Juridiska institutionen
Handelshögskolan vid Göteborgs Universitet

JURIS KANDIDAT PROGRAMMET
Tillämpade studier, 20 poäng
HT 2000

FÖRMEDLARANSVAR PÅ INTERNET

Marie Norén,
Malin Svensson.
Handledare: Professor Christina Hultmark Ramberg

INNEHÅLL

FÖRKORTNINGAR

ARPA	Advanced Research Project Agency
BrB	Brottsbalken
BBS	Bullentin Board System
DMCA	Digital Millenium Copyright Act
EG	Europeiska Gemenskaperna
EU	Europeiska Unionen
HD	Högsta domstolen
HovR	Hovrätten
IETF	Internet Engineering Task Force
IT	Informationsteknologi
JK	Justitiekanslern
LEA	Lag om Elektroniska Anslagstavlor
NJA	Nytt Juridiskt Arkiv (avdelning I)
PUL	Personuppgiftslagen
SkL	Skadeståndslagen
SOU	Statens Offentliga Utredningar
TF	Tryckfrihetsförordningen
TGD	Teledienstgesetz
URL	Upphovsrättslagen
WWW	World Wide Web
YGL	Yttrandefrihetsgrundlagen

1 INLEDNING

Internet utgör ett unikt medium för tillhandahållande och spridande av information. Genom olika siter förmedlas ständigt en mängd olika meddelanden. Informationsflödet är enormt vilket medför en intensifiering av möjligheten att sprida olagliga meddelanden. Kombinationen av brott, våld och Internet har debatterats mycket de senaste åren. Internet framställs på en del håll som ett skymningsland där bl a nazister, rasister och pedofiler okontrollerat breder ut sig. Naturligtvis är den som lägger ut eventuellt olaglig information också primärt ansvarig för denna. Det faktum att Internet utgör ett nytt medium hindrar således inte en tillämpning av traditionella straff- och/eller skadeståndsrättsliga regler. Internets internationella karaktär medför dock att platsen där en användare rent fysiskt befinner sig samt där informationen finns lagrad saknar betydelse. Användaren har följaktligen stora möjligheter att uppträda anonymt eller under falsk identitet.

Vid den förmedling av information som sker på Internet involveras en mängd aktörer med olika roller. Graden av kontroll över aktuell information varierar beroende på vilken roll aktören har i förmedlingsprocessen. Det är här förmedlaransvaret aktualiseras. Innehavaren av förmedlingstjänsten konfronteras med det material som förmedlas. Som en följd av detta har denne, av lagstiftaren, ålagts ett visst ansvar för handlingar som andra utför. Förmedlaren kan således bli straffrättsligt ansvarig i de fall ett olagligt meddelande aktualiseras på dennes tjänst.[1] Ett sådant ansvar kan förefalla underligt med tanke på att motsvarande aktörer på andra marknader, t ex Posten och Telia, inte alls har samma ansvar för material som förmedlas genom deras tjänster.[2] Varför man väljer att särskilja de här situationerna är inte klart. Möjligen anses en förmedlare on-line ha större möjligheter att kontrollera aktuell information än en förmedlare off-line. Här bör dock uppmärksammas att den höga genomströmningstakt, det stora antalet användare samt den enorma mängd meddelanden som förmedlas på en tjänst ofta medför betydande praktiska svårigheter för förmedlaren att kontrollera allt innehåll. Mot

[1] Lag om elektroniska anslagstavlor, 6 §
[2] Varken Posten eller Telia har någon uttalad skyldighet, och inte heller någon rättighet, att öppna ett brev respektive avlyssna ett telefonsamtal för att kontrollera innehållet.

bakgrund av vad som här anförts kan det således ifrågasättas om det kan anses rimligt att ålägga förmedlare ansvar.

1.1 SYFTE

Omfattningen av förmedlares ansvar är oklar. Det finns idag inte något klart definierat ansvarsområde. Förmedlare agerar följaktligen under stor osäkerhet vilket riskerar att påverka den tekniska utvecklingen. Syftet med denna uppsats är att utreda det straff- och skadeståndsrättsliga ansvar som enligt gällande lagstiftning åvilar förmedlare. En redogörelse för samtliga potentiella ansvarsgrunder kommer således att göras. En uppdelning görs mellan svensk rätt, där relevant lagstiftning redogörs för separat, och utländsk rätt där en mer övergripande bild ges av förmedlaransvaret.

Vår avsikt är vidare att uppmärksamma och analysera de brister och oklarheter som råder i den aktuella lagstiftningen. Utifrån det resultat som härvid uppnås kommer sedan en analys av rimligheten att ålägga förmedlare ett ansvar att presenteras. En redogörelse ges även över vilka möjligheter det finns vid sidan av lagstiftning att få klarhet i de problem som råder angående förmedlaransvar. Avslutningsvis ges praktiska råd till förmedlare.

1.2 AVGRÄNSNINGAR

Frågan om förmedlares ansvar på Internet ger upphov till en mängd olika juridiska frågeställningar. Då syftet med framställningen är att, på en djup och detaljrik nivå, utreda nämnda ansvar har flera avgränsningar fått göras. Uppsatsen begränsas således till en juridisk analys. Rent tekniska spörsmål har följaktligen helt negligerats. Problem som uppstår vid kombinationen juridik och teknik har dock uppmärksammats.

Som framgår senare i framställningen har ytterligare avgränsningar skett genom att vi i vissa fall fått nöja oss med att enbart peka på ett aktuellt problem. En närmare analys har följaktligen utelämnats i dylika fall. Medvetna avgränsningar görs främst avseende två omdebatterade problem. Det första problemet utgör den svåra gränsdragningen mellan yttrandefrihet och en effektiv brottsbekämpning. Frågan i vilken omfattning yttrandefrihet

gäller på Internet är idag omdiskuterad. Att inom ramen för denna framställning göra en djupgående utredning av denna fråga är dock inte möjligt. Vidare aktualiseras i uppsatsen, till följd av Internets globala karaktär, en mängd spörsmål kring lagval, domsrätt och verkställighet. Även dessa frågor ligger utanför uppsatsens ram varför inte någon närmare redogörelse görs.

Ämnesområdets snabba utveckling innebär svårigheter att garantera uppgifternas relevans. Arbetets slutdatum sattes till 2000-12-22. Eventuella förändringar efter detta datum har inte uppmärksammats.

1.3 METOD

Då syftet med denna uppsats är att utreda förmedlaransvar på Internet har vi initialt valt att studera Internetstrukturen med dess uppbyggnad och aktörer. Detta för att själva sätta oss in i strukturen men även för att i vår framställning inte ge en missvisande bild av verkligheten. Att *endast* redogöra för ansvarsproblematiken utifrån ett rättsligt perspektiv där man tar avstamp i befintliga regler utan hänsyn till konkreta förhållanden samt tekniska strukturer skulle omöjliggöra en korrekt analys. Kunskap inom detta område har således inhämtats från icke juridiska källor. Intervjuer med systemvetare samt studier i ämnet informatik har därför genomförts.

I vår undersökning av förmedlaransvaret har vi huvudsakligen använt oss av lagstiftning, praxis och doktrin. Vi har även intervjuat personer med kompetens inom området.[3] Vidare har offentliga utredningar utgjort en viktig informationskälla. Genom att studera dem kan man utläsa hur aktuell lagstiftning är tänkt att tillämpas samt vilken inställning lagstiftaren haft till problemet. Åsikter som framförs i doktrin tenderar dock att avvika från innehållet i offentliga utredningar. En jämförelse mellan lagstiftare och andra juridiska auktoriteter är intressant då den belyser diskrepansen. Då doktrin är mer relaterad till aktuella praktiska problem kan man genom att studera den se eventuella svårigheter som tillkommit sedan aktuell lagstiftning införts. Analyser har vidare skett utifrån ett marknadsperspektiv där de olika aktörerna satts i

[3] Bl a Patrik Hiselius jurist på Telia, Advokaten Lars Perhard, Cederquist Advokatbyrå AB samt handläggare på Justitie- och Näringsdepartementet.

centrum. Genom en analys av relevant avtalsreglering har vi försökt finna de olika synsätt som aktualiseras vid tillämpningen av befintlig reglering.

För inhämtande av generella fakta har vi främst haft hjälp av diverse artiklar i dagspress och facktidningar. Vissa delar av uppsatsen baseras på källor från Internet, vilket följer av ämnesvalet. Svårigheten med denna typ av källa är att avgöra dess informationsvärde. Enbart faktaåtergivande torde kunna användas utan svårigheter. Att använda juridiska texter publicerade på Internet är däremot förenat med större risker då det är svårt att avgöra textens juridiska värde. Informationen har dock haft stor betydelse för oss då vårt ämne är hett debatterat och nya synsätt således framförs kontinuerligt. Vidare har informationen varit viktig vid en undersökning av hur relevanta juridiska frågeställningar aktualiseras i praktiken.

Vid utformandet av uppsatsen har slutligen utländsk lagstiftning och framför allt praxis i ämnet använts. Framställningen är dock inte komparativ i traditionell bemärkelse. Lagstiftning utanför Sverige har granskats i de fall då denna ansetts påverka utvecklingen i Sverige. Många gånger sker denna påverkan indirekt genom EU. Som medlem av EU berörs Sverige naturligtvis av de harmoniseringsåtgärder som eftersträvas inom Gemenskapen. Relevanta harmoniseringsåtgärder har därför redovisats och analyserats. Beträffande de delar av uppsatsen som baserar sig på direktivet om elektronisk handel (e-handelsdirektivet) har både europeisk och amerikansk praxis använts som tolkningsunderlag. Då den juridiska utvecklingen inom dataområdet och digitalteknologin har kommit betydligt längre i USA samt haft betydande inflytande på det aktuella området har vi ansett det betydelsefullt att till viss del redogöra för denna utveckling. Relevant amerikansk lagstiftning och rättspraxis har således använts.

2 BAKGRUND

2.1 INTERNET

För att på ett korrekt sätt kunna belysa det ansvar som åvilar förmedlare av elektroniska tjänster samt för att förstå de olika juridiska frågeställningar som aktualiseras är det initialt nödvändigt att kort redogöra för Internets utveckling och uppbyggnad.

När datorer och annan teknisk utrustning kopplas samman så att data kan överföras från en punkt till en annan brukar man tala om ett nät. Det största och troligtvis mest kända nätverket av datanät är Internet. Internet härstammar från ett antal datorer i olika amerikanska städer som kopplades samman i något som man kallade ARPA-net (Advanced Research Project Agency). En central idé bakom detta projekt var att nätverket inte skulle ha något centrum eller mittpunkt som skulle kunna slås ut. ARPA-net utvecklades senare till dagens Internet. Internet utgör ett nätverk av nätverk som möjliggör kommunikation mellan omkring 30-40 miljoner människor i hela världen. Begrepp som tid, rum och avstånd har således helt ändrat innebörd och en helt ny värld, cyberspace, där geografiska positioner och landgränser saknar betydelse har skapats.[4]

1972 uppfanns e-posten och nätet fick därmed en ”mänsklig profil”. En kommunikations-länk mellan människor etablerades. 1979 upprättades USENET och dagens mycket välkända öppna nyhets– och diskussionsgrupper startade. Den absolut största och viktigaste uppfinningen för Internet, som även möjliggjorde dess spridning, kom dock 1991 i och med World Wide Web (WWW). WWW utgör en av de mest avancerade IT-tjänsterna och består av ett världsomspännande nät där själva trådarna utgörs av länkar. Med hjälp av dessa kan surfaren leta sig fram på nätet och finna information utan att egentligen ha någon uppfattning om var i världen informationen finns lagrad. Med WWW ökar omfånget på kommunikationen markant, allt mer avancerad information kan nu överföras i det globala nätet.

Internet utgör följaktligen inte ett nätverk utan består istället av ett stort antal nät som i olika strukturer kopplats ihop. Lite förenklat är det bara att koppla in sig hos någon som har ledig kapacitet och kontakt med något annat nätverk som i sin tur har kontakt med något annat nätverk som har kontakt med….[5]

2.2 AKTÖRER

[4] Owers, ”Jurisdiktion och lagvalsregler i elektronisk miljö”, Christoffer Owers, s 29-30
[5] Carlén-Wendels, ”Nätjuridik”, s 29-31

Det finns idag ingen klar definition av begreppet förmedlare. Såväl svensk som utländsk praxis visar tydligt på den osäkerhet som råder.[6] Vårt syfte är inte heller att försöka pressa fram en sådan definition. En utredning av förmedlaransvaret kräver dock, för att vara rättvisande, att någon form av begreppsförklaring ändå sker. Följande uppdelning bygger på den distinktion av aktörer som huvudsakligen används idag i aktuell praxis och övriga sammanhang.

