikasjoner som lagres på hans server dersom han videreformidler krenkende eller ulovlig informasjon eller aktivitet som ligger implementert i den applikasjon som han har utviklet etter at rettighetene til programapplikasjonen er overdratt til tjenestemottageren for hostingtjenestene, og han ikke fjerner eller stenger tilgangen til informasjonen.

2.7.6 Er kravene for ansvarsfrihet i e-handelsdirektivets art. 14 oppfylt for en host service provider som innfører rutiner for overvåkning og kontroll av det materialet som blir tilveieskaffet av tjenestemottageren for hostingtjenestene?⁷⁴

De rutiner for overvåkning og kontroll som jeg her behandler kan omfatte flere tiltak. Som eksempel kan jeg nevne tilfeller der host service provideren installerer teknologiske filter for å lokalisere ord eller uttrykk som kan indikere ulovlig eller krenkende innhold, tilfeller der det gjøres manuelle stikkprøver av innholdet i de programapplikasjoner som lagres og tilfeller der alle programapplikasjoner gjennomgås på en rutinemessig basis før de gjøres tilgjengelige gjennom host service providerens server.

Det første spørsmålet som må tas stilling til i denne sammenheng er hvorvidt den som opererer som host service provider overhodet har rett til å gjennomføre slike rutiner for kontroll og overvåkning som jeg skisserer ovenfor.

⁷⁴

Grunnen til at jeg stiller dette spørsmålet er at mange av de digitale mellomledd som tilbyr f.eks. handletjenester på Internett bruker til dels store ressurser på å overvåke eller gjøre stikkprøver i de programapplikasjoner som de lagrer for de enkelte nettbutikkene. Formålet med overvåkingen eller stikkprøvene er å lokalisere ulovlig eller krenkende innhold samt å fjerne dette for på denne måten å unngå eventuelt ansvar.

Mest iøynefallende i denne sammenheng er spørsmålet hvorvidt digitale mellomledd på et generelt plan skal ha rett til å gjennomføre undersøkelser av den informasjon som de lagrer. Forbudet i e-handelsdirektivets art. 15, som nekter de enkelte medlemsstatene å gjennomføre en generell undersøkelsesplikt i forhold til den informasjonen de lagrer, kan ikke legge hindringer i veien for den enkelte tjenesteyters adgang til, på eget initiativ, å utføre generelle undersøkelser av det materiale de lagrer. Poenget med art. 15 er at myndighetene ikke skal kunne legge en slik plikt på de digitale mellomledd mot deres vilje. Når det gjelder de formene for overvåkning og kontroll av innhold som ikke innebærer slike generelle undersøkelser som er nevnt i e-handelsdirektivets art. 15 er saken helt klar. I preambelens punkt (48) sies det at direktivet ikke skal medføre noen hindring for de nasjonale myndigheter, dersom det skjer gjennom lovgivning, å pålegge den som er host service provider for informasjon å være så aktsomme som det kan forventes for å oppdage og motvirke bestemte typer illegal aktivitet. På denne bakgrunn kan det ikke være tvilsomt at host service provideren har rett til å gjennomføre slike tiltak på eget initiativ.

I e-handelsdirektivets art. 14 oppstilles det ikke som noe vilkår for ansvarsfrihet at host service provideren ikke er involvert i den lagrede informasjon, enten ved at han endrer, velger ut eller stanser den informasjon han skal lagre. Dette innebærer at host service provideren kan spille en aktiv rolle i forhold til utvalg, endring og teknisk manipulasjon av den informasjon han lagrer, og fremdeles befinne seg innenfor rammene for ansvarsfrihet etter e-handelsdirektivet. Det er imidlertid viktig å peke på at host service providens ansvarsfrihet etter e-handelsdirektivet har to klare grenser avhengig av i hvilken grad han har befatning med den informasjon som han lagrer.

For det første vil en utstrakt grad av engasjement i den informasjon som lagres kunne reise spørsmål om ikke host service provideren må være å anse som en ren innholdsleverandør. Dersom det som angivelig er kontroll og overvåkning går så langt at den informasjon som er tilveieskaffet av tjenestemottageren, som følge av manuelle eller tekniske manipulasjoner, blir endret eller bearbeidet dithen at den får ny mening eller en vesentlig annen utforming enn den opprinnelige, vil det kunne hevdes at host service provideren er innholdsleverandør og dermed risikerer et direkte, selvstendig ansvar for ytringene. Det må understrekes at det generelt skal svært mye til før de manipulasjoner eller endringer som foregår i en overvåkning eller kontroll av materiale kvalifiserer til å være ren innholdsproduksjon. I forhold til aktører som søker å omgå regelverket er det likevel viktig å være klar over problemstillingen. Den kontroll og overvåkning jeg skisserer i problemstillingen ovenfor medfører ikke slik grad av innholdsmanipulasjon at host service provideren kan anses for å være innholdsleverandør.

For det andre vil mange måter å involvere seg i det materiale han lagrer, enten det er utsiling av bestemte ord og uttrykk ved hjelp av filter, eller rent fysisk gjennomlesning av informasjon, medføre at host service provideren enten må sies å ha faktisk kunnskap om ulovlig eller krenkende informasjon, eller at han må sies å være klar over fakta eller omstendigheter som gjør den ulovlige informasjon eller aktivitet synlig. De fakta som fremgår av problemstillingen ovenfor gir ikke tilstrekkelige holdepunkter for å vurdere hvorvidt gjennomføringen av overvåkning eller kontroll medfører at kravene til kunnskap i art. 14, nr. 1, litra (a) er oppfylt. Det forutsettes imidlertid at den kunnskap som er nødvendig for at ansvarsfriheten skal opphøre, ikke er tilstede i dette tilfelle.

På bakgrunn av at overvåkning og kontroll som kan medføre både utvelgelse, endring og tekniske manipulasjoner av det innhold som lagres på host service providerens server ikke faller utenfor de vilkårene som e-handelsdirektivets art. 14 oppstiller for ansvarsfrihet er jeg kommet til at ansvar på grunn av ansvarsfrihetsreglene i direktivet ikke kan pålegges host service provideren i dette tilfellet. Som det fremgår over gjelder dette kun så lenge kravene til kunnskap i art. 14, nr. 1, litra (a) ikke er oppfylt, og så lenge gjennomføringen av overvåknings-, og kontrollvirksomheten ikke må sies å medføre egen innholdsproduksjon.

Konklusjonen er at kravene for ansvarsfrihet i e-handelsdirektivets art. 14 er oppfylt for en host service provider som innfører rutiner for overvåkning og kontroll av det materialet som blir tilveieskaffet av tjenestemottageren for hostingtjenestene.

2.7.7 Er vilkårene for ansvarsfrihet i henhold til art. 14, nr. 1, litra (a) oppfylt dersom en host service provider ikke stenger tilgangen til informasjon, hvis lovlighet er omtvistet, og som han lagrer, etter at han har fått en melding som angir hvor informasjonen er å finne og på hvilket grunnlag den angivelig er ulovlig, og det senere viser seg at det var riktig å bygge på meldingsavgiverens rettsoppfatning?⁷⁵

I henhold til e-handelsdirektivets art. 14, nr. 1, litra (a) er vilkåret for ansvarsfrihet i forhold til den informasjon som host service provideren lagrer for en tjenestemottager at han ikke har faktisk eller konstruktiv kunnskap om «illegal» aktivitet eller informasjon.

Spørsmålet i dette punktet er hvem som skal ha risikoen for de rettsoppfatninger som knytter seg til hvorvidt en viss type aktivitet eller informasjon, hvis lokalisering er kjent, er lovlig eller ikke.

Verken direktivet eller preambelen gir noen nærmere veiledning mht. hvordan denne risikoavveiningen skal foretas.

Det er et alminnelig juridisk prinsipp at retten, for alle praktiske tilfeller, skal tolkes objektivt. Dette innebærer at alle involverte parter selv må bære risikoen for eventuelt gale rettsoppfatninger frem til tvistespørsmålet har fått sin avklaring i et kompetent tvisteløsningsorgan.⁷⁶ Som jeg tidligere har nevnt taler reelle hensyn i denne sammenhengen for at en næringsdrivende selv bærer den risiko hans virksomhet medfører. Det er nemlig rimelig at han som profesjonell aktør i markedet, etter beste evne, setter seg inn i og retter seg etter de regler som gjelder for den type virksomhet som han har valgt å drive.

Det er på denne måten klart at risikoen for rettsoppfatningen mht. hvorvidt den lagrede informasjon er krenkende eller ulovlig i forhold til tredjemann fullt og helt må påhvile host service provideren. Dersom det etter en objektiv vurdering skulle vise seg at aktiviteten eller informasjonen faktisk var ulovlig, medfører dette at host service provideren vil kunne risikere ansvar for lagringen.

⁷⁵ Grunnen til at jeg stiller dette spørsmålet er at det i mange tilfeller kan være tvilsomt hvorvidt innhold i et konkret tilfelle faktisk bryter mot lovgivningen. Dette gjør at host service provideren av hensyn til muligheten for eventuelt erstatningssøksmål fra en medkontrahent kan være motvillig til å stenge tilgangen til det aktuelle materialet. Det er derfor viktig å belyse hvor risikoen for de rettsoppfatninger som knytter seg til dette spørsmålet ligger i forhold til de ansvarsreglene som e-handelsdirektivet oppstiller. Problemstillingen danner for øvrig grunnlaget for en av de sentrale drøftelsen under oppgavens del 3, som tar for seg viktige de lege ferenda-spørsmål.

⁷⁶ I Norge er det Høyesterett som er tvisteløsningorgan i siste instans. Når dom er falt i Høyesterett er derfor tvistespørsmålet, og derved hvem som til slutt må bære risikoen for sin rettsoppfatning, endelig avgjort.

Konklusjonen er derfor at vilkårene for ansvarsfrihet i henhold til art. 14, nr. 1, litra (b) ikke er oppfylt dersom en host service provider ikke stenger tilgangen til informasjon som han lagrer, hvis lovlighet er omtvistet, etter å ha fått en melding som angir hvor informasjonen er å finne og på hvilket grunnlag den angivelig er ulovlig, og det senere viser seg at det var riktig å bygge på meldingsavgiverens rettsoppfatning.

2.8 Spørsmål om ansvarsfrihet for den virksomhet som i punkt 1.6.6 er beskrevet som bulletin board operator

2.8.1 Hjemmel

I henhold til e-handelsdirektivets art. 14, nr. 1 skal tjenesteyteren, så lenge vilkårene i artikkelens litra (a)-(b) er oppfylt, være ansvarsfri dersom han skaffer til veie en informasjonssamfunnstjeneste som består i lagring av informasjon som er skaffet til veie av en mottaker av tjenesten og informasjonen er lagret etter forespørsel fra en mottaker av tjenesten.

EU-direktivet skiller i art. 14, nr. 1, litra (a) mellom sivil-, og strafferettslig ansvar idet det etablerer forskjellige ansvarskriterier for at hver av disse type-ene ansvar skal inntre. Strafferettslig ansvar krever at host service provideren har faktisk kunnskap om den ulovlige aktivitet eller informasjon, mens et sivilrettslig ansvar krever at host service provideren har det jeg kaller konstruktiv kunnskap om den ulovlige aktivitet eller informasjon. På tross av at det foreligger slik kunnskap som jeg beskriver kan tjenesteyteren være ansvarsfri etter art. 14, nr. 1, litra (b) dersom han omgående, etter at han har fått kunnskap om de ulovlige forhold, fjerner eller stenger tilgangen til den ulovlige informasjonen eller aktiviteten.

2.8.2 Er den virksomhet som i punkt 1.6.6 er beskrevet som bulletin board operator omfattet av e-handelsdirektivets art. 14 når tjenesteyteren eier serveren som tjenestemottageren bruker?

Det første vilkåret for at en bulletin board operatørs tjeneste skal være omfattet av art. 14 er at den utgjør en informasjonssamfunnstjeneste i e-handelsdirektivets forstand. Kravet etter art. 14 nr. 1 er at virksomheten utgjør en tjeneste som normalt sett ytes mot vederlag, på avstand, med elektroniske midler og på individuell forespørsel fra en som er mottaker av tjenestene.

I følge drøftelsen som fremgår av punkt 2.3.2 er de krav som stilles for at virksomheten skal være av en karakter som normalt skjer mot vederlag ikke

særlig omfattende. I denne sammenheng må det avgjørende være hvorvidt bulletin board operatoren yter sine tjenester i en eller annen form for næringsvirksomhet. De typer bulletin board-virksomhet som jeg beskriver i denne oppgaven ytes alle i profesjonelle forhold der meningen er å sørge for verdiskapning. Jeg anser derfor vilkåret om at virksomheten normalt sett ytes mot vederlag oppfylt for bulletin board operatorens del.

Et videre vilkår er at bulletin board-virksomheten må utøves på avstand og med elektroniske midler. Fordi det ligger i bulletin board-virksomhetens funksjonalitet at den skjer mens partene ikke er sammen tilstede, samt at den skjer ved bruk av datamaskiner, finner jeg ikke grunn til å tvile på at dette vilkåret er oppfylt.

Siste vilkår for at bulletin board-virksomhet skal være en informasjons-samfunnstjeneste i e-handelsdirektivets forstand er at tjenesten må skje «at the request of a recipient of the service». Vilkalet volder ikke problemer i dette tilfellet fordi direktivets definisjon omfatter alle som gjør bruk av en informasjonssamfunnstjeneste både for å søke informasjon, samt å gjøre informasjon tilgjengelig over Internett, jfr. punkt 2.3.3. Vilkalet om individuell forespørsel sikter, som jeg tidligere har nevnt, mot å trekke opp grensen mot blant annet kringkastingstjenester, som ytes uten at tjenestemottageren faktisk har vært i kontakt med kringkasteren. Bulletin board-tjenestene ytes kun etter en konkret kontakt mellom tjenesteoperatøren og tjenestemottageren. Dette skjer enten ved at de slutter en personlig avtale, eventuelt ved at tjenestemottageren, før han kan ta i bruk tjenesten, har oppsøkt bulletin board operatorens tjenester på Internett. På bakgrunn av dette regner jeg det derfor som sikkert at bulletin board-tjenestene ytes på individuell forespørsel fra tjenestemottageren.