När viss information tillhandahålls på Internet involveras en lång kedja av olika aktörer, vilka med ett samlingsbegrepp benämns *Service Providers*. En service providers kontakt med själva informationsinnehållet kan variera avsevärt från en helt ”teknisk” kontakt till en mer konkret hantering av en särskild produkt, t ex en text. Service providers uppträder ofta i olika roller med följd att ansvarsfrågan varierar beroende på den aktuella rollen. Ansvarsområdet är komplext och oklart och det är inte möjligt att fastslå ett klart avgränsat område.[7] Negligeras denna komplexitet riskerar man dock en missvisande bild av aktuella ansvarsförhållanden. Eftersom ansvarsfrågan är så nära kopplad till den aktuella aktörsrollen är det alltså nödvändigt att man initialt försöker renodla den nya marknad och de aktörer som aktualiseras.

Internetuppkoppling sker vanligtvis genom att avtal sluts med en service provider. De service providers som finns idag kan delas upp i fyra olika huvudgrupper beroende på vilken typ av service de tillhandahåller. De som enbart erbjuder teknik för överföring av information, t ex ett telefonbolag, benämns *Network Operators*. Möjligheterna för denna aktör att kontrollera överförd information är minimal varför ansvaret är högst begränsat. *Access Providers* erbjuder slutanvändare själva accessen, tillgången till Internet. Access providern har normalt ett löpande avtal med slutanvändaren innebärande att den förre skall sköta all nättrafik. Här föreligger således en mer individualiserad relation till användaren än vad en network operator har. Användaren har i detta fall sin egen server eller sin egen dator och modem. Access providern tillhandahåller den utrustning som krävs för att servern respektive modemet skall kunna kopplas upp mot Internet och möjliggör således för användaren att komma åt det stora nätverket. En ansvarsbedömning brukar här vara problematisk då denna

[6] Se exempelvis MP3-målet, vilket redogörs för i avsnitt 3.3.3.6, där det var fråga om en länkläggare kunde åläggas straffrättsligt ansvar. Ytterligare ett exempel utgör fallet Napster, vilket redogörs för i avsnitt 7.2.1, där domaren inte ville erkänna Napsters roll som förmedlare.

aktör inte sällan erbjuder andra tjänster än enbart access. Det är således ofta svårt att hitta en så renodlad access provider som nyss beskrivits. Så kallade *Content Providers* tillhandahåller det faktiska innehållet på Internet. Var och en som väljer att ”lägga ut” eller på något annat sätt bidra med information faller alltså in under denna grupp. Då denna aktör följaktligen har större möjlighet att kontrollera aktuellt innehåll är han naturligtvis också primärt ansvarig för detta. Ansvarsfrågorna kompliceras dock av att content providers ofta kan agera anonymt eller från länder där de legala instrumenten inte är effektiva.[8]

Sista gruppen av service providers, *Hosting Service Providers*, erbjuder tjänster såsom utrymme på servern för lagring, e-mail, möjligheten att skicka sms och fax via Internet, aktiekurser, nyheter etc. Eftersom det sker en tydlig förmedling av information i detta fall är det, vid ett försök att renodla aktörskategorierna, naturligt att placera förmedlare under denna kategori. En renodlad access provider kan exempelvis inte anses vara en förmedlare då denne inte i sig förmedlar någon information. Förmedlingstjänsterna utvecklas hela tiden och nya tjänster tillkommer således regelbundet. Att mer detaljerat försöka fastslå en klar definition av förmedlarbegreppet är således inte meningsfullt.

Som redan nämnts erbjuder en service provider vidare vanligtvis samtliga eller en del av ovannämnda service. De flesta aktörer uppträder således med olika typer av kombinationer. Det kan t ex vara så att den som tillhandahåller accessen till nätet även erbjuder slutkunderna visst utrymme att lägga upp hemsidor. Trots att det enbart är fråga om en aktör har han två helt olika roller vilka är viktiga att särskilja. Beroende på vilka tjänster som erbjuds kan en förmedlare således hänföras till samtliga roller som beskrivits ovan. En hosting service provider har relativt stor möjlighet att kontrollera den information som erbjuds genom dennes tjänster. Den höga genomströmningstakten, det stora antalet användare samt den enorma mängd information som finns på tjänsten medför dock att det inte är möjligt att lägga ett alltför tungt ansvar på denna aktör. [9]

---

[7] I syfte att underlätta för läsaren har vi valt att huvudsakligen använda begreppet *förmedlare* i framställningen. Övriga begrepp används dock i de fall det är möjligt att klart definiera aktuell tjänst och således renodla aktörens roll.
[8] Rosén, ”Ansvar för utnyttjanden av skyddade prestationer i nätverk”, s 805-808
[9] Rapport 1998-05-25, ”God etik på Nätet”, s 40-43

3 SVENSK RÄTT

3.1 ALLMÄNT

De brottstyper som aktualiseras på Internet utgör ingen enhetlig grupp. Istället är det så att flera av brotten i brottsbalken och andra lagar helt eller delvis kan begås med hjälp av datorer. Det kan således röra sig om allt från upphovsrättsintrång till förtal, häleri eller t ex narkotikabrott. Den gemensamma nämnaren sägs dock vara att det vanligtvis handlar om brott som innefattar *överföring av information*. Flertalet brott faller således utanför Internets ramar. Vid brott som begås via Internet är det den som företar den brottsliga handlingen som primärt ansvarar för eventuella följder. Vår svenska strafflagstiftning får anses relativt väl utformad för att täcka de brott som aktualiseras. Det största problemet med att beivra brottslighet via Internet ligger ofta istället i svårigheten att identifiera gärningsmannen.

En fullständig redogörelse för förmedlaransvaret kräver att man studerar flera lagar. Ansvarsgrunder återfinns i grundlag och i vanlig lag. Viss speciallagstiftning är också aktuell. Svensk rätt innehåller inget strikt ansvar för den som tillhandahåller elektroniska förmedlingstjänster. Ansvar för den spridning som sker genom förmedlingstjänsten kan dock utkrävas enligt allmänna straff- och skadeståndsrättsliga regler. För att ge en distinkt och korrekt beskrivning är det viktigt att man skiljer på förmedlarens skadeståndsrättsliga och straffrättsliga ansvar.[10] Följande framställning bygger på en sådan uppdelning av ansvaret. Som framgår nedan finns det ett samband mellan dessa båda ansvarsregleringar.[11]

3.2 YTTRANDEFRIHET PÅ INTERNET

Med Internet har yttrandefriheten fått en mer konkret innebörd för betydligt fler människor. På Internet är alla publicister. Idag kan alla med Internetanslutning, genom möjligheten att

[10] Ett särskiljande av ansvaret är nödvändigt då man i den skadeståndsrättsliga bedömningen, i vissa fall, inte behöver ta hänsyn till det subjektiva rekvisitet. Enligt exempelvis URL kan en förmedlare bli skadeståndsskyldig utan att han varit medveten om att ett upphovsrättsintrång skett. Detta är inte möjligt inom straffrätten då det subjektiva rekvisitet här är av avgörande betydelse för om en förmedlare skall kunna dömas för brott.

[11] Westman och Lindberg, ”Praktisk IT-rätt”, s 79-81

publi-cera sina åsikter, skvaller, konspirationsteorier mm, agera journalist eller författare. Vår grundläggande yttrandefrihet fastställs i Regeringsformen 2:1. Yttrandefriheten regleras vidare mer detaljerat i Yttrandefrihetsgrundlagen (YGL) och Tryckfrihetsförordningen (TF). Frågan i vilken omfattning dessa grundlagar är tillämpliga på Internet och således i vilken utsträckning yttrandefrihet råder kan inte klart besvaras idag. En utförligare analys i denna fråga kommer att presenteras senare i framställningen, här följer endast en kortare redogörelse.[12]

Konflikten mellan yttrandefriheten och bekämpningen av brottsliga meddelanden är idag föremål för debatt. Två genuina intressen står emot varandra och problemet är således var gränsen mellan dessa båda intressen skall dras. Skall man acceptera total yttrandefrihet på Internet innebärande att brottsbekämpningen till viss del får ge vika eller skall brottsbekämpningen få väga tyngre? Ett praktiskt exempel där denna problematik aktualiseras utgör undergroundtidningen Flashback. Flashback har egna servrar och utgör således ett webbhotell där man kan finna diverse siter innehållande bl a pornografi, nazipropaganda samt olika våldsbudskap. Flashback som konsekvent har propagerat för total yttrandefrihet balanserar följaktligen ständigt på gränsen till vad som är olagligt. På grund av de kontroversiella åsikter som framförts via Flashback har Internetleverantören Powernet sagt upp avtalet med webbhotellet. I nuläget är således Flashback avstängt.[13]

Som nämns ovan utgörs Internet av flertalet sammankopplade nätverk med information från olika källor. Det är således inte fråga om *ett* medium, vilket var utgångspunkten då YGL och TF tillkom. För traditionella medier som tidningar och radioprogram finns regler om vem som ansvarar för presenterat innehåll. Oavsett vem som skrivit en artikel eller vem som framför en åsikt i ett radioprogram så är det alltid *ansvarig utgivare* som ansvarar för spridandet av brottslig information. Ansvaret är strikt och det behöver således inte visas vem som står bakom spridandet av den olagliga informationen för att någon skall kunna ställas till ansvar.

Reglerna om ansvarig utgivare kan dock endast i ett fåtal fall tillämpas på Internetverk-samhet. I YGL 1:6 stadgas att grundlagen är tillämplig på *sändningar* av radioprogram som är riktade till allmänheten samt avsedda att tas emot med tekniska hjälpmedel. Bestämmelsen

[12] Se kapitel 4.
[13] http://skolan.presstext.prb.se

omfattar även sändningar på Internet. Med sändning avses ljud, bild eller skriven text som aktivt skickas ut på nätet och som kan tas emot av en stor mängd mottagare. Kravet att sändningen skall vara riktad till allmänheten innebär att avsändaren utan särskild begäran från mottagaren riktar sändningen till vem som helst som vill ta emot den. Det är således avsändaren som svarar för den huvudsakliga aktiviteten. Mottagaren behöver bara slå på mottagningsapparaten och välja kanal. Problemet är dock att tillämpningar på Internet ofta är interaktiva. Interaktiva tjänster omfattas inte av YGL 1:6 eftersom de inte utgör sändningar. En interaktiv tjänst innebär att tillhandahållandet sker på särskild begäran. Det är således mottagaren som är aktiv. Interaktiva tjänster såsom webbsidor och elektroniska anslagstavlor där besökaren själv är aktiv och kan påverka innehållet faller följaktligen utanför bestämmelsens tillämpningsområde.[14]

Interaktiva tjänster skyddas enbart av YGL om de omfattas av den s k *databasregeln*.[15] Grundlagsskyddet i denna bestämmelse gäller dock inte till förmån för alla som tillhandahåller interaktiva tjänster utan enbart för traditionella massmedieföretag. Skyddet begränsas vidare av att användarna inte skall kunna ändra innehållet. Tjänster som chattar och diskussionsgrupper faller således utanför tillämpningsområdet. Anledningen är att tjänster där användarna själva kan påverka innehållet inte är möjliga för ansvarige utgivaren att kontrollera.[16] YGL:s tillämplighetsområde blir följaktligen snävt och ansvar enligt denna lag kan därför endast utkrävas i undantagsfall.

Tryckfrihetsförordningen

Ännu mer begränsat tillämpningsområde har TF. TF omfattar huvudsakligen tryckta skrifter. Enda undantaget utgör bilageregeln, 1 kap 7§, vilken omfattar webbsidor.[17] Förutsättningen för att denna regel skall kunna tillämpas är att ägaren till en periodisk skrift *oförändrat* sprider en

[14] Westman och Lindberg,"Praktisk IT-rätt", s. 89-90
[15] I 1 kap 9 § YGL stadgas således att *"Denna grundlags föreskrifter om radioprogram tillämpas också när en redaktion för en tryckt periodisk skrift eller för radioprogram, ett företag för yrkesmässig framställning av tekniska upptagningar eller en nyhetsbyrå med hjälp av elektromagnetiska vågor på särskild begäran tillhandahåller allmänheten upplysningar direkt ur ett register med upptagningar för automatisk databehandling. Det gäller dock inte om den mottagande kan ändra innehållet i registret."*
[16] Carlén-Wendels, "Nätjuridik", s 60-62
[17] Hänvisningen till radioprogram i 1:7 syftar tillbaka till definitionen i YGL där alltså även databaser inkluderas.

tryckt skrifts innehåll. TF blir således enbart tillämplig i de fall webbsidans och den tryckta skriftens innehåll är identiskt.[18] Upphovsrättsliga brott samt barnpornografiska brott är uttryckligen undantagna i TF och YGL.

3.2.1 PROBLEM MED YTTRANDEFRIHETSGRUNDLAGEN

En närmare granskning av det särskilda yttrandefrihetsskydd som stadgas i YGL och TF visar att dessa lagar endast täcker in en begränsad del av de olika tjänster som aktualiseras på Internet. Detta medför problem att fastställa i vilken omfattning yttrandefrihet gäller för detta medium. Att grundlagarnas tillämpningsområden är begränsade beror till stor del på de svårigheter som uppkommer när man försöker överföra traditionella grundläggande yttrandefrihetsprinciper på helt nya medier. Internets interaktivitet gör det exempelvis svårt att tillämpa principen om ensamansvar för utgivaren. Denna princip bygger på förutsättningen att utgivaren har kontroll över vad som publiceras. I t ex en elektronisk konferens kan tusentals meddelanden utväxlas mellan tusentals användare varje dag. Möjligheten för förmedlaren att kontrollera innehållet är därför minimal.

Svårigheterna att tillämpa YGL och TF beror vidare på att de aktörer som omfattas inte alltid går att återfinna bland Internets aktörer. Här finns ingen särskild utgivare, tryckare eller spridare. Istället finns det användare, hosting service provider, access provider etc. Frågan är om det är möjligt att tillämpa den aktuella regleringen på de nya medierna. Kanske är det så att den detaljerade yttrandefrihetsreglering som YGL och TF utgör är föråldrad i det nya informationssamhälle vi lever i idag. I de flesta länder i västvärlden saknas en sådan detaljerad reglering som den svenska.[19] Istället ges ofta yttrandefriheten ett generellt skydd genom konstitutionen. Mer detaljerade regler stadgas i vanlig lag eller utvecklas i praxis av landets

[18] SOU 1997:49, s 109-112 samt prop 1990/91:64, s 112. Se även Justitiekanslerns beslut 1999-08-26, Dnr 2778-99-30. Här rörde det sig om en artikel publicerad på en främlingsfientlig hemsida vilken anknöt till en partitidning. Artikeln ansågs inte omfattas av TF endast av den anledning att den inte fanns att återfinnas i tryckt upplaga. Däremot ansågs den uppfylla villkoren för att omfattas av databasregeln i YGL.

[19] Se t ex USA, varifrån vi annars ofta hämtar förebilder, som tillerkänner Internet fullt yttrandefrihetsrättsligt skydd.

domstolar. Det blir således lättare att ta hänsyn till den tekniska och samhälleliga utvecklingen. Nackdelen är att det är svårare att förutse omfattningen av yttrandefrihets-skyddet.[20]

3.3 STRAFFRÄTT

De brott som är särskilt aktuella i ett IT-perspektiv kan delas upp i två huvudgrupper av brott. Den första gruppen skulle med en gemensam beteckning kunna kallas för ”kommunikations-brott”. Typiskt för dessa brott är att själva informationsspridningen är det centrala. Som exempel kan nämnas ”spridande” av barnpornografisk bild eller ”tillgängliggörande” av upphovsrättsligt skyddat material. Den andra gruppen omfattas av brott som innebär obehörigt angrepp mot digitalt lagrad information t ex dataintrång och skadegörelse. Då något förmedlaransvar emellertid inte aktualiseras vid den senare typen av brott har följande framställning begränsats till en redogörelse av ansvaret vid den första typen av brott.[21]

Avgörande för förmedlarens ansvar som gärningsman eller medverkande är den brottsliga handlingens karaktär. Uppfyller förmedlaren aktuella brottsrekvisit i URL eller BrB kommer denne att ansvara som gärningsman. Är rekvisiten ej uppfyllda kan istället ett medverkande-ansvar aktualiseras. Kan förmedlaren inte göras ansvarig enligt någon av dessa lagar återstår ansvar enligt lagen om elektroniska anslagstavlor. Läsaren bör dock redan här upplysas om att ansvar enligt denna lag inte kan utkrävas för själva brottet utan endast för underlåtenhet att informera användarna av tjänsten samt underlåtenhet att hindra spridning av olagligt material.

3.3.1 ANSVAR SOM GÄRNINGSMAN

3.3.1.1 Personuppgiftslagen

Personuppgiftslagen (PUL) har till syfte att skydda den personliga integriteten och reglerar således behandling av personuppgifter. Förmedlaransvaret kan uppkomma om en användare

[20] Brinnen, ”Ansvar och yttrandefrihet i telemedier”, s 20-21

exempelvis använder dennes tjänst för att behandla personuppgifter som avslöjar politiska åsikter.[22] PUL ålägger emellertid inte någon annan än personuppgiftsansvarig ett direkt ansvar.[23] Då förmedlaren endast möjliggör tillgängliggörandet av personregistret kan denne inte ses som personuppgiftsansvarig varför ansvar enligt denna lag inte torde aktualiseras i praktiken.

3.3.1.2 Brottsbalken

I samband med användningen av Internet är följaktligen handlingar där den huvudsakliga gärningen är att *sprida* viss information centrala. Exempel på spridningsbrott utgör förtal (5 kap 1 §, BrB), barnpornografibrott (16 kap 10 a § BrB) samt hets mot folkgrupp (16 kap 8 § BrB). Det är vidare straffbart att erbjuda vissa typer av varor och tjänster, t ex narkotika, vapen etc. Spridning av information som kan användas för att begå brott utgör också exempel på en olaglig handling. Det kan röra sig om instruktioner om hur man lurar olika säkerhetssystem, listor med lösenord etc. En tillämpning av nämnda bestämmelser förutsätter alltså att det skett en otillåten spridning.

Kraven på spridning varierar mellan de olika brotten och det kan därför ofta vara svårt att fastställa om detta krav är uppfyllt eller inte. Vidare måste det aktuella brottets krav på subjektiv täckning vara uppfyllt. Flera brott i BrB kräver uppsåt varför förmedlaren i princip endast blir ansvarig i de fall han är medveten om att olaglig verksamhet förekommer.[24] Många brott är även utformade så att den brottsliga handlingen kan begås av flera personer som samtidigt utför brottet. Samtliga personer som uppfyller rekvisiten för brottet skall då också ses som gärningsman.[25]

3.3.1.3 Upphovsrättslagen

---

[21] Westman och Lindberg, ”Praktisk IT-rätt”, s 81-82
[22] Förbjudet enligt 13 § PUL.
[23] 49 § PUL. Subjektivt rekvisit är uppsåt alternativt oaktsamhet
[24] Se dock BrB 16:10a §, spridning av barnpornografi, BrB 16:10b §, olaga våldsskildring, samt relevanta straffrättsliga bestämmelser i Upphovsrättslagen och Kretsmönsterlagen där det räcker med grov oaktsamhet.
[25] Westman och Lindberg, ”Praktisk IT-rätt”, s 81-95

Samtliga brott i Upphovsrättslagen, URL, kräver uppsåt eller grov oaktsamhet.[26] Vid upphovsrättsliga brott är inte spridandet det väsentliga utan man talar istället om ”tillgängliggörande” av upphovsrättsligt skyddat material. Innebörden torde dock, anser vi, i stort vara densamma. Ett upphovsrättsintrång uppstår då mångfaldigande sker av ett upphovsrättsligt skyddat verk utan upphovsrättsinnehavarens samtycke. Upphovsrättsinnehavare har ensamrätt att förfoga över sitt verk med undantag för vissa inskränkningar, vilka dock lämnas utanför denna framställning. För ansvar enligt URL krävs någon form av aktivt handlande. Detta fastslogs av HD i det så kallade BBS-målet, NJA 1996 s 79 där en förmedlares ansvar såsom gärningsman prövades.[27]

Det var här fråga om en databas till vilken allmänheten kunde skicka in bl a upphovsrättsligt skyddade datorprogram, vilka därigenom blev tillgängliga för andra att hämta hem. Högsta Domstolen fastslog att förmedlaren inte var ansvarig för de upphovsrättsintrång som skedde på dennes databas då han inte på något sätt handlat aktivt. Enbart tillhandahållandet av en BBS, med syftet att denna skulle fungera som en elektronisk brevlåda och lager för program som får spridas fritt, ansågs alltså inte utgöra en sådan aktiv handling som kunde leda till straffrättsligt ansvar för upphovsrättsintrång.

Målet har varit föremål för en omfattande diskussion och är svårtolkat. Det är således osäkert vad utgången skulle ha blivit om det hade varit någon annan typ av brott som begåtts. Om förmedlaren t ex underlåtit att avlägsna barnpornografiska bilder eller uppenbart privatkopierade alster från sin anslagstavla borde denne få svårt att undgå ansvar för i varje fall medhjälp till respektive brott. Hade det vidare visats att systemoperatören utövat någon form av aktiv handling, t ex genom att flytta program från en upload- till en download area[28] eller på annat sätt granskat eller valt vilka av de insända programmen som skulle göras allmänt tillgängliga, skulle ansvar för tillgängliggörande troligen kunnat utkrävas.[29] De krav som dom-

[26] Se 53 § URL
[27] Med BBS avses en server dit Internet-användare, genom ett modem, kan sända in meddelanden samt ta del av vad andra sänt in. Begreppet kan jämställas med elektronisk anslagstavla i traditionell bemärkelse vilket redogörs för i avsnitt 3.3.3.2.
[28] I en upload area kan användare ladda upp program på servern. Download arean möjliggör sedan nedladdning, för andra användare, av samma program.
[29] Se t ex Göta Hovrätt 1998-04-29, dom B 1924/95. Den tilltalade ansågs här ha handlat aktivt då han bl a genom att sortera inkommande program till olika arenor bidragit till att kommersiella program blivit tillgängliga för allmänheten.

stolen ställer på aktivt handlande utgör ett tydligt exempel på svenska domstolars benägenhet att tillämpa legalitetsprincipen.[30] Mot bakgrund av det resonemang som förts visar BBS-målet följaktligen att en förmedlare endast ansvarar för olagligheter på sin site som han är eller borde ha varit medveten om.[31] Det bör slutligen uppmärksammas att något yrkande om ansvar för medverkan inte förekom varför denna fråga inte prövades.

3.3.2 MEDVERKANDEANSVAR

Någon som främjar en gärning med råd och dåd kan enligt BrB dömas som medverkande. En förmedlare kan således drabbas av ansvar trots att denne inte uppfyller de i brottsbeskrivningen uppställda rekvisiten för straffbarhet. Det är osäkert vilken grad av aktivitet som krävs för denna typ av ansvar. Ser man till rättspraxis har kravet satts förhållandevis lågt. För att kunna göras ansvarig måste kunna fastställas att förmedlaren hade subjektiv täckning dels vad gäller själva huvudbrottet dels vad gäller att denne främjat en viss gärning. En förutsättning för medverkandeansvar är vidare att huvudbrottet på något sätt är ”pågående”. Man kan inte främja en gärning som redan är avslutad.