I tillegg til at den virksomhet som utøves må være en informasjonssamfunnstjeneste er det et vilkår at bulletin board operatørens virksomhet innebærer en lagring av informasjon som er skaffet til veie av en tjenestemottager. Det gis verken i e-handelsdirektivets ordlyd eller i preambelen noen nærmere holdepunkter for hvordan ordet «storage», eller lagring skal fortolkes. Et aspekt av den virksomheten som en bulletin board operatøren driver må likevel trygt kunne sies å være innenfor den språklige forståelse av begrepet lagring slik dette må forstås i e-handelsdirektivets forstand. De tilfeller jeg her tenker på er der tjenestetilbyderen sørger for mer varig plassering av forskjellige typer informasjon, som for eksempel kontaktannonser, varebyttesider og leieformidling av husrom, på sine servere. I forhold til et annet aspekt ved bulletin board operatørens virksomhet kan spørsmålet hvorvidt det foreligger en lagring av informasjon være mer tvilsomt. Jeg tenker i denne sammenheng på de tjenester som innebærer at tjenesteyterens servere står til disposisjon for

forskjellige sanntids diskusjons-, og samtalegrupper på Internett. Det som skiller denne type virksomhet fra den gjenlegging av beskjeder eller meldinger som jeg skisserer i tilfellet over er at den informasjon tjenestemottageren legger inn på serveren eksisterer bare i de sekundene den er synlig på nettsiden. Med andre ord blir ikke noe av denne informasjonen arkivert på serveren til bulletin board operatøren. Det problem som reiser seg i forhold til e-handelsdirektivets art. 14 er om slike tjenester kan sies å medføre noen «storage» av informasjon. Den språklige forståelsen av ordet «storage» innebærer, slik jeg ser det, at den informasjon som skaffe til veie av tjenestemottageren må oppbevares over en viss tid. Hvorvidt den meget kortvarige oppbevaringen av data som bulletin board tjenestene innebærer faller innunder direktivets ordlyd kan derfor være noe tvilsomt. Til avklaring av dette spørsmålet er det derfor nødvendig å se hen til de reelle hensyn som gjør seg gjeldene i dette tilfellet. I denne sammenhengen kan det hevdes at det er urimelig å behandle bulletin board operatøren forskjellig fra host service provideren. Begge virksomhetene innebærer at det skaffes til veie serverkapasitet som er nødvendig for å tilgjengeliggjøre og spre informasjon, eller drive forskjellige andre aktiviteter på Internett. I denne sammenheng er det behov som virksomhetene har for ansvarsfrihet like stort. Dersom man skulle komme til at sanntidskommunikasjon faller utenfor hovedregelen om ansvarsfrihet i art. 14 vil dette medføre både at fraværet av en generell undersøkelsesplikt i direktivets art. 15 lett blir illusorisk ved at tjenesteyteren blir tvunget til å overvåke tjenesten, samt at hensynet til ytringsfrihet og Internett som et effektivt medium for å drive meningsutveksling ikke blir tilstrekkelig ivaretatt. På denne bakgrunn er det derfor, etter min mening, gode grunner til å åpne for en pragmatisk tolkning av direktivets begrep «storage» i dette tilfellet.

Resultatet av drøftelsen er på bakgrunn av argumentene ovenfor at sanntidstilfellene faller inn under e-handelsdirektivets begrep «storage».

Kravet om at informasjonen må være tilveieskaffet av tjenestemottageren er, som jeg tidligere har nevnt, ment for å trekke opp grensen mot de tilfeller der bulletin board operatøren selv må karakteriseres som innholdsleverandør. Det er nemlig bare i de tilfeller der hans virksomhet omfatter videreformidling av andres informasjon han kommer inn under ansvarsfriheten i e-handelsdirektivets art. 14. For de tilfeller der bulletin board-tjenestene ytes uten at den informasjon som videreformidles overvåkes eller på annen måte påvirkes av bulletin board operatøren, eventuelt representanter for denne, er derfor saken klar. Her er den informasjonen som videreformidles skaffet til veie av en aktør som er tjenestemottager i e-handelsdirektivets forstand. Der det imidlertid i bulletin board operatørens tjeneste inngår et engasjement fra

en såkalt host master, eller interaktiv gruppeleder⁷⁷, kan det være tvilsomt om den informasjon eller aktivitet som denne genererer kan sies å være tilveieskaffet av en som er tjenestemottager i direktivets forstand. Det må i denne sammenheng være på det rene at den informasjonen eller aktiviteten som den interaktive gruppelederen selv genererer og publiserer på vegne av bulletin board provideren gjennom tjenesten ikke kan sies å være tilveieskaffet av en som er mottager for tjenestene. I dette tilfellet kan det hevdes å foreligge en identifikasjon mellom den interaktive gruppelederen og bulletin board operatøren. På samme tid må det være klart at uavhengige aktører som deltar i for eksempel en diskusjonsgruppe som inngår i bulletin board operatørens tjenester må sies å være tjenestemottagere. Den informasjon eller aktivitet disse genererer må derfor sies å være skaffet til veie av en tjenestemottager i direktivets forstand.

Det spørsmål man etter dette må ta stilling til er hvorledes den bulletin board-tjenesten der operatøren stiller med interaktiv gruppeleder skal vurderes opp mot vilkåret om at den informasjon eller aktivitet som lagres må være skaffet til veie av en tjenestemottager. Det er klart at det må være en glidende overgang mellom de tilfeller der man kommer til at den informasjon eller aktivitet som genereres ved bruk av tjenesten er tilveieskaffet av en som er tjenestemottager og de tilfeller der informasjonen eller aktiviteten, ihvertfall delvis, må sies å være tilveieskaffet av bulletin board operatøren selv. Jeg ser i denne sammenheng ingen hindringer for at man, i tilfelle tvist om hvorvidt en tjeneste skal sies å være omfattet av art. 14 eller ikke, vurderer konkret hvilken grad av innholdsproduksjon den interaktive gruppelederens innblanding medfører. På denne måten kan man vurdere hver enkelt aktørs uttalelser separat i forhold til spørsmålet om ansvarsfrihet etter art. 14. Jeg kan ikke se at en slik ordning skulle by på verken tekniske eller juridiske problemer. I det tilfellet jeg drøfter under dette punktet forutsetter jeg at den digitale gruppelederens innblanding i bulletin board-tjenesten er på et minimalt nivå og kun strekker seg til overvåkning av den informasjon og aktivitet som tjenestemottagerne frembringer. Jeg forutsetter derfor at den informasjon som formidles er skaffet til veie av en tjenestemottager.⁷⁸

Til sist er det et vilkår for å komme innunder anvendelsesområdet for art. 14 at lagringen av informasjon skjer «at the request of a recipient of the ser-

⁷⁷ Se beskrivelsen i punkt 1.6.6.

⁷⁸ Et spørsmål som gjør seg gjeldende i forhold til et annet aspekt ved reguleringene i direktivets art. 14, er hvorvidt en slik overvåkning kan sies å medføre at kravene til kunnskap i nr. 1, litra (a) er oppfylt dersom det skulle vise seg at den informasjon eller aktivitet som videreformidles er ulovlig. Vilårene om kunnskap er behandlet tidligere i oppgaven, og jeg skal ikke vie dem mer plass her.

vice». Denne passusen avgrenser mot de tilfeller der lagringen av den informasjonen som andre enn bulletin board operatøren har skaffet til veie, skjer etter tjenesteyterens eget initiativ, og ikke etter initiativ fra en som er tjenestemottager i e-handelsdirektivets forstand. I de tilfeller jeg har beskrevet i punkt 1.6.6, skjer lagringen av informasjon utelukkende etter initiativ fra en som er tjenestemottager i e-handelsdirektivets forstand. Vilkåret volder derfor ikke problemer i vårt tilfelle.

Etter en vurdering av det rettskildematerialet som er tilgjengelig er det, slik jeg ser det, ikke tvilsomt at den virksomhet som bulletin board operatøren driver faller innunder anvendelsesområdet for art. 14.

Konklusjonen er at den virksomhet som i punkt 1.6.6 er beskrevet som bulletin board operator er omfattet av e-handelsdirektivets art. 14 når tjenesteyteren eier serveren som tjenestemottageren bruker.

2.8.3 Er den virksomhet som i punkt 1.6.6 er beskrevet som bulletin board operator omfattet av e-handelsdirektivets art. 14 når tjenesteyteren ikke selv besitter serveren han bruker for å lagre informasjon og tilgjengeliggjøre sine tjenester?

Som nevnt ovenfor kan tilbudet av en bulletin board operators tjenester omfatte så vel utleie/utlån av plass til bulletin board-applikasjoner på egen server, som fremleie/utlån av andre aktørers serverplass.⁷⁹ Spørsmålet som reiser seg i forhold til e-handelsdirektivets art. 14 er om bulletin board operatørens virksomhet er omfattet av bestemmelsen også i de tilfellene der han ikke selv besitter den serveren som bulletin board-programapplikasjonene ligger på.

Virksomheten jeg drøfter i dette punktet skiller seg fra den i punktet over i kun ett henseende, nemlig i forhold til hvem som besitter den server som informasjon lagres på. Jeg forutsetter derfor at vilkårene i art. 14 om at bulletin board-tjenesten må utgjøre en informasjonssamfunnstjeneste er oppfylt i dette tilfellet. Jeg forutsetter videre at bulletin board operatørens virksomhet under enhver omstendighet ikke strekker seg lenger enn til å skaffe til veie en

⁷⁹ Den funksjonsoppdelingen jeg beskriver her er ikke uvanlig i det digitale markedet. Blant annet kan jeg nevne at en stor internettaktør som Scandinavia Online AS, URL: <http://www.sol.no>, leier serverplass til sine programapplikasjoner hos teknologileverandøren Infostream AS. En slik funksjonsoppdeling er ofte hensiktsmessig ettersom driften av en serverpark forutsetter en helt annen type kompetanse enn tilrettelegging av bulletin board-tjenester. Hvis den teknologiske utviklingen forsetter i det tempo som vi har sett til nå, er det ventelig at flere og flere internettaktører vil sette ut den teknologiske driften av sine tjenester til spesialiserte firma. Spørsmålet jeg drøfter i dette punktet kan derfor vise seg å være prinsipielt viktig.

tjeneste som består i en tilretteleggelse for videreformidling over Internett av informasjon som er skaffet til veie av andre, for eksempel ved utlån/utleie av en programapplikasjon for virtuelle samtaletjenester.

Spørsmålet det gjenstår å ta stilling til er hvorvidt bulletin board operatørens virksomhet kan sies å være «storage» av informasjon, når han ikke besitter serveren han bruker for å tilgjengeliggjøre sine tjenester. E-handelsdirektivet gir utover ordlyden ingen veiledning om hvordan begrepet «storage» skal forstås. Spørsmålet må derfor løses på grunnlag av en språklig fortolkning av ordet, samt de reelle hensyn som gjør seg gjeldende i denne sammenheng.

En tolkning av ordet «storage» er at man lar begrepet omfatte kun en passiv oppbevaring av informasjon på en server. En slik forståelse innebærer at kun de virksomheter der det er skjedd en nedlasting av informasjon på en server som aktøren selv besitter, er omfattet av uttrykket. Oppfatter man ordet på denne måten leder det til at bulletin board-tjenesten faller utenfor hovedregelen om ansvarsfrihet i art. 14, nr. 1. En annen fortolkning kan etter min mening forsvares hvis man tolker ordet lagring i retning av å omfatte den handling som medfører selve innsamlingen av informasjon. I denne sammenheng kan det hevdes at den aktiviteten som bulletin board operatøren utviser ved tilretteleggelse for innhenting av informasjon gjør det naturlig å karakterisere hans virksomhet som lagring, selv om informasjonen ender på en fremmed server. Som det skulle fremgå gir imidlertid ikke e-handelsdirektivets ordlyd noen sikre holdepunkter for hvorvidt bulletin board operatøren skal nyte godt av hovedregelen om ansvarsfrihet i tilfellet jeg drøfter. Avgjørende må derfor være de reelle hensyn som gjør seg gjeldende.

For det første vil det, etter min mening, by på en urimelig og tilfeldig løsning dersom en bulletin board operatør, i forhold til e-handelsdirektivets ansvarsregler, skal bedømmes strengere enn en annen fordi han har valgt å organisere sin bedrift slik at teknologisk avanserte oppgaver plasseres ut til et organ som har større kompetanse og ressurser til å håndtere disse. En slik løsning medfører først og fremst en hensiktsmessig arbeidsfordeling.

For det annet er det nærliggende å anta hensynet til å sikre en godt fungerende Internett-infrastruktur vil stå i fare for å bli undergravet dersom bulletin board operatøren risikerer ansvar etter en slik funksjonsfordeling som jeg skildrer i dette punktet. Den naturlige konsekvens av en risiko for ansvar som oppstår i og med en outsourcing av teknologi er jo nettopp at outsourcingen opphører. Ressursfordeling på slike vilkårene kan derfor komme til å medføre at bulletin board-tjenestene vil lide pga. en større generell belastning på operatøren, samt at totalkapasiteten i Internett-infrastrukturen blir mindre enn det som er nødvendig.

På bakgrunn av de reelle hensyn synes jeg derfor det er naturlig å tolke av direktivets ordlyd dithen at bulletin board operatørens virksomhet omfattes av ordet «storage», selv om han ikke selv besitter den serveren som informasjonen lagres på.

Konklusjonen er at den virksomhet som i punkt 1.6.6 er beskrevet som bulletin board operator er omfattet av e-handelsdirektivets art. 14 selv om tjenesteyteren ikke eier den serveren som han bruker til å lagre informasjon og formidle sine tjenester

2.8.4 Er vilkårene for ansvarsfrihet i art. 14 oppfylt dersom en bulletin board operatør videreformidler en av sine arbeidstakers ulovlige eller krenkende ytringer når disse er fremsatt i arbeidstiden, men ikke har noen sammenheng med de oppgaver arbeidstakeren er satt til å gjøre, og arbeidstakeren er tjenestemottaker for arbeidsgiverens bulletin board-tjenester?

Jeg forutsetter i dette punktet at arbeidstakeren har en heltids stilling i bulletin board operatørens virksomhet. Videre legger jeg til grunn at forholdet aktørene imellom er etablert i arbeidsavtale som oppfyller alle lovens krav.

En annen forutsetning for drøftelsen er at bulletin board operatørens virksomhet oppfyller vilkårene for i utgangspunktet å falle innunder hovedregelen om ansvarsfrihet i art. 14 nr. 1. Bulletin board-tjenesten er derfor en informasjonssamfunnstjeneste som består i lagring av informasjon som er skaffet til veie av en som er tjenestemottager i direktivets forstand. I tillegg forutsettes det at bulletin board operatøren ikke har den kunnskap om arbeidstakerens krenkende eller ulovlige ytringer som skisseres i nr. 1, litra (a).

På bakgrunn av de forutsetningene jeg oppstiller er det klart at bulletin board operatørens virksomhet i utgangspunktet faller inn under e-handelsdirektivets hovedregel om ansvarsfrihet.

I henhold til art. 14 nr. 2 skal imidlertid ikke art. 14 nr. 1 komme til anvendelse når tjenestemottageren handler under bulletin board operatørens autoritet eller kontroll. Skulle man derfor komme til at arbeidstakeren handler under bulletin board operatørens autoritet eller kontroll når han i arbeidstiden, og uten sammenheng med arbeidet forøvrig, benytter dennes tjenester for å fremsette ulovlige eller krenkende ytringer, så kommer ikke art. 14 nr. 1 til anvendelse.