Avgörande för om ansvar kan utkrävas borde bli förmedlingstjänstens karaktär. Medverkandeansvar torde främst aktualiseras för den som tillhandahåller tjänster som huvudsakligen tjänar för brottsliga ändamål eftersom möjligheten, i dessa fall, att fastställa den subjektiva täckningen är relativt stor. Ansvar för webbhotell och andra liknande förmedlare, vars tjänster ej tillhandahålls i brottsligt syfte, borde aktualiseras mer sällan. En förmedlare som i legitimt syfte bedriver en förmedlingstjänst kan endast anses ha medverkat till gärningen om han främjat gärningen på något annat sätt än genom att tillhandahålla själva utrustningen.[32] En som länkar material borde i vissa fall kunna dömas till ansvar för medverkan. En länk till en

[30] Rosén, ”Ansvar för utnyttjande av skyddade prestationer i nätverk”, s 822
[31] Att så är fallet visar även NJA 1996 s. 74 där en operatör för en BBS blev dömd till ansvar såsom gärningsman. Brottet utgjordes av upphovsrättsintrång avseende minst 1000 olika datorprogram. Genom att olovligen mottaga och behålla kopior av programmen gjorde operatören dem sedan tillgängliga för ca. 300 betalande användare av BBS:en. Användarna hade sedan möjlighet att via modem och egna datorer framställa kopior av ovannämnda program. Förmedlarens *uppsåt* till upphovsrättsintrånget ansågs enligt hovrätten styrkt. Frågan om ansvar för brottet var ej föremål för prövning i HD då målet inte överklagades i denna del.
[32] Det subjektiva rekvisitet är således av avgörande betydelse för förmedlares medverkandeansvar.

webbsida där det bedrivs koppleriverksamhet kan i vissa situationer ses som medhjälp till koppleri.[33]

Medverkandeansvaret aktualiseras bl a i ett fall från 1998.[34] Det var fråga om ett upphovsrättsligt brott. De tilltalade var åtalade för medverkan till otillåten kopiering av datorprogram som skett genom deras BBS. Domstolen fastslog att det inte rådde något tvivel om att den aktuella BBS:en inrättats i syfte att fungera som en s k elite-databas[35] samt att de tilltalade på olika sätt medverkat till dess tillkomst och drift. Vidare konstaterades att samtliga tilltalade måste ha varit medvetna om möjligheten att det skulle kunna förekomma att program utan tillstånd kopierades till denna. Domstolen fann således att de tilltalade genom att tillhandahålla BBS:en för användare på det sätt som skett åtminstone genom grov oaktsamhet främjat den otillåtna kopieringen så att de skulle dömas för medhjälp till brott mot upphovsrättslagen.[36]

3.3.3 LAG OM ELEKTRONISKA ANSLAGSTAVLOR

Som nyligen redogjorts för är möjligheterna att ålägga en förmedlare ansvar enligt BrB eller URL relativt begränsade. Genom Lag om ansvar för elektroniska anslagstavlor, LEA, utvidgas emellertid förmedlarens ansvar ytterligare. Lagen ålägger förmedlare att i vissa fall *ta bort* material som finns på dennes server eller på annat sätt tillhandahålls genom dennes tjänst. Han blir således inte ansvarig för själva innehållet i material som innebär något av de i lagen uppräknade brotten. Den som skickat materialet har själv det fulla ansvaret om materialet är olagligt. Lagen omfattar endast ett fåtal typer av olagligheter och skall endast tillämpas i de fall tillhandahållaren inte kan straffas enligt bestämmelser i BrB eller URL.

3.3.3.1 Tillämpningsområde

[33] Westman och Lindberg, ”Praktisk IT-rätt”, s 96-97
[34] Svea Hovrätt 1998-09-29, dom DB 101, målnr B 318/97
[35] En Elite-databas innehåller datorprogram som endast varit utgivna en kort tid eller som inte varit utgivna överhuvud taget.
[36] Omständigheterna i detta mål är snarlika de i BBS-målet, vilket redogörs för i avsnitt 3.3.1.3. Trots detta har målen fått olika utgång. Förmedlaren friades helt från ansvar i BBS-målet. I förevarande fall från 1998 dömdes den tilltalade istället som medverkande till brottet. Domarna kan tyckas motstridiga. Avgörande borde dock vara att åklagaren i BBS-målet inte yrkade på ansvar för medverkan. Möjligen hade utgången blivit annorlunda om ett sådant yrkande gjorts.

I 1 § LEA stadgas att lagen gäller *elektroniska anslagstavlor*. Med elektronisk anslagstavla avses ”tjänst för elektronisk förmedling av meddelanden”. Meddelanden omfattar text, bild, ljud eller information i övrigt, t ex datorprogram. Vid en första anblick kan lagens tillämpningsområde uppfattas som klart definierat. Studerar man lagen lite närmare framträder emellertid diverse oklarheter. Ett tydligt och mycket centralt exempel utgör svårigheten att avgöra vilka tjänster som omfattas av definitionen ”tjänst för elektronisk förmedling av meddelanden”. Man har i förarbetena avsiktligen valt att inte fastslå någon klar definition. Avgörande för lagens tillämpning är dock att det rör sig om en tjänst för förmedling av meddelanden.[37]

3.3.3.2 Elektronisk anslagstavla

En elektronisk anslagstavla i traditionell bemärkelse utgörs av en dator/server dit allmänheten, eller en utvald krets med accesskod, kan sända in meddelanden och ta del av vad andra sänt in. Anslagstavlan nås genom ett modem som är kopplat till ett visst abonnentnummer. Begreppet har senare utvidgats till att idag även omfatta datorer/servrar med annat material än ”meddelanden” t ex datorprogram, bildarkiv osv. Genom LEA utvidgas innebörden ytterligare till att omfatta sådana tjänster som nås via Internet eller något annat nät för dator-kommunikation.

Den traditionella definitionen av begreppet elektronisk anslagstavla har således övergetts i LEA. Att tillämpningsområdet enligt lagen gjorts mycket bredare än det som traditionellt omfattas av begreppet har lett till diverse oklarheter. I förarbetena görs dock ett försök att reda ut dessa oklarheter. Syftet är att försöka klargöra vilka tjänster som omfattas. Ett avgörande kriterium som återkommer på flera ställen är att den som använder tjänsten skall kunna ta del av andras meddelanden *och* sända egna meddelanden till andra. Det handlar följaktligen om tjänster som möjliggör elektronisk kommunikation mellan människor. Den tekniska lösningen för kommunikationen saknar betydelse.

Lagen omfattar i princip alla tjänster för elektronisk förmedling av meddelanden. Samtidigt slås emellertid fast att det inte är möjligt att göra en heltäckande omfattning då den snabba

[37] Westman och Lindberg, ”Praktisk IT-rätt”, s 98

utvecklingen på området skulle medföra att en sådan uppräkning snabbt blev föråldrad. Exempel på tjänster som omfattas är dock newstjänster, chattjänster, elektronisk post som skickas via en öppen distributionslista samt webbhotell.[38] Ett webbhotell innebär att en Internetoperatör erbjuder användare lagringsutrymme för hemsidor. Det har ifrågasatts om portaler på Internet (t ex Passagen eller Torget) skulle kunna omfattas av begreppet elektronisk anslagstavla. En portal tillhandahåller en mängd tjänster som nyheter, väderleksrapporter, möjlighet till webbshopping etc. Då den praktiska möjligheten att kontrollera meddelanden på en stor portal är förhållandevis liten blir dock lagen svår att tillämpa. Vidare består stora portaler ofta av en kombination av tjänster, vilket gör att de blir mer svåröverskådliga. Rättsläget är dock osäkert varför frågan slutgiltigt får avgöras av domstol.[39]

Att konkret söka fastställa exakt vad som utgör en elektronisk anslagstavla samt vilka tjänster som omfattas är alltså inte möjligt. Ett försök att ange en klart avgränsad definition skulle troligtvis vidare stå i strid med de krav på flexibilitet som den tekniska utvecklingen ställer på lagstiftningen. Genom förarbetena till lagen försöker man dock bl a genom kriteriet ”sända och ta del av” fastställa vissa vägledande riktlinjer. Vi anser emellertid förarbetena vara relativt otydligt utformade eftersom man samtidigt, genom att t ex inkludera tjänsten webbhotell, talar emot en tillämpning av detta kriterium. Det är enligt vår mening inte möjligt att tillämpa nämnda kriterium på denna tjänst. Avgörande bör istället, mot bakgrund av ovanstående resonemang, vara om förmedlaren erbjuder lagringsutrymme eller inte. Avsikten borde således vara att samtliga tjänster där någon yrkesmässigt tillhandahåller elektroniskt lagringsutrymme, dit andra kan sända in eller på annat sätt få sitt material publicerat för en större krets, skall omfattas.[40] Detta synsätt överensstämmer med den inställning som huvudsakligen anammats i doktrin och övriga sammanhang.[41]

Vid en ansvarsbedömning utgår man således från själva hanteringen av den förmedlade informationen och skiljer följaktligen på tillhandahållande av teknik för enbart överföring av information, tillfällig lagring samt mera varaktig lagring. Avgörande för ansvarsfrågan är därför

[38] Prop 1997/98:15, s 6-10
[39] http://www.kultur.nu/juridik/itratt_ansvar.html
[40] Carlén-Wendels, “Nätjuridik”, s 66-67

på vilket av anförda sätt informationen hanterats. Någon undersökning av möjligheten att sända och ta del av information görs alltså inte. Då de tjänster som omfattas av LEA medför en varaktig lagring talar således detta för att ovannämnda kriterium bör användas som riktlinje vid en bedömning av lagens tillämpningsområde.

3.3.3.3 Undantag

Lagen riktar sig mot ”den som tillhandahåller en elektronisk anslagstavla ”. Avgörande för lagens tillämpning är således vem som sköter själva driften av anslagstavlan och som bestämmer över tjänstens användning. En samlad bedömning av vem eller vilka som har kontrollen och det bestämmande inflytandet måste därför göras. I 2 § följer en uppräkning på situationer då lagen inte skall tillämpas;

- Tillhandahållande endast av nät eller andra förbindelser för överföring av meddelanden eller av andra anordningar som krävs för att kunna ta i anspråk ett nät eller annan förbindelse. Renodlad ”accessproviding” d v s tillhandahållande av bara nät eller dylikt för överföring av elektroniska meddelanden omfattas alltså inte. Då network/accessprovidern inte har något direkt inflytande över vilka tjänster som tillhandahålls skall det inte heller vara möjligt att ställa denne till ansvar. Inte heller tillhandahållande av annan teknik, t ex lagringsutrymme, som är nödvändig för att kunna utnyttja ett nät skall omfattas av ansvaret.
- Förmedling av meddelanden inom en myndighet eller mellan myndigheter eller inom ett företag eller en koncern.
- Tjänster som skyddas av TF eller YGL.
- Meddelanden som är avsedda bara för en viss mottagare eller en bestämd krets av mottagare. Här avses e-brev där avsändaren bestämt vet vem eller vilka personer som skall ta emot meddelandet. På motsvarande sätt som inte Posten ansvarar för innehållet i de brev som förmedlas skall inte heller den som tillhandahåller en tjänst för

[41] Se t ex Artikel 12-14 e-handelsirektivet 2000/31/EG, där det stadgas att avgörande betydelse vid en ansvarsbedömning skall läggas på själva aktiviteten, relaterad till informationen, snarare än vid möjligheten att

elektronisk post ha något ansvar för detta. E-post som distribueras genom öppna distributionslistor, d v s mail–listor dit vem som helst kan anmäla sig, borde dock omfattas av lagen.

3.3.3.4 Information till användarna

Tillhandahållaren av en elektronisk anslagstavla är enligt 3 § tvungen att informera samtliga som ansluter sig till tjänsten om sin identitet samt i vilken utsträckning inkomna meddelanden blir tillgängliga för andra användare. För en användare kan det ha stor betydelse vem som tillhandahåller tjänsten. Att förmedlaren uppträder öppet är även av stor betydelse när det gäller det allmännas möjligheter att ingripa mot spridning av olagliga meddelanden. Det är också viktigt att användare förstår i vilken utsträckning insända meddelanden blir tillgängliga för andra användare. Informationen från förmedlaren skall vara tydlig och enkel att finna.

3.3.3.5 Uppsikt över tjänsten

I 4 § stadgas att förmedlaren är skyldig att ha sådan uppsikt över tjänsten som ”skäligen kan krävas med hänsyn till omfattningen och inriktningen av verksamheten”. Omfattningen av detta uppsiktskrav är inte fastställt, men att någon form av återkommande kontroll krävs är dock klart. Förmedlaren bör därför regelbundet se över innehållet i den elektroniska anslagstavlan. Hur frekvent en sådan kontroll skall ske får avgöras från fall till fall. Som riktmärke anges i förarbetena att en tjänst inte bör lämnas utan tillsyn under längre tid än en vecka. Faktorer som kan vara av betydelse för vilken grad av uppsikt som krävs är bl a mängden av meddelanden, antalet användare av tjänsten, om tjänsten erbjuds yrkesmässigt, om brottsliga meddelanden har varit vanligt förekommande samt kostnaderna för kontroll. Avsikten är inte att förmedlaren skall drabbas negativt på det sätt att verksamheten i väsentlig mån försvåras eller att uppkomsten av nya tjänster riskerar att äventyras. I de fall då mängden meddelanden är så stor att det är svårt att läsa alla anses uppsiktsplikten ändå vara uppfylld

---

sända och ta del av meddelande.

om en ”klagomur” till vilken användarna kan påtala eventuella brottsliga meddelanden upprättats.

3.3.3.6 Skyldighet att ta bort vissa meddelanden

Förmedlaren är enligt 5 § skyldig att ta bort eller på annat sätt förhindra spridning av ett meddelande om innehållet är *uppenbart* brottsligt enligt bestämmelserna i brottsbalken om uppvigling, hets mot folkgrupp, barnpornografibrott eller olaga våldsskildring. Endast denna typ av brottsliga meddelanden omfattas av skyldigheten. Samma skyldighet föreligger om det är *uppenbart* att användaren genom att sända in meddelandet gjort intrång i upphovsrätt eller närstående rättighet. I de fall förmedlaren uppdrar åt någon annan att hålla uppsikt över tjänsten bör samma skyldighet inträda för denne. Det finns inget krav att förmedlaren sparar meddelandet. Då det ibland kan vara svårt att avgöra om ett meddelande är brottsligt eller inte har skyldigheten alltså begränsats till meddelanden som uppenbart har ett sådant innehåll som avses i aktuella lagrum. Vid en bedömning huruvida något är uppenbart eller inte är det av betydelse hur tydligt meddelandet är. För fullbordat brott bör inte krävas att någon spridning till andra användare faktiskt har ägt rum. Det bör i detta avseende räcka att meddelandet hålls tillgängligt för användare av tjänsten vid den tidpunkt då meddelandet bort avlägsnas. Skyldigheten gäller enbart meddelanden som sänts in till tjänsten av en användare. Länkar till olagligt material som finns på andra tjänster omfattas således inte. [42] I 5 § 2 st ges förmedlaren en rätt att ta del av de meddelanden som förekommer i tjänsten.[43]

---

[42] Att en länkläggare emellertid kan ha ett allmänt straffrättsligt ansvar visar NJA 2000 s.292, ”MP3-målet”. Huruvida gärningsmannen här kan anses utgöra förmedlare eller inte förefaller emellertid oklart. Denna fråga aktualiserades inte heller i målet. Vi har dock ändå valt att kort redogöra för nämnda fall då vi i viss mån anser det relatera till den problematik som framställningen bygger på. I föreliggande fall hade den svenske länkläggaren underlättat åtkomst till olovligt tillgängliggjorda ljudfiler i MP3-format vilka fanns att hitta på främst amerikanska servrar. På länkläggarens hemsida fanns även en lista över tillgängliga ljudfiler. Prövningen i HD begränsades dock, genom gärningsbeskrivningen, till frågan om ett olovligt tillgängliggörande för allmänheten skett. Detta ansågs vara fallet men p g a undantagsregeln i 47 § URL, för offentligt framförda ljudfiler, var ej förfarandet straffbart. Gränsdragningen mellan upphovsrättsligt relevant tillgängliggörande och en ren hänvisning berördes inte. Möjligen innebär detta att HD anser att länkläggning kan utgöra ett upphovsrättsintrång. Frågan blir än mer relevant då man genom att dra paralleller till BBS-målet kommer fram till att det krav på aktiv handling som där fastställs är uppfyllt, genom enbart själva länkläggandet, i föreliggande fall. En länkläggares ansvar får sålunda, trots MP3-målet, fortfarande anses oklart. (Rosén, ”Ansvar för utnyttjande av skyddade prestationer i nätverk”, s 813 ff samt Westman, ”MP3-målet i HD –rättsläget kring länkning fortfarande oklart”.)

[43] Westman och Lindberg, ”Praktisk IT-rätt”, s 98-101

Ansvaret begränsas följaktligen till vissa typer av brott. Denna begränsning motiveras med att reglerna skulle bli för svåra att följa om alla slags brottsliga gärningar omfattades. Det kraftiga informationsflödet gör det omöjligt för den som tillhandahåller tjänsten att systematiskt granska och bedöma alla meddelanden som förmedlas. I syfte att underlätta ansvaret för förmedlaren har bestämmelsen därför konstruerats så att den tar direkt sikte på ett meddelandes utformning. Utgångspunkt tas således i meddelandets innehåll istället för den brottsliga gärningen hos användaren. Tillvägagångssättet avser att göra det lättare för förmedlaren att överblicka det straffbara området samtidigt som utredningen av brott skall underlättas.

Det straffbara området begränsas till vissa brott mot allmän ordning samt intrång i upphovsrätten. Vid brott mot allmän ordning är det ofta möjligt att göra en bedömning som grundas enbart på det specifika meddelandets innehåll. Den typ av meddelanden som de aktuella bestämmelserna är relaterade till anses relativt enkla att identifiera och en bedömning kan därför göras utifrån objektiva grunder. Vad gäller upphovsrättsligt skyddade meddelanden så knyts ansvaret till om användaren genom att sända in meddelandet har gjort intrång i upphovsrätt eller i närstående rättighet som skyddas genom föreskrift i 5 kap URL. En generell förutsättning för alla verkstyper som publiceras på Internet är att verket är utgivet samt att upphovsmannen givit sitt uttryckliga eller underförstådda samtycke till publiceringen. Bedömningen huruvida ett brott föreligger blir här svårare för förmedlaren.[44] Möjligen beror detta på att det inte är självklart, för förmedlaren, att innehållet i ett meddelande är upphovsrättsligt skyddat. Förmedlaren kan inte heller förutsätta att samtycke saknas.[45]

3.3.3.7 Straff

Den som uppsåtligen eller av oaktsamhet bryter mot skyldigheten att *lämna information* skall enligt 6 § dömas till böter. Vad gäller skyldigheten att *ta bort meddelanden eller på annat sätt förhindra spridning* kan förmedlaren istället vid uppsåt eller grov oaktsamhet dömas till böter eller fängelse i sex månader. Skyldigheten att ta bort och förhindra fortsatt spridning inträder när förmedlaren får kännedom om det aktuella meddelandet. Förmedlaren anses ha erhållit

[44] Prop 1997/98: 15, s 11-13

kännedom om denne själv läst meddelandet eller då någon, på annat sätt, gjort honom uppmärksam på meddelandet. Då även grovt oaktsamma förfaranden kriminaliserats kan förmedlaren bli ansvarig i fall då denne saknat kännedom om meddelandet.

Vid bedömningen av om grov oaktsamhet förelegat skall uppmärksamhet fästas vid huruvida förmedlaren uppfyllt sin uppsiktsplikt. Har brottsliga meddelanden förekommit ofta ställs högre krav på åtgärder av förmedlaren. Ett större krav på aktiva åtgärder bör då också krävas. Är brottet att anse som grovt är straffmaximum två års fängelse. I ringa fall döms inte till ansvar. Rör det sig t ex om ett enstaka meddelande i en i övrigt seriös verksamhet borde tillhandahållaren därför undgå straff. Datorer och andra hjälpmedel som använts vid utförandet av brottet kan enligt 8 § förklaras förverkade. Bestämmelsen som är ett komplement till straffbestämmelsen syftar främst till att förhindra fortsatt brottslighet.[46]

3.3.4 PROBLEM MED LEA

Ovanstående redogörelse visar hur förmedlares ansvar kommit att utvidgas i och med LEA. Lagen som ännu inte tillämpats en enda gång i svensk domstol har fått mycket kritik från olika håll. Vikten och betydelsen av denna lag kan således ifrågasättas. Frågan är om man vid utformandet tagit tillräckligt stor hänsyn till erfarenhet och synpunkter från parterna på marknaden. Som framgår längre fram i uppsatsen har lagstiftning som utformats i samarbete med aktörer på marknaden visat sig få stor genomslagskraft.[47] Tillvägagångssättet medför att bättre hänsyn tas till de problem som de facto föreligger i praktiken.

3.3.4.1 Otydligt utformad

Som redan nämnts medför LEA:s oklara utformning diverse frågetecken vad gäller dess tillämpning. Vi har redan nämnt de problem som råder angående definitionen av elektronisk tjänst.[48] Här saknas, menar vi, klara riktlinjer. Vårt syfte är inte på något sätt att försöka

---

[45] I sammanhanget skall dock inte glömmas bort att meddelandet måste vara uppenbart brottsligt för åläggande av ansvar.
[46] Westman och Lindberg, ”Praktisk IT-rätt”, s 101
[47] Se avsnitt 7.2.1.
[48] Se avsnitt 3.3.3.2.

tvinga fram ett klart definierat avgränsningsområde innebärande en uttömmande lista på vilka tjänster som omfattas. Vi instämmer med vad som anges i förarbetena om svårigheterna att fastställa en klar definition. En sådan definition skulle innebära att man bortsåg från den tekniska utveckling som ständigt sker och skulle således, för att vara korrekt, ständigt få redigeras i takt med denna utveckling. Det viktiga är dock att man försöker etablera konsekventa riktlinjer som sedan kan vara vägledande vid en eventuell bedömning. Vi menar att de försök som gjorts idag att fastställa sådana riktlinjer till viss del är motsägelsefulla. Att det trots aktuell lagstiftning och förarbeten föreligger stor osäkerhet leder till att förmedlares möjligheter att förutse eventuella konsekvenser av en handling är begränsade.

Att lagen är otydligt utformad visar vidare 2 § moment 4 ”Lagen gäller dock inte… meddelanden som är avsedda bara för en viss mottagare eller en begränsad krets av mottagare (elektronisk post)”. Eftersom meddelanden som är avsedda för en viss bestämd krets av mottagare kan spridas på flera andra sätt än med elektronisk post, t ex via slutna möten i konferenssystem eller genom Usenet News-grupper som bara sprids till användare vid en viss server, så är det oklart om lagen avser att undanta bara elektronisk post eller alla slags meddelanden som är avsedda för en begränsad krets av mottagare. Vidare kan lagstiftaren omöjligt ha beaktat den omfattande replikering som sker av meddelanden. Replikeringen innebär att ett meddelande kan *kopieras* från en värddator till en annan. Användarna har således möjlighet att hitta aktuell information i en lokal värddator trots att den ursprungligen kommer från någon annan dator i nätet. Detta sätt att sprida och förmedla information används av flera stora system på marknaden. Förarbetena till lagen stadgar att förmedlare är skyldig att förhindra spridning av olagliga meddelanden. Det framgår dock inte klart om detta enbart gäller meddelanden som skickas in lokalt, eller också meddelanden som kommer till servern via replikering.[49]

3.3.4.2 Övervakningsansvar

Enligt 4 § är förmedlaren skyldig att förhandsgranska information som tillhandahålls genom dennes tjänster. Sverige är idag det enda land i världen som genom lagstiftning stadgar ett

övervakningsansvar.[50] Utgångspunkten är, enligt förarbetena, att förmedlare som tillhandahåller en elektronisk anslagstavla inte passivt skall kunna se på utan att ingripa när användare missbrukar tjänsten. I rak motsats till lagtextens faktiska ordalydelse anges emellertid att ”Någon förhandsgranskning eller något generellt krav på att granska varje enskilt meddelande har regeringen aldrig avsett att slå fast. Skyldigheten att avlägsna meddelanden ur tjänsten måste också ses mot bakgrund av att det bara är uppsåtliga och grovt oaktsamma överträdelser av skyldigheten som är straffbara.”[51] Hur detta överensstämmer med ordalydelsen kan vi omöjligen finna något bra svar på. Möjligen är det så att kravet på uppsåt eller grov oaktsamhet medför att förmedlare i princip endast är skyldig att avlägsna ett meddelande om han får vetskap om dess existens. Någon förhandsgranskning krävs således inte. Måhända avser lagstiftaren att skilja på förmedlingstjänster där brottsliga meddelanden sällan förekommer och tjänster där de är mer vanligt förekommande. I de fall olagliga meddelanden förekommer frekvent måste således allt granskas i förväg medan i fall där dylika meddelanden inte är vanliga är förmedlaren endast skyldig att agera efter klagomål från användare.[52] Vad som gäller, förhandsgranskning eller inte, är som synes väldigt oklart.