Spørsmålet som reiser seg er om den situasjon jeg skisserer ovenfor medfører at en arbeidstaker handler under bulletin board operatørens autoritet eller kontroll slik disse begrepene må oppfattes i e-handelsdirektivets forstand. Til fortolkning av uttrykkene gis det i direktivet ingen veiledning utover hvorledes ordlyden må forstås etter en språklig analyse. Heller ikke i pream-

belen finnes det noen retningslinjer for hvordan begrepene skal forstås. Pga. det EU-rettslige tolkningsprinsipp, som sier at EU-direktiver skal undergis en autonom fortolkning⁸⁰, er det ikke riktig å legge vekt på de rettskilder som behandler tilvarende spørsmål innenfor norsk rett.⁸¹ Imidlertid er det ikke problematisk å bygge på de reelle hensyn man kan utlede av nasjonale rettskilder. En viktig tolkningsfaktor i forhold til spørsmålet vil da også være de reelle hensyn som gjør seg gjeldende i dette tilfellet.

En naturlig, språklig forståelse av at noen handler under andres autoritet eller kontroll innebærer etter min mening at det foreligger så vel et over-/underordningsforhold som en instruksjonsmyndighet fra den overordnede side. I forholdet mellom en arbeidsgiver og en arbeidstaker foreligger det tradisjonelt elementer av både over-/underordning og av instruksjonsmyndighet for arbeidsgiveren. Ordlyden taler derfor i utgangspunktet for at et forhold mellom en arbeidsgiver og en arbeidstaker generelt skal være omfattet av art. 14 nr. 2.

En slik vurdering må imidlertid også til en viss grad være avhengig av den fasthet og kontinuitet forholdet bærer preg av. For eksempel kan det være grunn til å trekke et skille mellom ordinære arbeidstakere og innleide konsulenter hvis funksjon grenser opp mot å være selvstendig oppdragstakere. På bakgrunn av denne drøftelsens forutsetninger som går ut på at arbeidstakeren, i en lovlig arbeidsavtale, er bundet til full stilling, finner jeg det ikke urimelig å gå ut fra at arbeidstakeren handler under bulletin board operatørens kontroll eller autoritet i e-handelsdirektivets forstand.

Reelle hensyn kan likevel sette spørsmålstegn ved hvorvidt arbeidstakeren skal sies å handle under bulletin board operatørens autoritet eller kontroll hvis han går utenfor det som er rimelig å regne med etter arten av virksomheten eller saksområdet og karakteren av arbeidet. Det kan virke støtende dersom man kommer til at arbeidsgiveren skal risikere ansvar på grunn av arbeidstakerens handlinger i de tilfeller der sistnevnte foretar ulovlige eller krenkende handlinger som er helt løsrevet fra oppgavene i stillingsinstruksen, og som arbeidsgiveren derfor vanskelig kan sikre seg mot. Dette må gjelde selv om de krenkende eller ulovlige handlingene er foretatt i arbeidstiden. Utgangspunktet for denne drøftelsen er at de handlingene arbeidstakeren

⁸⁰ Se oppgavens punkt 1.9

⁸¹ I forhold til arbeidsgiveransvaret i skl. §2-1 finnes det en omfattende rettspraksis. Her behandles blant annet spørsmålet om arbeidsgiveren er ansvarsfri fordi de krav skadelidte med rimelighet kan stille til virksomheten eller tjenesten, er tilsidesatt (eks. Tirrannadommen, Rt. 1970 s. 1154), eller fordi en arbeidstaker går utenfor det som er rimelig å regne med etter arten av virksomheten eller saksområdet og karakteren av arbeidet eller vervet (eks. Læreguttdommen, Rt. 1959 s. 849).

utfører ved hjelp av bulletin board operatørens tjenester ikke har noen sammenheng med de oppgaver som fremgår av stillingsinstruksen. I vurderingen av hvorvidt arbeidstakeren har gått utenfor det som er rimelig å regne med etter arten av virksomheten og karakteren av arbeidet, må det i hvert tilfelle vurderes hvor stort avvik det er fra de i stillingsinstruksen beskrevne oppgaver og den ulovlige eller krenkende handling.

De handlinger jeg her drøfter er utført ved at ulovlig aktivitet eller informasjon er videreformidlet ved hjelp av bulletin board operatørens teknologiske fasiliteter. Det er i denne sammenheng nærliggende å si at en arbeidstaker som er satt til å lede en diskusjonsgruppe e.l. på Internett, ved spredning av privat, ulovlig materiale utfører dette mens han handler under bulletin board operatørens autoritet eller kontroll. På den annen side lar det seg vanskeligere hevde at et av bulletin board operatørens kantinepersonale, som har skaffet seg tilgang til tjenestene gjennom en lånt brukerstasjon, handler under bulletin board operatørens autoritet eller kontroll dersom han sprer privat, ulovlig materiale. Man må anta at grensen for hva som er rimelig å forvente etter arten og karakteren av arbeidet, avhengig av de konkrete omstendigheter, ligger et sted mellom de to tilfellene jeg har skissert ovenfor.

I utgangspunktet til denne drøftelsen fremgår det at de ulovlige eller krenkende ytringer som arbeidstakeren fremsetter ikke har noen sammenheng med de oppgaver arbeidstakeren er satt til å gjøre. På bakgrunn av denne sparsomme informasjonen er det vanskelig å si om arbeidstakeren i det konkrete tilfelle har gått utenfor det som er rimelig å regne med etter arten av virksomheten eller saksområdet og karakteren av arbeidet. Selv om det generelt skal mye til for å tolke ordlyden i art. 14 nr. 2 innskrenkende i en sak som dette, forutsetter jeg likevel at arbeidstakeren har gått utenfor det som er rimelig å regne med sett på bakgrunn av den virksomheten han er satt til å drive for bulletin board operatøren. Resultatet av dette er at art. 14 nr. 2 ikke kommer til anvendelse i forhold til den virksomheten bulletin board operatøren driver i dette tilfellet. Følgelig skulle virksomheten falle innunder e-handelsdirektivets hovedregel om ansvarfrihet i art. 14 nr. 1.

Konklusjonen er at vilkårene for ansvarsfrihet i art. 14 er oppfylt dersom en bulletin board operatør videreformidler en av sine arbeidstakers ulovlige eller krenkende ytringer når disse er fremsatt i arbeidstiden, men ikke har noen sammenheng med de oppgaver arbeidstakeren er satt til å gjøre, og arbeidstakeren er tjenestemottaker for arbeidsgiverens bulletin board-tjenester.⁸²

⁸² Etter gjennomføringen av de regler som e-handelsdirektivet oppstiller om ansvarsfrihet i forhold til art. 14 nr. 1, jfr. nr. 2 i norsk rett, kan det reises spørsmål hvorvidt norske reg-

2.9 Spørsmål om ansvarsfrihet for de andre typer digitale mellomledd som er beskrevet i punkt 1.6

2.9.1 Er virksomheten som det i punkt 1.6.7 er beskrevet at en operatør av en søkemotor driver omfattet av anvendelsesområdet for art. 12-14 i e-handelsdirektivet?

Den virksomhet en søkemotor driver består, som det fremgår av forklaringen foran i punkt 1.6.7, i å generere en liste med internettadresser som er relevante sett på bakgrunn av søkte ord eller uttrykk. Virksomheten omfatter ikke tilveieskaffelsen av aksess til Internett eller tilveieskaffelse et kommunikasjonsnettverk for mottageren av tjenestene. Virksomheten faller derfor ikke innunder e-handelsdirektivets art. 12, som omfatter de aktørene som skaffer aksess til Internett, eller som stiller til disposisjon et nettverk for oversendelse av informasjon. Videre er det klart at søkemotorvirksomheten verken utgjør noen automatisk, mellomliggende og midlertidig mellomlagring av informasjon, slik dette er beskrevet i art. 13, eller noen lagring av informasjon, slik dette er beskrevet i art. 14.

På bakgrunn av søkemotortjenestenes egenart er det ikke tvilsomt at den ikke er omfattet av ansvarsreglene i e-handelsdirektivets art. 12-14.

Konklusjonen er at den virksomheten som det i punkt 1.6.7 er beskrevet at en operatør av en søkemotor driver ikke er omfattet av anvendelsesområdet for art. 12-14 i e-handelsdirektivet.

ler om arbeidsgiveransvar etter skl. §2-1 fullt ut kan praktiseres som tidligere. I denne sammenheng er det verdt å merke seg at e-handelsdirektivets formulering «acting under the authority or the control of the provider» rekker lenger enn til de tilfeller som faller innunder begrepet «Arbeidsgiver» i skl. §2-1. Hovedregelen om ansvarsfrihet i art. 14 nr. 1 begrenses derfor i den grad at forholdet til et arbeidsgiveransvar etter skl. §2-1 neppe vil skape konflikter på dette området. Den innskrenkende fortolkning jeg foretok av ordlyden i art. 14 nr. 2 utvider anvendelsesområdet for hovedregelen om ansvarsfrihet. Dersom en slik innskrenkende tolkning strekkes langt nok kan det reises spørsmål om det da oppstår konflikt i forhold til ansvarsregelen i skl. §2-1. Spørsmålet må trolig besvares benektende. Skl. §2-1 opererer med en tilsvarende begrensning av ansvar for de tilfeller der arbeidstakeren går utenfor det som er rimelig å regne med etter arten av virksomheten eller saksområdet og karakteren av arbeidet. På akkurat dette området kan det, etter min mening, overlates til rettspraksis å trekke opp en klar grense mellom reglene om ansvarsfrihet i e-handelsdirektivets art. 14 og arbeidsgiveransvaret i skl. §2-1.

2.9.2 Er virksomheten som i punkt 1.6.8 er beskrevet som portalvirksomhet omfattet av anvendelsesområdet for art. 12-14 i e-handelsdirektivet?

Den tjenesten som en operatør av portaltjenester leverer består, som det fremgår av punkt 1.6.8, av en samling linker til internettadresser i et virtuelt samlingspunkt (i praksis en nettside), som har til formål å tilgjengeliggjøre og segmentere informasjon fra en spesiell bransje eller for en spesiell gruppe nettsted. Portalvirksomheten omfatter verken tilveieskaffelse av aksess til Internett eller tilveieskaffelsen av et nettverk for kommunikasjon med Internett for den som mottar tjenestene. Virksomheten faller derfor ikke innunder e-handelsdirektivets art. 12 som regulerer forholdet til aksessleverandører og nettverksoperatører. Portalvirksomheten omfatter verken lagring av informasjon i sanntid eller på mer permanent basis. Den omfatter ikke automatisk, mellomliggende og midlertidig lagring av informasjon fra fjerntliggende servere på en lokal server. Virksomheten faller derfor heller ikke innunder art. 13 eller 14 som regulerer forholdet til operatører som driver henholdsvis caching og hosting. Resultatet av dette er at portalvirksomheten ikke er omfattet av bestemmelsene i e-handelsdirektivets art. 12-14.

Konklusjonen er at den virksomheten som i punkt 1.6.8 er beskrevet som portalvirksomhet ikke er omfattet av anvendelsesområdet for art. 12-14 i e-handelsdirektivet.

3. RETTSPOLITISKE VURDERINGER PÅ BAKGRUNN AV ANSVARSREGIMET I E- HANDELSDIREKTIVETS ART. 12-14

3.1 Innledning

I denne delen av avhandlingen skal jeg drøfte noen av de overordnede hensyn som begrunner reguleringene i e-handelsdirektivets art. 12-14. Samtidig er det min hensikt å peke på en rekke aspekter ved et ansvarsregime for digitale mellomledd som reguleringene i direktivet, etter min mening, ikke vier den nødvendige oppmerksomhet. Eksempel på to slike aspekter er hvorvidt det bør stilles formkrav til en melding om at mellomleddets server inneholder ulovlig eller krenkende informasjon, og hvorvidt det bør opereres med en såkalt notice-, and take-down prosedyre i forhold til de mellomledd som får melding om at deres server angivelig inneholder ulovlig materiale. Til slutt skal jeg si noen ord om de mellommannsvirksomhetene som jeg har nevnt i oppgaven, nemlig søkemotorvirksomhet og portalvirksomhet, men som ikke er omfattet av bestemmelsene 12-14 i e-handelsdirektivet.

3.2 I hvilken grad bør digitale mellomledd risikere ansvar for formidling av informasjon sett på bakgrunn av samfunnsinteresser som åpne kommunikasjonskanaler og ytringsfrihet?

3.2.1 Innledning⁸³

Ved første blick kan det synes rimelig at utelukkende den person som skaffer innhold til det digitale miljøet, og som på denne måten har direkte innflytelse og kontroll over det aktuelle materialet, skal risikere ansvar for eventuelt krenkende eller ulovlige forhold. Innføringen av et ansvarsregime for digitale mellomledd innebærer i denne sammenheng en fordeling av risiko mellom de involverte partene. Dersom vilkårene for å komme innunder hovedregelen om ansvarsfrihet er strenge for eksempel overfor en host service provider, risikerer denne i større grad å måtte bære de økonomiske konsekvensene av at tjenestemottagerne lagrer opphavsrettslig krenkende materiale på hans servere. Dersom vilkårene for å komme innunder ansvarsfriheten er lempelige må rettighetshaverne til det opphavsrettsbeskyttede materialet i større grad bære risikoen.

Hovedreglen i e-handelsdirektivet er at digitale mellomledd skal kunne drive sin virksomhet uten risiko for ansvar så lenge vilkårene i art. 12-14 er oppfylt. Imidlertid kan mellomleddene risikere ansvar dersom deres virksomhet faller utenfor hovedreglen.

Det spørsmål jeg skal drøfte i dette punktet er i hvilken grad plassering av ansvar hos en aktør som videreformidler informasjon reiser betenkeligheter ut fra en bredest mulig vurdering av de reelle hensyn som gjør seg gjeldene.