Frågan kommer troligtvis att ställas på sin spets i och med införandet av e-handelsdirektivet 2000/ 31/EG enligt vilket medlemsstaterna inte är tillåtna att ha ett allmänt övervakningsansvar i sin nationella lagstiftning.[53] Ser man till den debatt som idag förs angående 4 § så förefaller lagen stadga ett allmänt övervakningsansvar. I syfte att uppnå ett klargörande bör bestämmelsen, enligt vår mening, helt tas bort.

Den totala volymen av information som förmedlas via Internet är för stor för att en sådan granskning av förmedlare skall vara realistisk. I Usenet News distribueras t ex omkring en miljon nya artiklar varje vecka. Diskussionerna i elektroniska diskussionsgrupper bygger på snabbhet. Ofta skrivs inlägg, svar på inlägg och nya svar på svaren inom en tidsrymd av mindre än ett dygn. Erfarenheterna från de grupper som använder sig av förhandsgranskning är att en sådan granskning i praktiken innebär en fördröjning med flera dagar. En

---

[49] Palme, ”Ett misslyckat lagförslag”
[50] Källa: Patrik Hiselius, jurist på Telia AB
[51] Prop 1997/98:15, s 18
[52] Palme, ” Ett misslyckat lagförslag”
[53] Se utförligare beskrivning om e-handelsdirektivet och de problem som aktualiseras i kap 6.

förhandsgranskning kräver vidare att den som ansvarar för tjänsten går in och läser vad som skrivs i slutna diskussionsgrupper för att på så sätt ha kontroll över eventuella olagliga meddelanden. Frågan är om detta kan anses acceptabelt.[54]

Att lägga ansvaret på den aktör som ansvarar för servern där en hemsida rent fysiskt lagras är vidare ett klart exempel på hur ett beaktande av tekniken negligerats. Ett meddelande som förmedlas eller lagras på Internet utgör inte en klart avgränsad enhet. En bild behöver överhuvudtaget inte existera innan den når mottagarens dator. Något olagligt meddelande behöver således inte finnas förrän den millisekund någon väljer att titta på bilden. En bild kan delas upp i olika fragment som i sin tur lagras på olika webbhotell. Det blir i ett sådant fall oväsentligt hur ofta förmedlaren granskar sin tjänst eftersom han aldrig skulle kunna se vad bildfragmenten föreställer. Det finns därmed inte heller någon skyldighet att ta bort dem.[55]

3.3.4.3 Hindra spridning

Slutligen bör 5 § och skyldigheten att hindra spridning av olagligt material nämnas. Som redan antytts anses denna bestämmelse, på vissa håll, stå i konflikt med yttrandefriheten. En närmare analys av detta problem görs dock inte här. Läsaren hänvisas istället till avsnitt 4.3.

För att underlätta för förmedlaren att fullgöra sin övervakningsskyldighet har bestämmelsen begränsats till att avse endast vissa typer av brott. Frågan är dock om det i praktiken skulle utgöra någon större skillnad om istället samtliga brott omfattades. De åtgärder som krävs för att fullgöra skyldigheten enligt denna paragraf tycks, enligt vår mening, inte bli mer betungande för förmedlaren enbart av den anledningen att det tillkommer fler brott. Förmedlaren är fortfarande tvungen att vidta samma åtgärder för att kontrollera eventuellt olagligt material.

Vidare krävs för ansvar att förmedlaren haft uppsåt eller varit grovt oaktsam angående det olagliga meddelandet. Detta medför att den specifika brottsrubriceringen enligt vår mening får underordnad betydelse. Det blir således ingen större belastning för förmedlaren då han inte kan straffas för något han inte åtminstone inte varit grovt oaktsam till. Som exempel kan nämnas

[54] Palme, ”Ett misslyckat lagförslag”
[55] Josefsson, ”Fritt fram för rasism och barnporr på nätet i det nya lagförslaget”, artikel från Aftonbladet

förtalsbrotten vilka undantages från lagens tillämpningsområde. Det borde emellertid inte vara svårare för förmedlaren att upptäcka ett sådant brott. I praktiken sätts gränsen för vilka brott som omfattas vid förmedlarens kännedom om brotten. Detta borde, enligt vår mening, vara en följd av att samtliga brott skall inkluderas eftersom förmedlaren inte har något strikt ansvar.

Vi menar att bekämpningen av lagstridiga meddelanden skulle effektiviseras om istället samtliga brott omfattades. En tydlig, förutsebar reglering där samtliga brott inkluderas borde därför gynna förmedlaren framför en oklar reglering där endast ett fåtal brott innefattas. En sådan reglering torde även vara gynnsam för en effektiv brottsbekämpning. Idealet vore dock att helt avskaffa övervakningsskyldigheten.

En ytterligare svaghet med 5 § är att dess betydelse i praktiken, enligt vår mening, bör vara relativt begränsad. Vi ställer oss därför frågan om skyldigheten att hindra spridning av olagligt material, ur samhällelig synvinkel, utgör den mest effektiva lösningen på problemet med förekomsten av olagligt material på Internet. Det är idag väldigt lätt för en användare som blivit avstängd av en operatör att byta till en annan operatör. Ett praktiskt exempel där problemet aktualiseras är Netweasel-fallet. Netweasel blev polisanmäld av frilansjournalisten Victoria Wärmler, för förtal, ärekränkning och urkundsförfalskning då han bl a hade yttrat sig om henne i e-postmeddelanden och diskussionsinlägg. Förmedlaren, Swipnet, stängde av Netweasel med stöd av avtalet. Detta stoppade dock honom inte. Kort därefter var han tillbaka med ett nytt konto på Algonet. Detta exempel visar att avtalen ofta inte får eftersträvad genomslagskraft. Det är idag lätt för användare med illvilligt syfte att vända sig till en annan förmedlare. Tilläggas kan även att Netweasel inte är dömd för sina brott, åtalet lades ned eftersom det ej av särskilda skäl ansågs påkallat ur allmän synpunkt.[56]

3.4 SKADESTÅNDSRÄTTSLIGT ANSVAR

[56] http:www.kd.qd.se/safir/

Det skadeståndsrättsliga ansvaret ligger vid sidan av det straffrättsliga och aktualiseras i främst två olika fall. Båda dessa fall utgår från att det inte föreligger något avtal till grund för skadeståndsregleringen mellan parterna. Skadeståndslagen (SkL) är således tillämplig.[57]

Det första fallet relaterar till partsförhållandet mellan förmedlare och användare. En situation kan tänkas uppkomma där förmedlaren felaktigt avlägsnar ett meddelande från sin tjänst. Här föreligger således ett kontraktsbrott som utgör grund för ett skadeståndsyrkande. I praktiken regleras dock förmedlares skadeståndsansvar oftast i avtal mellan denne och användaren.[58] SkL blir då inte tillämplig. Endast i de fall avtalet inte berör skadeståndsregleringen mellan parterna kan de allmänna reglerna i SkL tillämpas. Beroende på vad som står i avtalet begränsas möjligheten för användare att få ut skadestånd.

Det andra fallet relaterar till ett annat partsförhållande, förhållandet mellan förmedlare och tredje man. Sprider exempelvis en användare ett meddelande vars innehåll utgör förtal skulle detta kunna föranleda ett skadeståndsanspråk gentemot förmedlaren. Huvudregeln i svensk rätt är att den som uppsåtligen eller av vårdslöshet vållar person- eller sakskada skall ersätta denna skada.[59] Ren förmögenhetsskada ersätts om den vållats genom brott.[60] De skador som uppkommer i IT-verksamhet utgörs oftast av rena förmögenhetsskador. Ersättning för ren förmögenhetsskada uppkommer endast om förmedlaren också kan åläggas ansvar enligt BrB eller LEA. Den skadelidande måste följaktligen visa att en brottslig handling begåtts. Ett utkrävande av ansvar bör vidare kräva att förmedlaren känt till meddelandets innehåll och karaktär innan det spreds. Till skillnad från fransk och brittisk praxis har en svensk förmedlare aldrig ålagts skadeståndsrättsligt ansvar för material förmedlaren inte känt till.[61]

I praktiken aktualiseras tredje mans rätt till skadestånd således endast i de fall denne lyckas bevisa att förmedlaren begått ett brott. Möjligheterna för den skadelidande att utkräva ansvar, av förmedlaren, enligt SkL får anses begränsade. Genom införandet av LEA har dock möjligheterna att erhålla ersättning ökat till viss del. Då denna lag genom skyldigheten att

[57] Hellner, ”Skadeståndsrätt”, s 21
[58] Se utförligare redogörelse i avsnitt 3.4.1.
[59] 2 kap 1 § SkL
[60] 2 kap 4 § SkL
[61] Anonym källa på Justitiedepartementet. Observeras bör dock att man i dessa länder har en mer generös inställning till ersättning för ren förmögenhetsskada än i svensk rätt.

plocka ned olagligt material, utvidgar förmedlarens straffrättsliga ansvar ökar samtidigt den skadelidandes möjlighet till ersättning för ren förmögenhetsskada.[62]

Vid sidan av SkL finns enstaka regler som fastslår ersättningsskyldighet för handlingar som inte är brottsliga. Det behöver således inte alltid finnas en direkt koppling mellan ersättningsskyldigheten för ren förmögenhetsskada och straffansvar. Exempel på en sådan regel, vilken i och för sig inte riktar sig mot den typiske användaren, är URL 54 § som reglerar skäligt vederlag till *rättighetsinnehavare.* Ersättningsskyldigheten uppkommer utan hänsyn till det subjektiva rekvisitet. Då ett intrång i upphovsrätten har skett finns det således möjlighet att kräva skadestånd oberoende av om förmedlaren har uppsåt till att intrång görs eller inte. Skadestånd utgår således oberoende av brott.[63]

3.4.1 REGLERING GENOM AVTAL

Reglering av skadestånd kan ske avtalsvägen. En analys av olika avtalstyper visar att en viss praxis har utformats på området. I syfte att begränsa förmedlares ansvar har man i avtalen så långt lagligen möjligt inskränkt möjligheterna för någon att rikta anspråk gentemot denne. Följande redogörelse tar utgångspunkt i två olika avtalsförhållanden.

3.4.1.1 Avtal mellan förmedlare och content provider

I detta avtal åtar sig förmedlaren att, för kundens räkning, göra viss information och vissa tjänster tillgängliga via Internet. Det finns ett standardavtal på området utformat av svenska IT-företagen: ”Elektroniska tjänster – Allmänna bestämmelser för elektroniska tjänster för publika nät” (Avtalet). Avtalet används mestadels av mindre förmedlare och har således fått mindre genomslagskraft än IT-företagens standardavtal på andra områden. De stora operatörerna har istället utformat egna standardavtal. Avtalet har dock troligen haft viss betydelse vid utformandet av dessa avtal.

---

[62] SOU 1996:40, s 190

[63] En liknande bestämmelse finns i 11 § Kretsmönstelagen men då denna lagstiftning enbart aktualiseras i mindre skala kommer den lämnas utanför denna framställning.

Avtalet utgår från att det finns tre olika aktörer: (1) Förmedlare (2) Content provider och (3) Användare. Förmedlaren förmedlar content providerns innehållstjänster till användaren. Avtalet är primärt avsett att reglera förhållandet mellan förmedlare och content provider, men kan även användas som utgångspunkt i förhållandet mellan förmedlare och användare.[64] Avtalet har begränsats till att inbegripa de tjänster som omfattas enligt LEA och är uppbyggt kring att denna lag är tillämplig på tjänsten. De ansvarsområden som LEA ålägger förmedlare har uttryckligen reglerats dem emellan. Content providern ansvarar bl a gentemot förmedlaren för att information som överförs eller hanteras via tjänsten inte utgör intrång i tredje mans rätt eller på något annat sätt står i strid mot gällande lagstiftning.[65] Vidare skall content providern ha uppsikt över tjänsten i den utsträckning som krävs enligt LEA. Rätten att efter underrättelse ta bort eventuellt olaglig information tillkommer emellertid förmedlaren.[66]

Ansvaret övervältras alltså på content providern som härigenom får överta flera av de betungande funktioner som LEA ålägger förmedlaren. Det är dock viktigt att påpeka att förmedlaren naturligtvis inte kan avtala bort sitt straffrättsliga ansvar. Gentemot tredje man ansvarar förmedlaren således helt i enlighet med de regler som stadgas i LEA. Obligationsrättsligt, d v s i avtalsrelationen mellan leverantör och content provider, kommer ansvarsfördelningen i avtalet emellertid att vara giltig. I de fall förmedlarens straffrättsliga ansvar aktualiseras har han således möjlighet att, med stöd av avtalet, vända sig mot content providern och hävda att denne inte fullgjort sina skyldigheter enligt avtalet varför kontraktsbrott föreligger.

Till skillnad från det straffrättsliga ansvaret är förmedlares skadeståndsrättsliga ansvar enligt SkL fullt möjligt att avtala bort. Långtgående begränsningar av detta ansvar har också gjorts i avtalet. Content providern åtar sig, att hålla förmedlaren skadelös från krav riktade från tredje man, som grundar sig på information som content providern ansvarar för.

3.4.1.2 Avtal mellan förmedlare och användare

[64] Westman och Lindberg, ”Praktisk IT-rätt”, s 373
[65] Se punkt 9 i Avtalet.
[66] Se punkt 9.5 i Avtalet.

I denna typ av avtal erbjuder förmedlaren en användare access och/eller tjänster på nätet. Numera är det nästan standard att man vid tecknande av abonnemang med en service provider även erbjuds lagringsutrymme för att kunna lagra sin egen webbsida på förmedlarens server. Som tidigare nämnts intar förmedlaren alltså två olika roller.[67] Någon uttalad bransch- eller rättspraxis på detta avtalsområde finns inte idag och något allmänt branschavtal existerar inte heller. Även här har dock samtliga stora svenska service providers egna standardavtal.

Vad gäller förmedlarens rättigheter respektive begränsningar i ansvaret är innehållet i stort detsamma i samtliga av de avtal vi studerat.[68] Avtalen kännetecknas av ansvarsbegränsningar för förmedlaren. Förmedlaren ansvarar oftast inte för någon direkt eller indirekt skada i anledning av tjänsten och tar inte heller ansvar för tredje mans uttalanden eller uppförande. Beroende på hur ingående förmedlaren har varit vid utformandet av användaravtalet begränsas rätten för användaren att få ut skadestånd. Samtidigt förbinder sig användaren, i flera fall att vid äventyr av avstängning, inte missbruka tjänsten.

Vidare förbehåller sig förmedlaren oftast en rätt att både ändra tjänsten samt att avsluta användarens konto. Flera förmedlare tar sig t ex rätt att stänga av ett konto i situationer där användaren underlåtit att ändra sitt beteende trots varningar om avstängning. De avtal som enbart reglerar tillhandahållande av en tjänst förefaller begränsa ansvaret mer långtgående än övriga avtal. Detta bör, enligt vår mening, vara en naturlig följd av den övervaknings-skyldighet som stadgas i LEA.

Amerikanska studier visar att en avstängning av ett konto, ur samhällelig synvinkel, utgör en relativt ineffektiv åtgärd.[69] I praktiken har användaren möjlighet att vända sig till en ny förmedlare i de fall kontot stängs av hos den första. Brottsliga meddelanden försvinner ej från nätet permanent utan kan återuppstå så fort avtal slutits med ny operatör. För förmedlare fungerar regleringen emellertid tillfredsställande då ansvar ej kan åläggas dem efter att användaren stängts av.

---

[67] Se avsnitt 2.2.
[68] Aktuella avtal som analyserats är avtal från Altavista, Yahoo Sverige, MSN, Everyday.com, Passagen, Utfors AB, HogiaNet, databasen Webbhotellet samt NU Internet.
[69] Rapport 1998-05-25, ”God etik på nätet”, s 74

Sammanfattning

Förmedlaransvaret kan delas in i ett straffrättsligt och ett skadeståndsrättsligt ansvar. De huvudsakliga problemen hänför sig till det specialstraffrättsliga området. Det skadeståndsrättsliga ansvaret regleras oftast genom avtal. Relevant lagstiftning får således underordnad betydelse.

4 SJÄLVREGLERING

4.1 INLEDNING

Den exakta innebörden av begreppet självreglering kan inte klart fastställas. Självregering uppkommer efter samarbete mellan förmedlare. Syftet med självreglering är att skapa ett förtroende på marknaden. Webbhotellet Flashback, vilket blivit svartlistat på grund av den information som fanns att hitta på tjänsten, utgör ett tydligt exempel där marknadens förtroende för webbhotellet ifrågasatts mot bakgrund av tjänstens innehåll.[70]

Genom självreglering skapas även en möjlighet för förmedlare att medverka till ett förtydligande av rättsläget. Ingen vill agera på en marknad där man inte riktigt vet vad som gäller. Förmedlare har ett mycket stort intresse av ett klargörande av det osäkra rättsläge som råder idag. Fördelarna med självreglering är att den är mer flexibel än vanlig lagstiftning eftersom den snabbt och smidigt kan anpassa sig till den tekniska utvecklingen samt de nya förhållanden som råder på Internet. Det är fråga om regler man gemensamt säger sig vilja anta varför de krav på precision och tydlighet som är relaterade till lagstiftningen inte aktualiseras. Det är viktigt att betona att det råder ett samband mellan lagstiftning och självreglering, där självregleringen är underställd lagstiftningen. Självregleringen fyller ut vissa luckor där lagen inte är riktigt specifik, exempelvis hur begrepp som ”god sed” eller ”god affärssed” skall definieras. Självregleringen kan bidra till ett mer substantiellt innehåll i själva lagstiftningen. För att uppnå effektivitet och klarhet krävs en struktur uppbyggd av både lagstiftning och

[70] Se avsnitt 3.2.

självreglering där ramarna sätts av lagstiftningen. Noteras bör dock att den utveckling och utformning som sker av marknaden bidrar till vissa svårigheter för en sådan reglering.[71]

4.2 PRAKTISK UTFORMNING

Självreglering sker, i det här fallet, ofta genom information och frivillig påverkan. Frivillig påverkan sker vanligtvis genom föreskrifter till nya användare, utfärdande av etikregler mm. Det finns ett flertal etikregelsamlingar vilka innehåller bestämmelser om exempelvis hur användare skall använda förmedlares erbjudna tjänster. Den mest innehållsrika och genomtänkta regelsamlingen utgör ”Netiquette Guidelines”. Reglerna som har utarbetats av IETF[72] är dock långa och detaljerade vilket gör dem svårlästa och komplicerade att tillämpa. Även inom EU pågår arbete för att stimulera självreglering.[73] Syftet är inte på något sätt att åsidosätta aktuella nationella regler utan ambitionen är istället att förmedlare, i samarbete, skall medverka till snabba och konkreta lösningar på förekommande problem.

Självreglering kan även ske genom ett ensidigt agerande från förmedlaren där denne t ex stänger av linjen för en kund eller raderar dennes meddelanden på ett webbhotell. Åtgärden sker på förmedlarens initiativ och utan inblandning av polis eller domstol. Flera förmedlare har upprättat s k ”*abusefunktioner*” där en användare som hittar material som bryter mot lag eller etikregler, via mail, kan göra en anmälan om detta. Abuse granskar det som anmälts samt tar ställning till om det utgör ett brott mot avtalet mellan kunden och operatören. Utgör materialet ett brott mot lagstiftning eller etikregler föreligger således ett kontraktsbrott varför kunden kan stängas av från tjänsten. I de fall materialet utgör ett lagbrott anmäls detta till polisen. Ett exempel på självreglering utgör det internationella samarbete som Usenet News utvecklat

---

[71] Konvergens mellan olika branscher blir idag allt vanligare. Med detta följer naturligtvis också ökade svårigheter att självreglera. Man kan endast självreglera sin egen bransch. Konvergensen bidrar emellertid till att det blir svårare att klart definiera vilka aktörer som ingår i den aktuella branschen. Här kan alltså uppstå vissa problem vad gäller utformandet av eventuell självreglering.

[72] Internet Engineering Task Force

[73] Se t ex ”Illegal and harmful content on the Internet” samt ”Green Paper on the protection of minors and human dignity in audiovisual and information services” där man behandlar frågan om hur användare skall kunna hindras från att åtkomma skadligt material. Inte bara tekniska lösningar, såsom filtrering, förespråkas utan även föräldraöversyn och hot lines etc tas upp. Vidare har en mer konkret handlingsplan för åren 1999-2002 utformats; ”Action plan on promoting safe use on the Internet”. Syftet med denna är att försäkra genomdrivandet av EU:s olika förslag för hur man ska handskas med skadligt material på Internet.

mellan olika förmedlare av newstjänster. Samarbetet består bl a av s k *death penalties* vilket innebär en möjlighet att stänga av dem på Usenet News som bryter mot allmänt accepterade etikregler. Reglerna utvecklas successivt och är mycket snävt utformade. Av hänsyn till yttrandefriheten ingriper man endast mot uppenbara missbruk. Självregleringen har visat sig effektiv och fungerar utmärkt trots att den inte understöds av lagstiftning. [74]

4.3 PROBLEM MED SJÄLVREGLERING

Yttrandefrihet contra effektiv brottsbekämpning

Genom självreglering har förmedlarna själva skapat en struktur för att beivra olika yttrandefrihetsbrott. En förmedlare har varken en domstols eller en myndighets uppgift att kontrollera att lagar följs. I praktiken är det dock förmedlaren som har störst möjlighet att inskrida och vidta effektiva åtgärder mot material som bryter mot lagar eller etikregler. Frågan är nu vad som väger tyngst; vår grundlagsskyddade yttrandefrihet eller en effektiv brottsbekämpning. Det finns de som menar att förmedlaren, när han vidtar olika tvångsåtgärder, tar över lagstiftarens roll genom att indirekt stadga inskränkningar i yttrandefriheten.[75] Som nämnts tidigare utgör webbhotellet Flashback ett tydligt exempel där detta problem aktualiseras.[76] Webbhotellet som har öppnats och stängts i flera omgångar på senare tid är alltså i nuläget stängt. Efter att ha vänt sig till flera av Sveriges operatörer som t ex Tele 1, Telenordia, Telia etc och fått kalla handen verkar det som Flashback tycks vara totalt svartlistad.[77] Frågan är om förmedlare, utifrån en egen moralisk bedömning, har rätt att neka användare access och svartlista dem på detta sätt. Det som har drabbat Flashback utgör, enligt vår mening, en naturlig följd av den osäkerhet som idag råder angående förmedlares ansvar. Här föreligger ett dilemma. Å ena sidan riskerar förmedlaren att anklagas för censur. Å

[74] Rapport 1998-05-25, ” God etik på nätet”, s 75-91

andra sidan riskerar han att när som helst pekas ut för att sprida barnpornografi och nazistpropaganda.

Flashbacks grundare Jan Axelsson har nu vänt sig till Konkurrensverket och hoppas på att saken skall tas upp i Marknadsdomstolen. Konkurrensverket ställer sig emellertid något avvaktande till fallet. I normala fall är det en konkurrent som stänger ute någon annan för att vinna ekonomisk fördel.[78] Så är dock inte fallet här och några rättsfall som klargör problemet finns inte heller.[79] Frågan om Flashbacks framtid är oviss. Problemet som inledningsvis endast gällde YGL:s tillämpning på Internet har övergått till att beröra konkurrensrättsliga aspekter. Att göra en djupare analys samt presentera en detaljerad lösning skulle falla utanför ramen för denna framställning. Vi har valt att enbart peka på samt kort beskriva de problem som aktualiseras. Som antyds ovan finns det två aspekter på problemet;

(a) Inskränkningar i vår grundlagsskyddade yttrandefrihet bör endast göras genom lagliga åtgärder av polis, åklagare och domstol. Går det inte till på detta sätt riskerar man att få ett sluttande plan där allt mer av politiskt inkorrekta åsikter riskerar att stoppas.
(b) Det ansvar som idag åvilar förmedlare av information och som bidrar till en effektiv brottsbekämpning. Se t ex LEA och det ansvar som åvilar förmedlare när olagliga meddelanden aktualiseras på deras tjänst.