3.2.2 «Den dype lomme»

Det kan hevdes at en ansvars plassering hos de digitale mellomledd kun er begrunnet i at mulighetene til å få dekning for sitt krav er større. Grunnen til de større dekningsmulighetene ved plassering av ansvar hos mellomleddene, er at

⁸³ Onsdag 4. april 2001 var ett av hovedoppslagene i Nettavisen at Tele2 var blitt bøtlagt av Økokrim for formidling av barnepornografi. Forelegget på 350.000 kroner hadde Tele2 fått fordi det gjennom lengre tid har vært mulig for kundene å laste ned barneporno som noen av disse har lagret på Tele2s server. Det er første gang et slikt ansvar har blitt pålagt en digital aktør i Norge. Tele2 har nektet å vedta forelegget, og dermed ender saken trolig i retten. Økokrims plassering av ansvar på det digitale mellomleddet Tele2 er ikke uten betenkeligheter, sett på bakgrunn av samfunnets interesse i å sikre ytringsfriheten samt å beholde Internett som en åpen kommunikasjonskanal. Det er betenkeligheter som knytter seg til denne typen ansvarliggjøring som er utgangspunktet for denne drøftelsen.

disse jevnt over er i besittelse av større økonomiske ressurser enn f.eks. de aktørene som mottar deres tjenester. Sistnevnte kan i mange tilfeller være privatpersoner som ikke har de økonomiske forutsetninger for å dekke tap av noen størrelse. Selv om en ansvars plassering hos de digitale mellomledd i et flertall av tilfeller fører til at skadelidte får kompensasjon for påførte skader, må det imidlertid være klart at hensynet til betalingsdyktighet ikke er tilstrekkelig begrunnelse for en slik løsning. I denne sammenheng henviser jeg til John Peter Salts diskusjon av de hensyn en ansvars plassering skal ivareta. Salt⁸⁴ fremholder at dersom domstolens ønske først å fremst er å kompensere skadelidte økonomisk, så vil en plassering av ansvaret hos aktøren med den dypeste lomme være hensiktsmessig. Dersom ønsket imidlertid er å plassere ansvaret hos den part som har lettest for å minimere risikoen, vil dette, ihvertfall teoretisk, ikke alltid være den part som har den dypeste lommen. I forhold til teknisk videreformidling av informasjon ser vi ofte at digitale mellomledd er den aktør som lettest kan minimere risikoen ved formidling av informasjon, f.eks. ved å innføre teknologiske kontrollordninger. Noen konklusjon er det derfor vanskelig å trekke på bakgrunn av disse argumentene. Imidlertid kan man fastholde en ting: Et ansvarsregime som i for stor grad gir digitale mellomledd et påskudd til å sensurere informasjon er ikke ubetinget positivt i forhold til ønsket om å sikre fri informasjonsflyt samt en reell ytringsfrihet på Internett. I punktet under skal jeg komme nærmere inn på diskusjonen rundt hvorvidt muligheten til å kontrollere informasjon som videreformidles bør være et argument for plassering av ansvar hos digitale mellomledd.

3.2.3 Muligheten for teknologisk kontroll av informasjon.

Begrensningene, praktisk og teknologisk, når det gjelder muligheten til å kontrollere informasjon som digitale mellomledd har på sine servere, eller oversender gjennom sitt nettverk, er et moment som i juridisk litteratur⁸⁵ ofte blir diskutert i tilknytning til spørsmålet om digitale mellomledds ansvar. Spørsmålet jeg skal ta stilling til i denne drøftelsen er om teknologiske kontrollordninger for å hindre at krenkende eller ulovlig materiale blir gjort tilgjengelig og spredt via digitale mellomledds teknologiske fasiliteter, er et passende kriterium for å avgjøre hvilken ansvarsstandard man skal operere med i forhold til digitale mellomledd. I denne sammenheng må det både tas stilling til om teknologiske kontrollordninger gir mellomleddene et effektivt redskap for å kontrollere videreformidlingen av krenkende eller ulovlig materiale, og om det, dersom de teknologiske kontrollfunksjonene viser seg effek-

⁸⁴ Se Salt (1997 s. 312 flg.).

⁸⁵ Se Julia-Barceló (1999a s 16-24)

tive, er ønskelig at de digitale mellomleddene skal utøve sensur av Internett og på denne måten kontrollere hvilken informasjon som skal være tilgjengelig for allmennheten.

Det er utvilsomt at den mulighet som mellomleddene, fra et teknologisk synspunkt, har til å overvåke og kontrollere den informasjon de har på sine servere gir dem et godt utgangspunkt i forhold til å minimere risikoen ved videreformidling av informasjon. I følge argumentasjonen i punktet ovenfor er dette et moment som taler for at ansvar allokeres til de digitale mellomleddene. En rekke betenkeligheter reiser seg imidlertid i forhold til å la dette være et avgjørende kriterium for hvor ansvaret skal plasseres. En betenkelighet er at det, i følge personer som har teknologisk kompetanse, for både nettverksoperatører, aksessleverandører og host service providere, vil medføre en fysisk umulighet å overvåke eller kontrollere all informasjonen som videreformidles eller lagres. Dette skyldes både den enorme informasjonstilgangen i seg selv, og det faktum at det tilføyes nye nettsteder daglig. I tillegg til dette er de fleste allerede eksisterende nettsteder under konstant endring og oppdatering.

En annen betenkelighet er, under forutsetning av at en effektiv teknologisk kontroll eller overvåkning av informasjon lar seg gjennomføre, at de mellomledd som har teknisk mulighet til å overvåke informasjon blir ansvarlig for ulovlig eller krenkende materiale dersom de ikke faktisk gjennomfører overvåkingen. Motsetningsvis vil, dersom teknologisk overvåkning ikke lot seg gjennomføre, de samme mellomleddene ikke risikere ansvar. Innvendingen mot dette er at ansvarsstandarden for digitale mellomledd blir gjort avhengig av hvorvidt teknologiske kontrollordninger faktisk er implementert. En ansvarsstandard som er avhengig av teknologiske kontrollordninger har flere svakheter. For det første kan den medføre en trussel mot ytringsfriheten ved at de implementerte kontrollordningene uberettiget stenger tilgangen til lovlig informasjon på Internett. For det annet kan det særlig reises spørsmål om teknologien er egnet til å løse de vanskelige spørsmål som knytter seg til hvorvidt f.eks. opphavsrettslige, eller personvernrettslige regler er krenket. Disse spørsmålene er i seg selv så vanskelige at de byr på problemer for erfarne jurister. For det tredje kan implementasjonen av teknologiske kontroll-, og overvåkningsordninger skape problemer dersom lover og regler fra forskjellige land er involvert. F.eks. vil det by på problemer å implementere en teknologi som tar høyde for at enkelte juridiske spørsmål løses på forskjellig måte i forskjellige land. F.eks. kan ytringer som blir ansett for ærekrenkende i ett land bli ansett for å ha vern av ytringsfriheten i et annet. Dette problemet blir særlig aktualisert når man tar i betraktning Internetts grenseoverskridende preg.

Kriteriet som går ut på teknologisk mulighet til å kontrollere informasjon virker derfor ikke velegnet som eneste ansvarskriterium. Begrunnelsen er de

betenkeligheter gjennomføringen av et teknologiregime reiser i forhold til ytringsfriheten, og da særlig sett på bakgrunn av den begrensede nøyaktigheten teknologien viser når det gjelder å skille lovlig og ulovlig informasjon fra hverandre. På tross av disse argumentene bør man ikke se bort fra teknologiens rolle i forhold til all kontroll og overvåkning av Internett. Blant annet kan teknologiske filter være velegnet for å beskytte mindreårige mot skadelig informasjon.

3.2.4 Den krenkedes interesser

I mange tilfeller kan den krenkedes interesser tale for at digitale mellomledd bør gjøres ansvarlig for sin videreformidling av ulovlig eller krenkende materiale. Ofte kan den som står for den direkte krenkelsen, f.eks. ved at han ærekrenker noen grovt i sin bruk av en samtaletjeneste på Internett, være hjemmehørende i et annet land enn den krenkede. I disse tilfellene kan skadelidtes eneste mulighet for å få saken opp i sin hjemmejurisdiksjon være å gå til sak mot et digitalt mellomledd. Søksmål i sin hjemmejurisdiksjon er som ofte lønnsomt både ut fra et økonomisk og et tidsmessig perspektiv. Dessuten vil eventuelle rettsavgjørelser fra en domstol i en utenlandsk jurisdiksjon være vanskeligere å gjennomføre i forhold til skadevolderen.

Et annet aspekt som taler for at digitale mellomledd skal risikere et ansvar for videreformidling av informasjon er at det fremdeles er teknologisk mulig for en bruker å operere anonymt gjennom mellomleddets teknologiske fasiliteter, for eksempel ved at han får tilgang til videreformidlingstjenestene gjennom en offentlig tilgjengelig brukermaskin. I denne sammenheng taler usikkerheten som knytter seg til sporing av skadevolderen for at de lettere identifiserbare digitale mellomledd også bærer et ansvar.

3.2.5 Medvirkningsbetraktninger

Ut fra rene medvirkningsbetraktninger har det blant annet fra aktører som disponerer over opphavsrettigheter blitt hevdet at de digitale mellomledd må gjøres ansvarlig på lik linje med den som står på for de direkte krenkelsene. Ansvar for medvirkende opphavsrettskrenkelse betyr at mellomleddet anses for å ha ytet en selvstendig innsats i fremstillingen av ulovlige kopier av rettighetsbeskyttet materiale. Det kan også hevdes at medvirkning må anses å foreligge selv om mellomleddet ikke har noen kunnskap om den ulovlige eksemplarfremstillingen. Rent praktisk kan disse påstandene begrunnes med at det er mellomleddet som sørger for den teknologiske infrastruktur som er nødvendig for å gjennomføre den ulovlige fremstillingen. En annen begrun-

nelse kan være at mellomleddenes virksomhet gjør opphavsrettighetskrenkelser svært enkelt for et stort publikum.

En rekke betenkeligheter knytter seg til den argumentasjonen som her anføres. Et slikt generelt medvirkningsansvar ville skape store vanskeligheter for de digitale mellomledd. For det første måtte mye mer av de i mange tilfeller begrensede ressursene mellomleddene disponerer gå til å kontrollere den informasjon som blir videreformidlet gjennom deres teknologiske fasiliteter. Særlig på grunnlag av det enorme omfanget av informasjon ville kontrolltiltakene legge en stor bær på mellomleddene. En konsekvens av dette vil være at ytringsfriheten og hensynet til effektiv informasjonsflyt blir truet. Den naturlige reaksjon fra mellomleddenes side vil jo være å sørge for streng overvåking og sensur, eventuelt implementering av teknologiske filter for siling av informasjon.

Resultatet av den argumentasjonen jeg har presentert ovenfor, er at rene medvirkningsbetraktninger ikke danner et tilstrekkelig godt utgangspunkt i alle tilfeller der man søker å begrunne en plassering av ansvar hos digitale mellomledd.

3.2.6 Aktsomhetsbetraktninger

Under forutsetning at det digitale mellomleddet er noe å bebreide for at en skade oppstår, er et tungtveiende argument for å illegge mellomleddet ansvar å finne i aktsomhetsbetraktninger. Dersom informasjonsformidleren vitende eller uaktsomt bryter mot en aktsomhetsplikt han har i forhold til skadelidte er det heller ikke urimelig at ansvar pålegges. Løsningen innebærer for det første at det er den aktør som er noe å bebreide som risikerer ansvar, men for det annet at ansvaret legges på den aktør som billigst og ved de enkleste midler kan minske risikoen for skade. En slik ansvarsfordeling er fordelaktig av to grunner. For det første er det den part som ikke har utvist den nødvendige aktsomhet som får belastningen med et erstatningsoppgjør. For det annet gis de involverte aktører et incitament til å forebygge fremtidige krenkelser.⁸⁶ Som vi har sett bygger enkelte av reguleringene i e-handelsdirektivet på en slik prevensjonstanke. I direktivets art. 14, nr. 1, litra (b) oppstilles det eksempelvis en plikt for det digitale mellomleddet til å fjerne det krenkende eller ulovlige innholdet dersom det foreligger faktisk kunnskap om det, eller dersom det er klar over fakta eller omstendigheter som gjør den ulovlige aktiviteten synlig.

⁸⁶ Dette gjelder under enhver omstendighet så lenge kostnadene ved et eventuelt erstatningsansvar er høyere enn kostnadene med de tiltak som må iverksettes for å motvirke skadetilfeller, se Salt (1997 s. 312).

3.2.7 Ytringsfriheten

Et argument som kan tale mot et strengt ansvar for videreformidling av informasjon legges på digitale mellomledd er hensynet til ytringsfriheten. I et særskilt vedlegg til Ytringsfrihetskommisjonens rapport⁸⁷ skriver Kyrre Eggen om videreformidlerens rolle og hvorvidt et ansvar for formidleren krenker det internasjonale vern om ytringsfrihet. Han fremholder særlig to årsaker til at det er betenkelig å holde den tekniske videreformidleren ansvarlig: Den første er den «chilling effect» et medvirkningsansvar vil få for ytringsfriheten og den andre er det betenkelige med at formidleren blir stående mellom sine kontraktsmessige forpliktelser til å videreformidle ytringen og risikoen for å bli holdt medvirkningsansvarlig dersom ytringen skulle vise seg å være ulovlig⁸⁸.

I relasjon til det første punktet er det på det rene at et strengt ansvarsregime kan medføre at ytringsfriheten blir truet som følge av at digitale mellomledd enten gjennomfører en form for redaksjonell kontroll, eller implementerer forskjellige teknologiske ordninger for å sensurere det materiale som skaffes til veie av tjenestemottageren. Ofte vil vurderingen av en ytrings lovlighet innebære at det må tas stilling til vanskelige juridiske spørsmål. Normalt vil den aktør som opererer som videreformidler av informasjon ikke besitte den kompetanse som er nødvendig for å avgjøre disse vanskelige spørsmålene. Dertil vil han sjelden ha noen selvstendig interesse i å beskytte ytringsfriheten. Det er derfor en betydelig risiko for at mellomleddet istedenfor å risikere ansvar for videreformidling av ulovlige eller krenkende ytringer sikrer seg ved å stanse tilgangen til det omstridte materialet.

I relasjon til det andre punktet er det klart at et strengt ansvar i mange tilfeller vil tvinge digitale mellomledd til å foreta en vurdering av den videreformidlede ytringens lovlighet før han bestemmer seg for om formidlingen skal stanses. Et slikt ansvar fremtvinger med andre ord en viss grad av privat sensur fra mellomleddets side. Mens en aktør som formidler informasjon gjennom en avis eller gjennom fjernsyn selv kan velge om han ønsker å formidle ytringen, er det digitale mellomledd ofte kontraktsmessig forpliktet til å gjøre informasjonen tilgjengelig. Dersom mellomleddet stanser formidlingen av slikt materiale risikerer han å bli saksøkt av sin tjenestemottager. På den annen side risikerer han medvirkningsansvar dersom ytringen viser seg å være

⁸⁷ Se NOU 1999:27.

⁸⁸ Et eksempel på at begge disse betenkelighetene ble aktualisert så vi i månedsskiftet februar/mars 2001 da sol.no valgte å sensurere en nettside som de hostet for et medlem av den nynazistiske grupperingen «Boot-boys». Siden inneholdt ikke påviselig ulovlig materiale. Likevel valgte sol.no å stanse videreformidlingen av informasjonen for å minimere risikoen for rettslig forfølgelse.

ulovlig eller krenkende. Som en følge av dette risikerer man at den totale tilgangen på informasjon i samfunnet blir mindre.

I NOU 1999:26 drøfter det såkalte Konvergensutvalget videreformidlerens ansvar på Internett. Utvalget konkluderer med at «hensynet til ytringsfriheten og størst mulig bredde av ytringer på Internett taler for at man bør vise tilbakeholdenhet med å pålegge aktører som utelukkende fungerer som distributører ansvar for kontroll med innholdet som blir formidlet». Videre er utvalget «på prinsipielt grunnlag skeptisk til ordninger som innebærer at mellommenn (teleselskap, nettverter mv.) pålegges ansvar for selv å vurdere lovligheten av ytringer som tilgjengeliggjøres på Internett.»⁸⁹ Utvalgets konklusjon er begrunnet i ønsket om å unngå privat sensur av ytringer på Internett.

Ved vurderingen av hvilken type ansvarsregler som skal gjelde i forhold til digitale mellomledd bør det av de grunner jeg har nevnt ovenfor vurderes nøye hva som er det minste ondet av å hindre ytringsfrihet og informasjonstilgang contra å operere med et noe lempeligere ansvar.

3.2.8 Økonomisk vekst

Den økonomiske vekst i informasjonsbransjen er blant annet betinget av at aktørene i næringen gis gode rammevilkår for sin drift. Jo strengere ansvar mellomleddene risikerer, jo større er faren for at en tilfredsstillende økonomisk vekst hindres. Dette skyldes både at aktørene som følge av et strengt ansvarsregime, må bruke større ressurser på å forebygge at et ansvar skal inntre, samt at ansvar i praksis trolig vil bli pålagt i flere tilfeller, noe som medfører et økonomisk tap for aktørene i bransjen. Den økonomiske veksten er på samme tid avhengig av at de digitale aktørene har tillit markedet. Et ansvarsregime som er for lempelig, kan i denne sammenheng gjøre at tilliten til de digitale aktørene svekkes. En svekket tillit kan f.eks. skyldes at personer hvis rettigheter er krenket ikke når frem med sine krav mot digitale mellomledd som åpenbart spekulerer i å videreformidle ulovlig informasjon. Man kan derfor vanskelig se seg tjent med et ansvarsregime som ikke legger de nødvendige rammene rundt internettaktørenes virke, og som på denne måten heller ikke legger gunstige føringer på bransjens utvikling.

Et ansvarsregime for digitale mellomledd hjemmehørende i Europa etablerer videre rammevilkår for hvilken konkurranseevne disse skal ha i global sammenheng. Et meget strengt ansvarsregime for digitale mellomledd hjemmehørende i EU/EØS-området vil trolig ha negative konsekvenser for deres konkurranseevne i forhold til aktører som er etablert i det amerikanske markedet. Dersom europeiske aktører skal gis noen reell mulighet til å ta igjen

⁸⁹ NOU 1999:26, side 151 flg.

det teknologiske og forretningsmessige forspranget som USA har, er det viktig at de ansvarsregimer for digitale mellomledd som gjennomføres i de enkelte nasjonalstaters rettssystem gir gode rammevilkår.

Videre vil et strengt ansvarsregime kunne virke dempende på investeringer i IT-bransjen. Dette gjelder særlig investeringer fra selskap eller personer som er hjemmehørende i USA, der man generelt setter ytringsfriheten høyt, men også investeringer fra aktører i det europeiske markedet som pga. for strenge reguleringer får næring til eventuell skepsis til IT-bransjen.

3.2.9 Avveining og konklusjon

Det er ikke gitt at noen av de ovenfor nevnte interessene skal være mer tungtveiende enn andre. Mye taler imidlertid for at man skal være forsiktig med å pålegge digitale mellomledd et for strengt ansvar i forhold til den rolle de spiller som videreformidlere av informasjon. Dette kan særlig begrunnes med hensynet til ytringsfriheten og hensynet til informasjonsflyt over Internett.

Dersom informasjonsformidleren er noe å bebreide for at ulovlig eller krenkende materiale gjøres tilgjengelig gjennom hans teknologiske fasiliteter, er et ansvar imidlertid lettere å begrunne. Det subjektive elementet kan i slike tilfeller veie tyngre enn de betenkelighetene som blant annet forholdet til ytringsfriheten og åpne kommunikasjonskanaler skaper.

Argumentasjonen ovenfor medfører heller ikke at man skal se helt bort fra teknologiens rolle i forhold til vurdering av et ansvar. Som nevnt ovenfor kan det ikke være tvil om at en teknologisk filtreringsmodell kan vise seg svært nyttig i forhold til sluttbrukerne av Internett, f. eks. for å beskytte barn mot skadelig informasjon.

3.3 Horisontal eller vertikal regulering av ansvarsfrihet for digitale mellomledd?

I dette punktet skal jeg drøfte hensiktsmessigheten av e-handelsdirektivets innføring av en horisontal regulering av ansvarsfrihet fremfor å oppstille regler som pålegger ansvar avhengig av hvilket underliggende lovverk som er krenket. Nok en gang ønsker jeg presisere at en horisontal ansvarsregulering innebærer at det opereres med én ansvarsstandard uavhengig av hvilken type materiell lov som er brutt.

En fordel med å oppstille regler om ansvarsfrihet avhengig av hvilket underliggende rettsområde som er krenket er at det derved blir mulig for lovgiver å nyanseere ansvaret for krenkelse av bestemte rettsområder. En slik nyan-

sering kan være ønskelig fordi man tillegger hensynet til å unngå krenkelser større eller mindre vekt i forhold til hensynet til å sørge for konfidensialitet, effektivitet og ytringsfrihet ved oversendelse av informasjon på Internett. Det er i denne sammenheng klart at reglene om opphavsrett og personvern, som følge av den digitale revolusjonen, står i vesentlig større fare for å bli krenket, enn reglene om f.eks. ærekrenkelser. Når det gjelder for eksempel opphavsrettskrenkelser kan disse ikke umiddelbart sammenlignes med andre typer materiale som formidles over Internett. I motsetning til formidling av barnepornografi eller rasistiske ytringer vil det ikke være noe galt med innholdet i seg selv, men derimot de manglende underliggende avtaleforhold. Dette kan gi grunnlag for en noe annen vurdering av hva et digitalt mellomledd skal ha kunnskap om før han skal risikere et ansvar. Rettsteknisk kan derfor mye tale for at spørsmålet om ansvarsfrihet for mellomledd som videreformidler opphavsrettslig krenkende materiale reguleres i de enkelte lands opphavsrettslovgivning.⁹⁰

Mye tyder imidlertid på at et horisontalt ansvarsregime er den mest hensiktsmessige måten å regulere ansvarsfrihet på. Dersom Kommisjonen hadde etablert bestemmelser om ansvarsfrihet som var avhengige av hvilken materiell lovgivning som var krenket, ville dette effektivt medført at digitale mellomledd begynte å overvåke informasjonen som passerer gjennom deres teknologiske fasiliteter. En slik reaksjon ville være den naturlige konsekvens dersom man for visse typer informasjon risikerte et strengt ansvar, mens man for andre typer ikke risikerte ansvar overhodet. I denne sammenheng er det viktig å ta i betraktning at informasjonen som videreformidles gjennom mellomleddenes systemer, som f.eks. kabler, rutere og servere, er kun sekvenser bestående av nuller og ettall. Sekvensene har i seg selv ingen direkte tilknytning til den informasjon som videreformidles. For å kunne ha noen formening om hvilken type informasjon som faktisk passerer gjennom deres teknologiske fasiliteter måtte derfor mellomleddene i ethvert tilfelle gjøre om sekvensene til tekst, musikk eller bilder, og deretter overvåke hver del av dette. Innføringen av et slikt ansvarsregime ville derfor raskt true både funksjonaliteten i nettverket og konfidensialiteten og integriteten til den videreformidlede informasjonen.

Ved å operere med et horisontalt ansvarsregime har Kommisjonen valgt en annen løsning enn i den som er valgt i den amerikanske lovgivningen. I DMCA behandles digitale mellomledds ansvar for videreformidling av

⁹⁰ I norsk rett reguleres både sivil-, og strafferettslige sanksjoner for krenkelse av opphavsrettigheter i lov om opphavsrett til åndsverk av 12.05.1961 nr. 2 (åndsverksloven) kap. 7.

opphavsrettslig materiale i en separat lov. Ansvar for underliggende krenkelse av annen lovgivning behandles blant annet i CDA.⁹¹

Hvorvidt man velger en horisontal eller en vertikal regulering av ansvarsfrihet for digitale mellomledd må i første rekke bero på hvilken interesse de lovgivende myndighetene har i å sørge for et Internett som er funksjonelt og som tillater effektiv kommunikasjon. I e-handelsdirektivet kommer ønsket om å sikre effektivitet og funksjonalitet, foruten ved den horisontale ansvarsreguleringen, til uttrykk i art. 15, som oppstiller et forbud mot å innføre en generell undersøkelsesplikt i forhold til den informasjon som passerer gjennom, eller lagres på teknologiske fasiliteter. På bakgrunn av ønsket om å sikre fri flyt av informasjonssamfunnstjenester i det indre marked, for på denne måten blant annet å styrke konkurranseevnen i forhold til USA, samt å sikre forutberegnelighet for ulike markedsaktører, er det ikke oppsiktsvekkende at Kommisjonen har falt ned på en horisontal regulering. Løsningen er den som etter min mening balanserer de forskjellige hensyn som e-handelsdirektivet er ment å ivareta på best mulig måte.

3.4 E-handelsdirektivets risikofordeling mellom digitale mellomledd omfattet av art. 14, rettighetshaverne til den informasjon som lagres og mellomleddenes tjenestemottagere

3.4.1 Innledning

Min drøftelse av en rekke praktiske tilfeller opp mot regelen om ansvarsfrihet i art. 14 har vist at reguleringene i e-handelsdirektivet ikke gir alle de avklaringer som er nødvendige for å skape rettslig forutberegnelighet i forhold til digitale mellomledds virksomhet. I dette avsnittet skal jeg derfor undersøke hvorledes reguleringene i e-handelsdirektivet håndterer de spørsmål som dukker opp mht. plassering av risiko mellom digitale mellomledd som er omfattet av e-handelsdirektivets art. 14, rettighetshaverne til det materiale som lagres og den som har et rettslig grunnlag for å kreve informasjon tilgjengeliggjort gjennom mellomleddenes teknologiske fasiliteter.

Kravet til kunnskap om ulovlig eller krenkende innhold, jfr. art. 14 nr. 1, litra (a) er sentralt i denne sammenhengen. Jeg skal derfor særlig se på de

⁹¹ Communication Decency Act, 1996

spørsmål som kan oppstå når man på forskjellige grunnlag skal forsøke å avgjøre hvorvidt mellomleddet har kunnskap om ulovlig eller krenkende materiale i e-handelsdirektivets forstand. I forlengelsen av dette skal jeg drøfte hvorvidt e-handelsdirektivets reguleringer byr på hensiktsmessige løsninger. I denne sammenhengen skal jeg sammenlikne ansvarsregimet i direktivet med ansvarsregimet i den amerikanske DMCA. Spørsmål som oppstår her er hvorvidt også direktivet burde etablere underrettelses-, slettings- og tilbake-settingsregimer for informasjon eller aktivitet som etter påstand fra blant annet rettighetshavere til forskjellige typer digitalt materiale er ulovlig eller krenkende. I denne sammenhengen skal jeg vurdere hvorvidt det bør implementeres krav til innhold og form på en privat underrettelse som går ut på at digitale mellomledds servere inneholder informasjon eller aktivitet som er ulovlig eller krenkende. Dessuten skal jeg peke på hvorledes de krav man stiller til vilkåret om faktisk kunnskap som man velger å implementere kan virke kontra hensynet til effektiv konkurranse i internettmarkedet.

Til slutt skal jeg kort skissere en fremgangsmåte for å konstatere faktisk kunnskap hos digitale mellomledd der handleplikt til å fjerne ulovlig eller krenkende aktivitet eller informasjon gjøres avhengig av underrettelse fra en offentlig instans eller en domstol.

3.4.2 Kravet til kunnskap om ulovlig eller krenkende innhold i art. 14 nr. 1, litra (a) kontra fraværet av en generell undersøkelsesplikt i art. 15

E-handelsdirektivets art. 14 oppstiller som vilkår for ansvarsfrihet at et digitalt mellomledd som lagrer informasjon verken må ha faktisk eller konstruktiv kunnskap⁹² om ulovlige eller krenkende informasjon på deres servere. På den annen side etablerer art. 15 en regel om at medlemsstatene verken skal pålegge digitale mellomledd plikt til å overvåke informasjonen de videreformidler eller lagrer, eller til aktivt å søke fakta eller omstendigheter som kan tyde på at det foregår en ulovlig aktivitet.

Med utgangspunkt reguleringene i art. 15, samt den sparsomme veiledning e-handelsdirektivet gir i forhold til problemet, kan det stilles spørsmål om under hvilke omstendigheter digitale mellomledd, omfattet av art. 14, skal sies å ha fått den nødvendige kunnskap om den ulovlige eller krenkende informasjon de lagrer på sine servere. Spørsmålet må også ses på bakgrunn av e-handelsdirektivets preambel, punkt (48). Denne bestemmelsen legger til grunn at reguleringene i e-handelsdirektivet ikke skal påvirke medlemsstatenes mulighet til å pålegge mellomledd som lagrer informasjon for andre en

⁹² Med konstruktiv kunnskap mener jeg kunnskap om fakta eller omstendigheter som gjør den ulovlige aktivitet eller informasjon synlig, jfr. art. 14 nr. 1 litra (a).

aktsomhetsplikt som man rimeligvis kan forvente for å oppdage og motvirke forskjellige typer ulovlige aktiviteter.

Det er lett å argumentere for at en nettside med f.eks. en svært eksplisitt URL, som signaliserer at den inneholder opphavsrettslig krenkende eller annet straffbart materiale⁹³, gir grunnlag for å hevde at det digitale mellomledet har den nødvendige kunnskap i forhold til e-handelsdirektivets art. 14 nr. 1, litra (a). Digitale mellomledd kan imidlertid skjule seg bak art. 15s fravær av en generell undersøkelsesplikt i denne sammenhengen. Dersom spørsmålet skulle komme på spissen kan mellomledet i tråd med bestemmelsen i art. 15 fastholde at innholdet på serverne ikke har blitt overvåket, og at det ulovlige innholdet, herunder den eksplisitte URLen, ikke har blitt oppdaget. På bakgrunn av de enorme informasjonsmengdene som til enhver tid kan være lokalisert på mellomleddenes servere trenger en slik påstand ikke være usann.

I tilfeller der den som lagrer informasjon for andre driver en mindre og mer oversiktlig virksomhet, eventuelt der han er involvert i prosessen med å skaffe tilveie domenenavn for sin tjenestemottager, eller der han deltar i utviklingen av programapplikasjoner for tjenestemottageren⁹⁴, kan spørsmålet om kunnskap stille seg noe annerledes. Dette kan skyldes informasjonsmengden i seg selv, men også den grad av aktivitet mellomledet viser i forhold til det materiale som lagres.

På bakgrunn av punkt (48) i direktivets preambel kan det også, til tross for fraværet av en undersøkelsesplikt i art. 15, hevdes at digitale mellomledd i en konkret sak der det finnes et grunnlag for å anta at noe er galt, har en plikt til å forsikre seg om at tjenestemottagerne ikke bruker hans teknologiske fasiliteter til å spre ulovlig eller krenkende materiale.

Bestemmelsene om kunnskap i art. 14 nr. 1 litra (a) og fravær av en generell undersøkelsesplikt som følge av art. 15 må derfor tolkes med de reserver som ligger i det ovennevnte.

3.4.3 Kravet til kunnskap om ulovlig eller krenkende innhold i art. 14 nr. 1, litra (a) kontra implementeringen av teknologiske kontroll-, og utsilingsfunksjoner

Både i forhold til de aktører som ovenfor er beskrevet som host service providere og som bulletin board operatører kan det i større grad være grunnlag for å hevde at den nødvendige kunnskap etter art. 14 nr. 1, litra (a) foreligger dersom det faktisk er implementert teknologiske filter for å lokalisere eller

⁹³ Eksplisitte URLer som kan signalisere ulovlig innhold kan være f.eks. «gratishits.com», «piratspill.com» eller «barneporno.com»

⁹⁴ Typisk ASP-leverandører, jfr. fotnote 22.

stenge tilgangen til bestemte typer materiale. I forhold til kravet om faktisk kunnskap er det ikke betenkelig å operere med en slik forutsetning. Dersom de implementerte teknologiske løsninger faktisk har brakt oppmerksomheten til ulovlig eller krenkende materiale kan det ikke være tvilsomt at kravet om faktisk kunnskap er oppfylt. Denne argumentasjonen kan imidlertid fort vise seg å være overflødig ettersom tilgangen til den ulovlige informasjonen i de fleste tilfeller allerede vil være stanset i den teknologiske kontrollen og derfor ikke lenger representerer noen krenkelse. På den andre side vil det heller ikke eksistere faktisk kunnskap i e-handelsdirektivets forstand dersom ulovlig eller krenkende informasjon ikke er blitt oppdaget av utsilingsmekanismene.

I forhold til kravet om konstruktiv kunnskap reiser det seg flere betenkeligheter i forhold til implementeringen av teknologiske kontrollfunksjoner. Til dags dato har ingen implementerte teknologiske kontrollfunksjoner vist seg å virke effektivt i forhold til å sile ut materiale som er ulovlig eller krenkende. I overskuelig fremtid synes det nesten umulig å utvikle utsilingsmekanismer som verken inkluderer for mye eller for lite informasjon. Med andre ord vil enhver utsilingsfunksjon enten slippe for mye informasjon igjennom, eller filtrere ut for mye lovlig materiale.⁹⁵ Dersom det faktisk at mellomleddet har implementert en teknologisk utsilingsmekanisme blir brukt som et argument for at konstruktiv kunnskap i hht. art. 14 nr. 1, litra (a) skal sies å foreligge, vil det oppstå en situasjon som er urimelig sett fra mellomleddenes side. Fordi utsilingsmekanismene er såpass upålitelige som det fremgår av drøftelsen ovenfor, kan implementeringen føre til at mellomleddets risiko i forhold til et ansvar for videreformidling av informasjon øker betraktelig. En utsilingsmekanisme innebærer nemlig på den ene side at mellomleddene får silt ut noe ulovlig eller krenkende informasjon, mens det på den annen side blir lettere å si at de har kunnskap om fakta eller omstendigheter som gjør eventuelt ulovlige aktiviteter eller informasjonen synlig. Skulle en domstol komme til at kravet til konstruktiv kunnskap på dette grunnlaget er oppfylt, vil dette kunne oppfattes som urimelig. Dette er fordi mellomledd som faktisk gjør tiltak for å hindre eller motvirke at ulovlig aktivitet eller informasjon blir tilgjengeliggjort gjennom deres teknologiske fasiliteter, risikerer ansvar i større utstrekning enn mellomledd som overhodet ikke tar forhåndsregler i dette henseendet.

⁹⁵ Dette kan særlig reise problemer i forhold til ytringsfriheten.

3.4.4 Kravet til kunnskap om ulovlig eller krenkende innhold i art. 14 nr. 1, litra (a) kontra underrettelser fra tredjemann

Dersom vi forutsetter at digitale mellomledd ikke blir ansett for å ha kunnskap om ulovlig eller krenkende informasjon selv om de lagrer nettsider med eksplisitte URL-adresser, samt at teknologiske utslingsfunksjoner ikke blir implementert, blir spørsmålet hvorledes mellomleddene ellers skal få kunnskap om ulovlig eller krenkende innhold på deres servere. Et nærliggende alternativ er i denne sammenheng at mellomleddet blir underrettet av tredjemenn. For eksempel kan vi tenke oss at digitale mellomledd underrettes av store plateselskaper eller programvareprodusenter, som rutinemessig overvåker Internett om at deres servere inneholder materiale som krenker selskaperens opphavsrettigheter. E-handelsdirektivet gir ingen klare holdepunkter for å avgjøre hva en underrettelse må inneholde for å oppfylle de krav art. 14 nr. 1, litra (a) stiller til kunnskap.⁹⁶ Direktivet gir heller ingen retningslinjer mht. håndteringen av den risiko digitale mellomledd påtar seg dersom de stenger tilgangen til informasjon på sine servere og det senere viser seg at stengingen var uberettiget. I det følgende skal jeg forklare hvordan problemene har blitt forsøkt løst i DMCA og hvordan mangelen på slike reguleringer kan komme til å påvirke situasjonen til de digitale mellomledd som faller innunder anvendelsesområdet for e-handelsdirektivets art. 14.

I DMCA §512, litra (c), jfr. punkt (3) er det etablert en klar prosedyre for hvorledes digitale mellomledd skal underrettes om tilstedeværelsen av påstått krenkende eller ulovlig materiale. I praksis innebærer bestemmelsen at den rettighetshaver som påstår seg utsatt for en krenkende handling utarbeider og oversender en liste inneholdende spesifiserte elementer som gjør det mulig for mellomleddet å identifisere informasjonen. Konkret stilles det krav om at underrettelsen må skje skriftlig, til rette vedkommende og i signert form fra rette vedkommende. Dessuten må det opphavsrettslig beskyttede verk som påstås krenket identifiseres. Videre må det verk eller den handling som påstås å være krenkende og som tilgangen ønskes stengt til identifiseres og kontaktinformasjon må være vedlagt. Godtroerklæring mht. at vilkårene for lovlig bruk ikke er oppfylt må også vedlegges. Til slutt må det legges ved en erklæring om at den underrettende part er autorisert i forhold til rettighetshaver, samt at underretteren under trussel om rettslig forfølgelse garanterer at den avgitte informasjon er riktig. Dersom det digitale mellomleddet mottar en slik underrettelse, og deretter stenger tilgangen til det påstått krenkende materialet, vil det nyte godt av

⁹⁶ DMCA stiller i §512, litra (c), jfr. punkt (3) klare krav til hva en underrettelse om påstått krenkelse til et digitalt mellomledd skal inneholde for å oppfylle lovens krav.

hovedregelen om ansvarsfrihet uavhengig av om den videreformidlede aktivitet eller informasjon faktisk krenker opphavsmannens rettigheter.

Fremfor å etablere et underrettelses-, og stengingsregime i formelle former, slik det er gjort i DMCA, oppstiller e-handelsdirektivet kun en plikt for Kommisjonen til å revurdere behovet for et slikt regime innen tre år etter at direktivet er trådt i kraft, jfr. art. 21 nr. 2. Direktivet gir derfor ingen løsning på det risikospørsmål som oppstår for digitale mellomledd ved uberettiget stenging av tilgangen til angivelig krenkende eller ulovlig informasjon. Løsningen for digitale mellomledd som faller innunder anvendelsesområdet for e-handelsdirektivets art. 14 må derfor bli å bidra i utviklingen av, samt å stole på, utviklingen av selvreguleringsordninger i tråd med målsetningen i direktivets art. 16. Resultatet av denne mangelen på lovgivningsinitiativ kan likevel lett bli at digitale mellomledd som omfattes av art. 14, for å unngå risikoen for ansvar, stenger tilgangen til påstått krenkende eller ulovlig materiale etter mottagelse av alle typer underrettelser. En annen nærliggende løsning er at mellomleddene tar inn i de brukeravtaler som tjenestemottagerne må vedta før de kan benytte seg av hosting-, eller bulletin board-tjenestene at de skal ha rett til å stenge tilgangen til informasjon etter eget forgodtbefinnende. På denne måten vil ytringsfriheten over Internett i stor grad bli kontrollert av host service providere og bulletin board operatører som forståelig nok heller stenger tilgangen til en påstått krenkende eller ulovlig nettside fremfor å risikere ansvar for videreformidling av denne informasjonen.

På bakgrunn av det ovennevnte kan det virke som om det mest hensiktsmessige er å implementere en ordning med et underrettelses-, og stengingsregime i nasjonal rett. En slik ordning bør innebære at underrettelser fra både rettighetshavere og tredjemenn, som oppfyller visse krav til identifikasjon av partene samt til lokalisasjon av det påstått krenkende eller ulovlige materiale, blir ansett som lovlig grunn for aktører som er omfattet av art. 14 til å fjerne, eller stenge tilgangen til påstått krenkende eller ulovlig materiale. En slik ordning vil øke den rettslige forutberegneligheten for aktørene i markedet på samme tid som den ville bidra til å sikre ytringsfriheten.⁹⁷

⁹⁷ Implementering av et underrettelses-, og stengingsregime for digitale mellomledd som lagrer informasjon er under vurdering i Nærings-, og Handelsdepartementet. I et høringsnotat med høringsfrist 21. mai 2001, som gjelder innføring av direktiv om elektronisk handel i norsk rett, foreligger det to forslag til implementering av art. 14. I det ene forslaget oppstilles det i utkast til §12 nr. 3 en prosedyre der kunnskap om ulovlig innhold skal sies å foreligge som følge av et underrettelses-, og slettingsregime for private meldinger, ved kunnskap om forbud mot offentliggjøring fra en domstol eller en offentlig myndighet, eller etter at mellomleddet har fått «konkret kunnskap» om nærmere bestemte krenkelser. Der som kunnskap foreligger etter disse forslagene vil dette utløse en handleplikt for å oppnå

Et annet aspekt som reguleringene i e-handelsdirektivet ikke tar hensyn til dreier seg om det ansvar digitale mellomledd risikerer dersom det viser seg at stenging av tilgang til påstått krenkende eller ulovlig informasjon er uberettiget. Som jeg har beskrevet ovenfor kan et resultat av manglende ordninger for stenging av tilgang til påstått krenkende eller ulovlig informasjon være at lovlig materiale blir uberettiget fjernet. Dersom det digitale mellomleddet har påtatt seg en forpliktelse til å ha denne informasjonen tilgjengelig for tredjemann, risikerer det nå søksmål fra sin medkontrahent på grunn av den uberettigede stengingen. DMCA etablerer i §512, litra (g) en regel om ansvarsfrihet for en tjenesteyter som i god tro stenger tilgangen til materiale eller aktivitet som er påstått krenkende eller ulovlig, eller dersom han stenger tilgangen basert på fakta eller omstendigheter som gjør den krenkende eller ulovlige aktiviteten synlig. Dette gjelder uten hensyn til om materialet eller aktiviteten til sist blir ansett for å være ulovlig eller krenkende. Unntak fra hovedregelen om ansvarsfrihet fremgår imidlertid av bestemmelsens punkt (2). Her bestemmes det at tjenesteyteren må risikere ansvar i forhold til materiale som er lagret etter oppfordring fra en tjenestemottager dersom tilgangen til dette blir stengt, og tjenesteyteren ikke: (A) gjør rimelige tiltak for å varsle tjenestemottageren om at materialet fjernes, (B) gjenåpner tilgangen til det fjernede materialet ikke mindre enn 10, og ikke mer enn 14 virkedager etter at han har fått svarmelding fra tjenestemottageren. Dersom den person som innga den opprinnelige underrettelse om det påståtte krenkende eller ulovlige materialet først gir melding om at han har tatt rettslige skritt for stanse en ny tilgjengeliggjøring av tjenestemottagerens materiale, skal imidlertid mellomleddet nyte godt av ansvarsfriheten selv om materialet ikke gjøres tilgjengelig på nytt. Den ordningen som her er beskrevet innebærer et tilbakesettingsregime, som i sin konsekvens medfører en «safe harbour», eller en trygg havn, for digitale mellomledd. Resultatet av ordningen er nemlig at mellomleddet heller ikke risikerer ansvar i forhold til tjenestemottagere hvis materiale de har forpliktet seg til å holde tilgjengelig for tredjemann.

Etter e-handelsdirektivets system vil de mellomledd som faller inn under art. 14 risikere ansvar for stenging av tilgangen til materiale som mellomleddet har forpliktet seg til å holde tilgjengelig etter alminnelige nasjonale regler. E-handelsdirektivet oppstiller med andre ord ikke en trygg havn for mellomledd, slik DMCA gjør. Dette kan lede til dårlig rettslig forutberegnelighet for aktørene i markedet. Samtidig risikerer man at det oppstår avvikende lovgiv-

ansvarsfrihet etter bestemmelsen. I det andre forslaget legges det opp til at enten en rettslig avgjørelse eller et notifikasjonssystem skal være tilstrekkelig for å utløse en handleplikt for å oppnå ansvarsfrihet.

ning i medlemslandene i forhold hvorledes risikoen skal håndteres. En ytterligere konsekvens av de manglende reguleringene i e-handelsdirektivet er at aktørene kan utnytte den usikkerhet som eksisterer i forhold til risikoplassering ved spørsmål om stenging av tilgangen til informasjon. Dette kan skje ved at det inngis usanne og ondsinnede underrettelser om angivelig ulovlig eller krenkende informasjon på mellomleddenes servere. Med slike underrettelser kan useriøse aktører oppnå å sabotere konkurrerende virksomheter, eventuelt å hindre rettferdig konkurranse i markedet. DMCA legger i §512, litra (f) et ansvar på aktører som forsettlig inngir uriktige notifikasjoner om ulovlig eller krenkende innhold på andres servere. I e-handelsdirektivet er det ingen bestemmelser som berører problemet. Dette faktum, i tillegg til at e-handelsdirektivet ikke oppstiller klare prosedyrer for når faktisk kunnskap etter en privat underrettelse skal sies å foreligge, er ikke med på å motvirke at useriøse aktører misbruker den rettslige usikkerheten og på denne måten hindrer effektiv konkurranse.

3.4.5 Kravet til kunnskap i art. 14 nr. 1, litra (a) kontra underretning fra et ytre, uavhengig organ

Innføringen i nasjonal rett av et ansvarsregime som gjør ansvarsfriheten avhengig av et kunnskapskrav skaper, som det fremgår i drøftelsene i denne oppgaven, en rekke problemer i forhold til hvor risikoens skal plasseres. På denne bakgrunn kan det være nyttig å vurdere om det finnes andre måter å konstatere faktisk kunnskap på som er egnet til å avgrense den handleplikten digitale mellomledd som er omfattet av art. 14 har. En mulig løsning i denne sammenheng er at spørsmålet hvorvidt en tjenesteyter skal anses for å ha faktisk kunnskap gjøres avhengig av det foreligger en underretning fra en domstol eller en offentlig instans som er satt til å gjøre vurderinger av hvorvidt videreformidlet aktivitet eller informasjon er ulovlig eller krenkende. Etter en slik fremgangsmåte vil man ikke kunne hevde at det foreligger faktisk kunnskap hos digitale mellomledd før en ytre, uavhengig instans har avgjort at innholdet er krenkende eller ulovlig. Fordelen med en slik ordning er at mellomleddet blir fratatt risikoen for den ofte kompliserte vurderingen av om det materiale som lagres eller videreformidles er ulovlig eller ikke. Man vil på denne måten unngå de betenkeligheter som reiser seg ved å overlate kompliserte, rettslige vurderinger til aktører som i mange tilfeller heller sensurerer informasjon enn løper risikoen ved å gjøre den tilgjengelig.

Det kan imidlertid oppstå problemer også med å gjøre en handleplikt for de digitale mellomledd avhengig av kunnskap fra et ytre, uavhengig organ. Jeg tenker i denne sammenhengen særlig på at det kan gå noe tid før en avgjørelse

fra organet foreligger. I den tiden som går fra en mulig krenkelse i det lagrede eller videreformidlede materialet er oppdaget og frem til en avgjørelse om at det faktisk er ulovlig foreligger risikerer man ytterligere krenkelser. En slik tregghet i systemet kan kun motvirkes ved at det kontrollerende organ tildeles de økonomiske og personelle ressurser som er nødvendige for å kunne drive effektivt. Med andre ord er spørsmålet om hvilken ordning man ved implementeringen av e-handelsdirektivet i nasjonal rett skal velge for å plassere risikoen hensiktsmessig mellom digitale mellomledd, rettighetshavere til beskyttet materiale og mellomleddets tjenestemottagere ikke uten politisk interesse.⁹⁸

3.5 Forholdet til digitale mellomledd som ikke er omfattet av e-handelsdirektivets art. 12-14

Som jeg slo fast etter diskusjonen i punkt 2.9 er portaler og søkemotorer digitale mellomledd som ikke omfattes av artiklene 12-14 i e-handelsdirektivet. Virksomhetene nyter derfor ikke godt av direktivets hovedregel om ansvarsfrihet for videreformidling av informasjon.

Det amerikanske DMCA §512, litra (d) oppstiller i motsetning til EU-direktivet en hovedregel om ansvarsfrihet også for søkemotorers og portalers videreformidling av informasjon. Til gjengjeld inneholder DMCA kun reguleringer innenfor det opphavsrettslige området.

På denne bakgrunn er det oppsiktsvekkende at søkemotorer og portaler etter e-handelsdirektivets system ikke nyter godt av den samme ansvarsfriheten som aksessleverandører, nettverksoperatører og host service providere.

Søkemotorer og portaler er både vanlige og viktige aktører i all virksomhet på Internett. Samfunnets interesse i å ivareta hensynet til ytringsfrihet og hensynet til fri informasjonsflyt er derfor like fremtredende i forhold til disse virksomhetene som for de som faktisk omfattes av e-handelsdirektivets art. 12-14. Konsekvensen av de manglende reguleringene er at forutberegneligheten i forhold til visse rettslige aspekter ved søkemotorer og portaler blir dårligere enn for de som omfattes.

Noen begrunnelse for det manglende reguleringsinitiativet gir ikke e-handelsdirektivet. Det er imidlertid flere momenter som taler for at søkemotorer og portaler i første omgang holdes utenfor reguleringene.

⁹⁸ I høringsnotatet fra Nærings- og handelsdepartementet foreslås underretning fra en offentlig instans innført i norsk rett som ett alternativ til kunnskap som skal utløse plikt til å fjerne eller stenge tilgangen til informasjon, jfr. forslagens §12, alternativ 1 og 2.

For det første kan det tenkes at Kommisjonen har funnet det hensiktsmessig å gå skrittvis frem i arbeidet med å regulere ansvarsspørsmålet for digitale aktører. Dette kan begrunnes med at de fleste mellomleddsvirkighetene er relativt nye, og alle konsekvensene av en ansvarsfrihet lar seg umulig forutsi. Tilbakeholdenhet kan derfor være ønskelig for å unngå en ansvarsfrihet som strekker seg for langt, og som av den grunn gir internettaktørene for frie tøyler for. En slik tilbakeholdenhet harmoniserer med uttalelsene i e-handelsdirektivets preambel, punkt (10), som fastholder at de reguleringene som fremgår av direktivet, i tråd med EU-rettens forholdsmessighetsprinsipp, er begrenset til det minimale av det som er nødvendig for å sikre god funksjonalitet innad i det europeiske markedet.

For det annet kan det tenkes at Kommisjonen har funnet det påkrevet å vurdere spørsmålet om ansvarsfrihet for portaler og søkemotorer i sektorvise bestemmelser, etter DMCA's mønster.

Det er vanskelig å trekke noen konklusjon om hvorfor ikke søkemotorer og portaler er regulert i e-handelsdirektivet. Klart er det imidlertid at virksomheten disse aktørene vil skape rettslige tvister i den nære fremtiden. Frem til slike tvister har funnet sin løsning i de nasjonale rettsystemer er det å håpe at erfaringene som er gjort i forhold til de virksomhetene som faktisk er regulert i e-handelsdirektivet kan gi noen svar på hvordan man mest hensiktsmessig skal innføre ansvarsregler for søkemotorer og portaler.

Det er verdt å merke seg at Kommisjonen i henhold til e-handelsdirektivets art. 21 nr. 1 og nr. 2 er pålagt å inngi en rapport til Europaparlamentet, Rådet og Den Økonomiske og Sosiale Komitéen innen 17. juli 2003 og hvert andre år deretter. Rapporten skal ta for seg gjennomføringen av direktivet i de enkelte nasjonalstatene. Herunder skal den skal blant annet analysere behovet for forslag til ansvarsregler for aktører som skaffer til veie linker til etterspurt materiale og for aktører hvis tjenester består i å skaffe til veie lokaliseringverktøy.⁹⁹

⁹⁹ De virksomheter som nevnes i art. 21 nr. 2 tilsvarer de jeg i punkt 1.6.7 og 1.6.8 beskriver som søkemotorer og portaler.

4. OPPSUMMERING OG KONKLUSJON

Mitt generelle inntrykk er at ansvarsregimet i e-handelsdirektivet byr på en balansert løsning som hindrer digitale mellomledd i å bli holdt ansvarlige dersom de ikke har kunnskap om den krenkende eller ulovlige aktiviteten som deres tjenestemottagere utøver, eller dersom de ikke endrer eller manipulerer den informasjonen de videreformidler. Samtidig byr direktivet på løsninger som beskytter de tredjepersoner som utsettes for krenkelser. Sett på denne bakgrunn tror jeg ikke det kan herske tvil om at reguleringene i art. 12-14 vil ha en positiv effekt i forhold til å skape rettslig forutberegnelighet for digitale mellomledd på samme tid som de vil skape et grunnlag for alminnelige brukeres tillit til de aktørene som har sitt virke på Internett.

Kritikken mot e-handelsdirektivets art. 12-14 må etter min mening for det første være at det byr på relativt grovmaskede reguleringer, som ikke nødvendigvis tar høyde for alle aspekter ved den teknologiske utvikling. En annen innvending er at hensynet til ytringsfrihet, informasjonsflyt og effektiv konkurranse ikke er tilstrekkelig ivarettatt i forhold til de aktørene som lagrer informasjon for andre (det vil si de som omfattes av art. 14).

I forhold til det første punktet kan det virke som om den teknologiske virkeligheten, samt visse hensiktsmessige måter å drive forretninger på Internett, har gjennomgått en utvikling som ikke e-handelsdirektivets art. 12-14 har tatt høyde for i alle sammenhenger. F.eks. kan det ut fra en naturlig forståelse av ordlyden i art. 14 være tvilsomt hvem som skal anses for å lagre informasjon i e-handelsdirektivets forstand dersom mellomleddets hele teknologiske infrastruktur er outsourcet til en ren teknologileverandør. Som denne oppgaven forhåpentlig viser, må riktig tilnærmingstype til direktivets bestemmelser i denne sammenheng være å se direktivets ordlyd i et noe videre perspektiv og konsentrere seg om å analysere hvilke funksjonelle særtrekk som preger den mellomleddsrolle hver enkelt aktør i praksis fyller.

Når det gjelder det andre punktet er kritikken særlig at e-handelsdirektivet ikke etablerer omstendigheter eller krav til hvordan private underrettelser om ulovlig innhold til mellomleddene skal foregå. I forhold til sistnevnte punkt er det å håpe at de nasjonale myndighetene ved implementeringen sørger for å etablere ordninger som stiller klare krav til når host service provideren, eventuelt bulletin board operatøren, skal sies å ha kunnskap om at hans servere inneholder krenkende eller ulovlig materiale. På denne måten er det å håpe at den rettslige forutberegneligheten for digitale mellomledd som er etablert

innenfor EU-området blir god nok til at de kan hevde seg i den internasjonale konkurransen.

Konklusjonen er at e-handelsdirektivets reguleringer i art. 12-14 er et steg i riktig retning når det gjelder plassering av risiko der den hører hjemme hos de forskjellige digitale aktørene. Samtidig tar direktivet et langt skritt i retning av å ivareta viktige hensyn som ytringsfrihet og fri informasjonsflyt på Internett. Det gjenstår imidlertid ennå en del arbeide både når det gjelder å innarbeide direktivets bestemmelser i nasjonal rett på en forsvarlig måte, samt å tolke de bestemmelser som implementeres. Når det gjelder arbeidet med å trekke opp grensene for hvor langt hovedregelen om ansvarsfrihet skal strekke seg i forhold til allerede eksisterende ansvarsbestemmelser i nasjonal rett, f.eks. arbeidsgiveransvar for mellomleddene og redaktøransvar på Internett, er dette et komplisert og møysommelig arbeide der det ennå gjenstår en del arbeide for de lovgivende myndigheter.¹⁰⁰

¹⁰⁰

En ekspertgruppe som utgår av personer fra forskjellige departementer og Universitetet i Oslo er i skrivende stund i gang med dette utredningsarbeidet.

LITTERATURLISTE

Elektroniske dokumenter

- Bing, Jon (1999). *The identification of applicable law with regard to the use of protected material in the digital context*: Esprit Project 27028: Electronic Legal Issues Platform (ECLIP). URL: <http://www.jus.uio.no/iri/rettsinfo/seminarer/eclip.html>.
- Julia-Barceló, Rosa (1999a). *Liability for On-line Intermediaries: A European Perspective*: ESPRIT Project 27028: Electronic Commerce Legal Issues Platform (ECLIP) s. 16-24. URL: <http://www.jus.uio.no/iri/rettsinfo/seminarer/eclip.html>.
- Julia-Barceló, Rosa (1999b). *Comparing EU and U.S. i Legal Frameworks*: ESPRIT Project 27028: European Commerce Legal Issues Platform (ECLIP). URL: <http://www.jus.uio.no/iri/rettsinfo/seminarer/eclip.html>.
- Julia-Barceló, Rosa & Koelman J. Kamiel (2000). *Intermediary Liability in the E-commerce proposal: So far so good, but it's not enough*: Elektronisk tilgjengelig: <http://www.ivir.nl/publications/koelman/notenough.html>. Tidsskrift: Computer Law & Security Report 2000 nr. 4, s. 231-239.
- Lenda, Peter (1999). *The choice-of-law in European electronic commerce contracts*: Esprit Project 27028: Electronic Legal Issues Platform (ECLIP). URL: <http://www.jus.uio.no/iri/rettsinfo/seminarer/eclip.html>.
- Ukjente forfattere (2000). *Draft Brochure: Legal Issues of Electronic Commerce – A practical Guide for SMEs*: ESPRIT Project 27028: Electronic Commerce Legal Issues Platform (ECLIP) s. 98. URL: <http://www.jus.uio.no/iri/rettsinfo/seminarer/eclip.html>.

Bøker

- Hellebust, Anders (redaktør)/Andersen, Ulf/Flage Bratsberg, Haakon/ Haraldsen, Arild/ Hovland, Øyvind/ Methlie, Leif B./ Nysveen, Herbjørn/ Scheel, Marianne/ Traasdal, Are Helge (1999). *Elektronisk handel*, Oslo: Cappelen Akademisk Forlag 1999. s. 33 flg. ISBN 82-456-0756-8.
- Sejersted, Fredrik/ Arnesen, Finn/ Rognstad, Ole-Andreas/ Foyn, Sten/Stemshaug, Helge (1995). *EØS-rett*, Oslo: Universitetsforlaget AS 1995, kap. 3.1. ISBN 82-00-22469-4.

Artikler

- Angel, John (1996). *Legal risks of providing services on the Internet*: Journal of Computer, Media and Telecommunications Law: Tolley's Communication Law: Vol 1, No 3, 1996, s. 105-115.
- Einstabland, Nils Kristian (1992). *Kringkastingsbegrepet*: COMPLEX 2/92, s. 105-113.
- Hagstrøm, Viggo (1989). *Informasjonsansvar, om villedning av annen enn kontraktspart*: Tidsskrift for Rettsvitenskap 1989: Universitetsforlaget, side 196-220.
- Loundy, David (1993). *E-Law: Legal Issues Affecting Computer Information Systems And System Operator Liability*: Computer Law Journal, Vol. XII, No. 1, 1993.
- Lloyd, Ian J. (1996). *Liabilities For The Contents Of On-Line Services*: International Journal of Information Technology, Vol. 3, No. 3, 1996.
- Salt, John Peter (1997). *Liability for Information and the Information Society*: International Journal of Law and Information Technology, Vol. 5, No. 3 s. 312 flg.
- Øien, Märtha K (1998). *Notat 42/98*: Telenor FoU.

Offentlige publikasjoner

- Høringsnotat: Innføring av direktiv om elektronisk handel i norsk rett: Lov om visse sider ved elektronisk handel (07.03.2001) Nærings- og handelsdepartementet.
- St. prp. nr. 55 (2000-2001). Om samtykke til godkjenning av EØS-komiteens beslutning nr. 91/2000 av 27. oktober 2000 om endring av vedlegg XI i EØS-avtalen (direktiv om elektronisk handel).
- Ot.prp. nr. 36 (1999-2000) Om lov om opplysningsplikt og angrerett mv. ved fjernsalg og salg utenfor fast utsalgssted (angrerettloven).
- NOU 1999:27 (Særskilt vedlegg nr. 1). Dahl, Hans Fredrik/ Bastiansen, Henrik G./ Eggen: Kyrre. Ytringsfrihetskommisjonen: *Ytringsfriheten i det 20. århundre og Norges internasjonale forpliktelser på ytringsfrihetens område*.
- NOU 1999:26 SD. (Konvergens – Sammensmelting av tele-, data- og medie-sektorene).
- St. meld. nr. 41 (1998-99). *Om elektronisk handel og forretningsdrift*, NHD, s. 6. Tilråding fra Nærings- og handelsdepartementet av 11. juni 1999, godkjent i statsråd samme dag.

Internasjonal lovgivning, traktater og avtaler

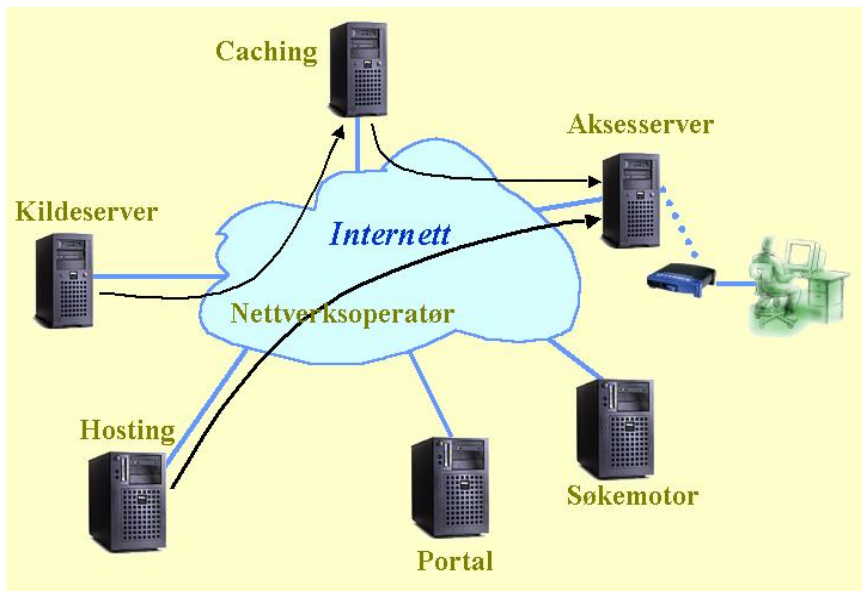
- EU-dir. 2000/31/EF, i kraft fra 8. juni 2000 (OJ L 178, 17/07/2000 p. 0001-0016): Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.
- EU-dir. 98/34/EC, sammenslått og endret ved EU-dir. 98/48/EC. EFT (OJ L 204 21/07/1998 p. 0037), endret ved EU-dir. (OJ L 217 05/08/1998 p. 0018).
- EU-dir. 89/552/EEC, (OJ L 298 17/10/1989 p. 0023). Sist endret ved EU-dir. 97/36/EC (OJ L 202 30/7/1997 p. 0001).
- Amended proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the Internal Market: Dok. nr. 599PC0427.
- 17 U.S.C.A §512: Digital Millennium Copyright Act (DMCA), 28. oktober 1998
- 47 U.S.C.A §230: Communication Decency Act (CDA), 8. feb 1996
- Avtale om Det europeiske økonomiske samarbeidsområde (EØS): Oporto 2. mai 1992 (EØS-avtalen).
- International Covenant on Civil and Political Rights (SP), vedtatt 16.12.1966.
- Traktat om opprettelse af Det europeiske økonomiske Fællesskab: Roma 25. mars 1957 (Romatraktaten)
- Convention for the Protection of Human Rights and Fundamental Freedoms (EMK), vedtatt 04.11.1950.

Rettsavgjørelser

- EF-domstolens sak 109/92, domsgrunn 15.
- EF-domstolens sak C-352/85, domsgrunn 16.
- EF-domstolens sak 283/81.
- Rt. 1970 s. 1154 (Tirrannadommen).
- Rt. 1959 s. 849 (Læreguttdommen).

VEDLEGG 1 ENKEL OVERSIKT OVER DE INTERNETTVIRKSOMHETER SOM ER BESKREVET I OPPGAVEN

Figur 1



TIDLIGERE UTGITT I COMPLEX-SERIEN

CompLex er Institutt for rettsinformatikk skriftserie. Serien startet i 1981, og det har blitt utgitt mer enn hundre titler. Bøkene i CompLex-serien kan bestilles fra GnistAkademika (se bestillingsskjema bak i boken eller www.gnist.no).

2002

- 1/02 Koblingshandel og forholdet til fysisk og teknologisk integrasjon i relasjon til EØS-avtalens art.54(d)**
Ole Jacob Garder NOK 180,-
- 2/02 To opphavsrettslige arbeider:**
Bjarte Aambø – Opphavsrettslige rettsmangler
Erlend Rignes Efskind – Skjermbildets rettslige natur
Aambo / Rignes Efskind..... NOK 201,-
- 3/02 Arbeidstakeroppfinnelser ved universiteter og høyskoler. Innstilling fra et utvalg oppnevnt av universitets- og høyskolerådet 31 januar 2000. Avgitt til universitets- og høyskolerådet i oktober 2001**
..... NOK 213,-
- 4/02 Utøvende kunstners direkteoverføringer på Internett – med hovedvekt på kringkastingsbegrepet**
Irina Eidsvold Tøien..... NOK 225,-
- 5/02 Administrasjon av radiofrekvensspekteret. Rettslige problemstillinger knyttet til telemyndighetenes forvaltning av frekvensressursene**
Øyvind Haugen..... NOK 177,-
- 6/02 Overføring av personopplysninger til tredjeland. Kravet til tilstrekkelig beskyttelse etter EU-direktivet om personvern art. 25**
Mona Naomi Lintvedt og Christopher J. Helgeby.....198,-

2001

- 1/01 **Internet and Choice-of-Law – The International Sale of Digitised Products through the Internet in a European Context**
Peter Lenda..... NOK 275,-
- 2/01 **Internet Domain Names and Trademarks**
Tonje Røste Gulliksen NOK 227,-
- 3/01 **Internasjonal jurisdiksjon ved elektronisk handel – med Lugano-konvensjonen art 5 (5) og elektroniske agenter som eksempel**
Joakim S. T. Øren NOK 204,-
- 4/01 **Legal issues of maritime virtual organisations**
Emily M. Weitzenböck..... NOK 164,-
- 5/01 **Cyberspace jurisdiction in the U.S. – The International Dimension of Due Process**
Henrik Spang-Hanssen..... NOK 685,-
- 6/01 **Norwegian border control in a Europe without Internal Frontiers – Implications for Data Protection and civil liberties**
Stephen Kabera Karanja..... NOK 252,-

2000

- 1/00 **Klassikervernet i norsk åndsrett**
Anne Beth Lange..... NOK 268,-
- 2/00 **Adgangen til å benytte personopplysninger. Med vekt på det opprinnelige behandlingsformålet som begrensningsfaktor**
Claude A. Lenth NOK 248,-
- 3/00 **Innsyn i personopplysninger i elektroniske markedsplasser.**
Line Coll..... NOK 148,-

1999

- 1/99 International regulation and protection of Internet domain and trademarks**
Tonje Røste Gulliksen NOK 248.-
- 2/99 Betaling via Internett**
Camilla Julie Wollan..... NOK 268.-
- 3/99 Internett og jurisdiksjon**
Andreas Frølich Fuglesang & Georg Philip Krog NOK 198.-

1998

- 1/98 Fotografiske verk og fotografiske bilder, åndsverkloven § 1 og § 43 a**
Johan Krabbe-Knudsen..... NOK 198.-
- 2/98 Straffbar hacking, straffelovens § 145 annet ledd**
Guru Wanda Wanvik NOK 238.-
- 3/98 Interconnection – the obligation to interconnect telecommunications networks under EC law**
Katinka Mahieu..... NOK 198.-

1997

- 1/97 Eksemplarframstilling av litterære verk til privat bruk**
Therese Steen..... NOK 158.-
- 2/97 Offentlige anskaffelser av informasjonsteknologi**
Camilla Sivesind Tokvam..... NOK 175.-
- 3/97 Rettslige spørsmål knyttet til Oppgaveregisteret**
Eiliv Berge Madsen..... NOK 170.-
- 4/97 Private pengespill på Internett**
Halvor Manshaus NOK 160.-

- 5/97 **Normative Structures in Natural and Artificial Systems**
Christen Krogh..... NOK 255.-
- 6/97 **Rettslige aspekter ved digital kringkasting**
Jon Bing..... NOK 178.-
- 7/97 **Elektronisk informasjonsansvar**
Tomas Myrbostad NOK148.-
- 8/97 **Avtalelisens etter åndsverksloven § 36**
Ingrid Mauritzen NOK 120.-
- 9/97 **Krav til systemer for forvaltning av immaterielle rettigheter**
Svein Engebretsen..... NOK 168.-
- 10/97 **American Telephony: 120 Years on the Road to Full-blown Competition**
Jason A. Hoida..... NOK 140.-
- 11/97 **Rettslig vern av databaser**
Harald Chr Bjelke NOK 358.-

1996

- 1/96 **Innsynsrett i elektronisk post i offentlig forvaltning**
Knut Magnar Aanestad og Tormod S. Johansen..... NOK 218.-
- 2/96 **Public Policy and Legal regulation of the Information Market in the Digital Network Enviroment**
Stephen John Saxby..... NOK 238.-
- 3/96 **Opplysning på spill**
Ellen Lange..... NOK 218.-
- 4/96 **Personvern og overføring av personopplysninger til utlandet**
Eva I. E. Jarbekk..... NOK 198.-
- 5/96 **Fjernarbeid**
Henning Jakhell..... NOK 235.-

- 6/96 A Legal Advisory System Concerning Electronic Data Inter-
change within the European Community**
Andreas Mitrakas NOK 128.-
- 7/96 Elektronisk publisering: Utvalgte rettslige aspekter**
Jon Bing og Ole E. Tokvam NOK 186.-
- 8/96 Fjernsynsovervåking og personvern**
Finn-Øyvind H. Langfjell NOK 138.-

1995

- 1/95 Rettslige konsekvenser av digitalisering: Rettighetsadministra-
sjon og redaktøransvar i digitale nett**
Jon Bing NOK 368.-
- 2/95 Rettslige spørsmål i forbindelse med utvikling og bruk av stan-
darder innen telekommunikasjon**
Sverre Sandvik NOK 178.-
- 3/95 Legal Expert Systems: Discussion of Theoretical Assumptions**
Tina Smith NOK 278.-
- 4/95 Personvern og straffeansvar – straffelovens § 390**
Ole Tokvam NOK 198.-
- 5/95 Juridisk utredning om filmen «To mistenkelige personer»**
Johs. Andenæs NOK 138.-
- 6/95 Public Administration and Information Technology**
Jon Bing and Dag Wiese Schartum NOK 348.-
- 7/95 Law and Liberty in the Computer Age**
Vittorio Frosini NOK 158.-

1994

- 1/94 **Deon'94, Second International Workshop on Deontic Logic in Computer Science**
Andrew J. I. Jones & Mark Sergot (ed)..... NOK 358.-
- 2/94 **Film og videogramrett. TERESA (60)**
Beate Jacobsen NOK 318.-
- 3/94 **Elektronisk datutveksling i tollforvaltningen – Rettslige spørsmål knyttet til TVINN**
Rolf Risnæs..... NOK 225.-
- 4/94 **Sykepenger og personvern – Noen problemstillinger knyttet til behandlingen av sykepenger i Infotrygd**
Mari Bø Haugestad..... NOK 148.-
- 5/94 **EØS, medier og offentlighet. TERESA (103)**
Mads Andenæs, Rolf Høyer og Nils Risvand NOK 148.-
- 6/94 **Offentlige informasjonstjenester: Rettslige aspekter**
Jon Bing..... NOK148.-
- 7/94 **Sattelittfjernsyn og norsk rett. MERETE (3) IV**
Nils Eivind Risvand..... NOK 138.-
- 8/94 **Videogram på forespørsel. MERETE (14) IV**
Beate Jacobsen (red) NOK 158.-
- 9/94 **«Reverse engineering» av datamaskinprogrammer. TERESA (92) IV**
Bjørn Bjerke..... NOK 198.-
- 10/94 **Skattemessig behandling av utgifter til anskaffelse av datamaskinprogrammer. TERESA (75)**
Gjert Melsom NOK 198.-

1993

- 1/93 **Artificial Intelligence and Law. Legal Philosophy and Legal Theory**
Giovanni Sartor..... NOK 148.-
- 2/93 **Erstatningsansvar for informationstjenester, særlig ved databaseydelser**
Connie Smidt..... NOK 138.-
- 3/93 **Personvern i digitale telenett**
Ingvild Hanssen-Bauer..... NOK 178.-
- 4/93 **Consumers Purchases through Telecommunications in Europe. – Application of private international law to cross-border contractual disputes**
Joachim Benno..... NOK 198.-
- 5/93 **Four essays on: Computers and Information Technology Law**
Morten S. Hagedal..... NOK 218.-
- 6/93 **Sendetidsfordeling i nærradio MERETE (3) III**
Marianne Rytter Evensen..... NOK 148.-
- 7/93 **Essays on Law and Artificial Intelligence**
Richard Susskind..... NOK 158.-

1992

- 1/92 **Avskrivning av mikrodatamaskiner med tilbehør – en nordisk studie TERESA (87)**
Beate Hesselvedt..... NOK 138.-
- 2/92 **Kringkastingsbegrepet TERESA (78)**
Nils Kr. Einstabland..... NOK 208.-
- 3/92 **Rettskilderegistre i Helsedirektoratet NORIS (94) I & II**
Maria Strøm..... NOK 228.-

- 4/92 Softwarepatent – Imaterialrettens enfant terrible. En redegjørelse for patenteringen af softwarerelaterede opfindelser i amerikansk og europæisk ret**
Ditlev Schwanenfügel NOK 158.-
- 5/92 Abonnementskontrakter fro kabelfjernsyn TERESA (78II)**
Lars Borchgrevink Grindal NOK 248.-
- 6/92 Implementing EDI – a proposal for regulatory form**
Rolf Riisnæs NOK 118.-
- 7/92 Deponering av kildekode«escrow»-klausuler TERESA (79)**
Morten S. Hagedal NOK 128.-
- 8/92 EDB i juridisk undervisning – med en reiserapport fra England og USA**
Ola-Kristian Hoff NOK 228.-
- 9/92 Universiteters ansvar for bruk av datanett TERESA (94)**
Jon Bing & Dag Elgesem NOK 198.-
- 10/92 Rettslige sider ved teletorg**
Andreas Galtung NOK 148.-

BESTILLING

Jeg bestiller herved følgende CompLex-utgivelser:

Nummer / årgang: _____

Tittel: _____

Nummer / årgang: _____

Tittel: _____

Nummer / årgang: _____

Tittel: _____

Nummer / årgang: _____

Tittel: _____

Nummer / årgang: _____

Tittel: _____

Navn: _____

Adresse: _____

Postadresse: _____

Telefon: _____

Bestillingsskjemaet sendes pr.post eller telefaks til:



Fagbokhandelen i Oslo

Avd. juridisk litteratur Aulabygningen

Karl Johansgt. 47, 0162 Oslo

Telefon: 22 42 54 50

Telefaks: 22 41 17 08

Complex kan også bestilles via nettbokhandelen www.gnist.no