Frågan är var gränsen skall dras mellan dessa intressen. Det finns flera gränsfall där det kan vara svårt att avgöra vilket intresse som väger tyngst. Ser man t ex på webbhotell så omfattas dessa av LEA, varför alternativ (b) borde gälla. Frågan är dock vad som gäller för de brott som inte omfattas av lagen. Vilka möjligheter har webbhotellägaren att ingripa mot ett meddelande som t ex utgör förtal? Vidare skall nämnas det fall där en network/ accessprovider enbart tillhandahåller nätverksaccess. Eftersom detta fall undantages från LEA:s tillämpningsområde

---

[75] Källa: Jakob Palme, professor
[76] Se avsnitt 3.2.
[77] http:// skolan.presstext.prb.se/bin/neta2gate?f=doc&state=25kngv.4.3
[78] Wierup, ”Flashbacks grundare vägrar backa”, artikel från Sydsvenskan
[79] Viss vägledning kan dock möjligen inhämtas från marknadsdomstolens dom MD 1999:18. Telia sa här upp flera konton vilka användes till 071-nummer vilka erbjöd inslag av våld av sex. Frågan avgjordes mot bakgrund

gäller alternativ (a). Ser man till verkligheten så innehåller emellertid, som redan påpekats, flertalet avtal mellan användare och förmedlare bestämmelser där förmedlaren ges en rättighet att avsluta abonnemanget i de fall användaren på något sätt bryter mot avtalet. Frågan är emellertid om aktuella avtalsklausuler kan anses juridiskt hållbara då de indirekt medför att förmedlaren avgör vad som omfattas av yttrandefriheten. Mot detta kan dock anföras principen om avtalsfrihet; parterna äger själva stor frihet att bestämma ett avtals innehåll. Accepterar en användare avtalet med förmedlaren är detta således giltigt dem emellan.[80] Möjligen skulle 36 § avtalslagen kunna anföras i enskilda fall.

Vi anser det angeläget att rättsläget omgående klargörs. Ingen kan idag säkert säga i vilken omfattning yttrandefrihet råder på Internet. Samtidigt är förmedlare dock under straffrättsligt ansvar skyldiga att ingripa mot eventuellt olagliga meddelanden. Detta förhållande kan medföra att förmedlare tillsammans sluter överenskommelser om vad som anses tillåtet respektive otillåtet att uttrycka på deras aktuella tjänst. Indirekt medför detta att förmedlare, istället för grundlagen, avgör yttrandefrihetens omfattning på Internet. Yttrandefriheten inskränks, i detta fall, på privaträttslig väg, något som enligt vår mening inte kan anses acceptabelt.

Telelagen

Rätten att stänga av användares konto har på vissa håll ifrågasatts såsom stridande mot telelagens kontraheringsplikt.[81] Detta verkar dock inte ha vunnit något allmänt gehör varför frågan endast kort berörs. Det råder osäkerhet om i vilken omfattning denna lag är tillämplig i detta fall.[82] Som stöd för att aktuella villkor skulle vara i strid mot lagen anges flera generella bestämmelser. Som exempel kan nämnas 2 § där det stadgas att alla skall få tillgång till telefonitjänster på lika villkor samt 15 § där det anges att var och en som efterfrågar tjänsten skall få tillgång till den. Det kan dock ifrågasättas om man kan stödja sig mot nämnda bestämmelser i det här fallet. 30 § är den enda regel som direkt berör frågan om avbrytande av tjänst. I 30 § stadgas att tillhandahållandet av tjänst får avbrytas om kunden inte betalar i rätt

---

av konkurrenslagen. Telias agerande ansågs vara legitimt. Frågan om prövning gentemot Telelagen togs aldrig upp i målet vilket eventuellt antyder att agerandet är i överensstämmelse med denna lag.

[80] Principen om avtalsfrihet balanseras i viss mån av kontraheringsplikt då avtalsvägran i en del fall ej accepteras. Vi anser dock detta falla utanför framställningens ram.

[81] Se t ex Rapport 1998-05-25, ”God etik på nätet s 74

tid. Frågan är dock om denna paragraf över huvud taget är tillämplig eftersom den grundar sig på en regel i ett direktiv som inte anses omfatta Internet.[83]

5 TEKNISKA ÅTGÄRDER

Det finns, genom att använda sig av tekniska åtgärder, möjlighet för förmedlare att hindra spridning av olagligt material. Vi är medvetna om att detta till viss del ligger utanför framställningen, men då dessa åtgärder har visat sig ha stor betydelse i praktiken, har vi ändå valt att kort redogöra för dem.

5.1 TEKNISK FILTRERING

Som redan påpekats är det ofta väldigt svårt att identifiera den som begått en brottslig gärning på Internet. Möjligheterna att hitta den ansvarige är dock beroende av hur beräknande och tekniskt kunnig personen är. Om en person en enstaka gång lägger ut olaglig information är han i stort sett omöjlig att spåra. Lägger han emellertid vid ett flertal tillfällen ut information på samma sätt är det lättare att hitta honom. När man lägger ut olagligt material och inte önskar bli spårad skall man gå flera steg i taget. Genom att koppla upp sig mot en dator i t ex USA som är kopplad till en dator i Australien som är kopplad till en dator i Sverige minskar man möjligheterna att bli spårad avsevärt. För att identifiera gärningsmannen i sådana fall måste man gå samma väg tillbaka, alla steg. Vidare krävs ett samarbete mellan de inblandade länderna där man först går till USA, sedan Australien och slutligen Sverige.[84]

Tidigare i framställningen har endast redogjorts för de rättsliga möjligheter som finns att avlägsna brottsliga meddelanden på Internet. Det finns dock även möjlighet att på teknisk väg bekämpa en spridning av sådana meddelanden. Genom teknisk filtrering granskar datorn själv dokument för att sedan sortera eller välja ut dem åt användaren. Det finns flera olika typer av teknisk filtrering. Genom personlig filtrering, för en enda person eller för en grupp av personer,

---

[82] Rapport från Post & Telestyrelsen 1999-10-08, ” Telelagen och Internet”
[83] Källa: Jurist på Post & Telestyrelsen
[84] Rapport 1998-05-25, ” God etik på nätet”, s 71

kan man med hjälp av ett filter hitta det som man tycker är mest intressant. Teknisk filtrering kan vidare användas för att hindra vissa personer att ta emot speciella dokument. Det kan t ex vara ett land som vill hindra folk att läsa ”statsfientliga dokument” eller en förmedlare som vill undvika åtal enligt LEA.

När det gäller denna typ av filtrering skall man dock vara medveten om vad tekniken medger och inte medger. Datorer är inte bra på att göra nyanserade bedömningar. Teknisk filtrering kan således inte avgöra vad som är rätt och fel, lämpligt och olämpligt, etiskt och oetiskt. En dator kan inte analysera en text för att avgöra vad som är olagligt och lagligt. Det går t ex inte att installera ett program som kan upptäcka om en bild är pornografisk eller inte. Ett sådant program kan resultera i oönskade effekter som t ex att information om bröstcancer felaktigt filtreras bort.

5.2 SOCIAL FILTRERING

En variant av filtrering utgör social filtrering. Social filtrering bygger på att människor har värderat meddelanden och lagrat sin värdering i datorn. Det kan t ex vara författare som sätter märken på sina egna meddelanden. Det kan också vara andra personer som lägger upp databaser av märkningar av meddelanden som sedan används för filtrering. Till skillnad mot teknisk filtrering är det här möjligt att avgöra vad som är rätt och fel eller lagligt och olagligt. Ett exempel på där social filtrering används är de företag i USA som erbjuder olika typer av program för att föräldrar skall kunna hindra barn att få tag på viss information som pornografi och våldsskildringar. Företagen bygger upp databaser över olämpliga dokument och dokumentsamlingar. Mest kända för att bedriva social filtrering är Yahoo. Företaget fungerar ungefär som en tidning med en redaktör som väljer ut och släpper in enbart sådant material som han anser vara bra. Användaren kan markera sina egna objekt. Detta tillvägagångssätt har visat sig fungera mycket väl när det gäller pornografiska meddelanden. Enligt amerikansk lagstiftning är det i vissa delstater olagligt att sända pornografi till någon som inte har begärt

det. För att undvika åtal väljer därför porrproducenterna att tydligt märka sina meddelanden. Märkningarna kan sedan användas för filtrering.[85]

6 E-HANDELSDIREKTIVET 2000/31/EG

De oklarheter som råder angående förmedlares ansvar har uppmärksammats på EU-nivå. I syfte att uppnå en harmonisering av medlemsstaternas lagstiftning på området har flera rättsakter utformats. Bl a är ett direktiv om harmonisering av delar av upphovsrätten och närstående rättigheter under utarbetande.[86] E-handelsdirektivet syftar bl a till att fastställa klara regler för förmedlarens ansvar vid upphovsrättsintrång.[87] Vidare har ett direktiv om elektronisk handel utformats.[88] E-handelsdirektivet behandlar flera rättsfrågor relaterade till elektronisk handel. Bakomliggande ändamål är effektivitetshänsyn samt en strävan efter en djupare marknadsintegration. Genom en enhetlig reglering söker man således öka rättssäkerheten för de enskilda aktörerna. E-handelsdirektivet har utformats i syfte ”att se till att informationssamhällets tjänster till fullo skall kunna utnyttja den inre marknadens regler om fri rörlighet för tjänster och etableringsfrihet samt att tjänsteleverantörer skall kunna tillhandahålla sina tjänster inom hela EU utan rättsliga hinder”.[89] En informationssamhällets tjänst inbegriper näst intill alla tjänster på Internet. Samtliga tjänsteleverantörer omfattas av e-handelsdirektivet.[90] Till skillnad från LEA inbegrips renodlade network providers och access providers.

Mest centrala för denna uppsats är ansvarsbegränsningarna i artiklarna 12 till 15. Artiklarna har huvudsakligen utformats under vägledning av amerikansk lagstiftning och praxis.[91] Vidare har 1997 års tyska Multimedialag tjänat som förebild.[92] I likhet med sistnämnda lag gäller artiklarna i alla former av potentiellt civilrättsligt och straffrättsligt ansvar. Ansvarsfrihet kan

[85] Rapport 1998-05-25, ”God etik på nätet”, s 70-74
[86] Rådets föreslagna direktiv om harmonisering av vissa aspekter av upphovsrätt och närstående rättigheter i informationssamhället.
[87] Preambel p 50, e-handelsdirektivet
[88] Europaparlamentets och rådets Direktiv 2000/31/EG av den 8 juni 2000
[89] Meddelande från Kommissionen till Europaparlamentet enligt artikel 251.2, 2 st EG-fördraget, 1998/0325 (COD)
[90] Uttrycket ”tjänsteleverantör” är en direkt översättning av den engelska samlingsbeteckningen service provider.
[91] Delar av the Digital Millennium Copyright Act har fungerat som en direkt förlaga till artiklarna.

således aktualiseras vid flertalet, enligt nationell rätt, kriminaliserande och skadeståndsgrundande handlingar. Det faktiska ansvaret förutsätts vara reglerat på nationell nivå. Något som till viss del kan verka underligt med tanke på att denna fråga förefaller högst oklar i flertalet medlemsstater. Behovet av en reglering på gemenskapsnivå intensifierades dock efter att europeiska, nationella, domstolar på olika sätt, genom följande tre rättsfall, utvidgat förmedlares straff- och/eller skadeståndsrättsliga ansvar.[93]

6.1 LAURENCE GODFREY - AND - DEMON INTERNET LIMITED[94]

Fallet Laurence Godfrey and Demon Internet Limited, hämtat ur brittisk rättspraxis, föranledde att en förmedlare fick betala skadestånd för förtalsbrott. Brottet bestod i att en privatperson i USA hade postat material, på Internet, innehållande förtal mot en forskare, Laurence Godfrey, på Demon Internets server. Godfrey påtalade detta tre gånger men då materialet inte togs ned valde han att gå till domstol. Demon Internet hävdade till sitt försvar att de såsom förmedlare inte hade kontroll över vad individer postade. Man hänvisade särskilt till det amerikanska rättsfallet Cubby v. Compuserve[95] där förmedlaransvaret fastslogs vara begränsat och inte omfatta förtalsbrott. Domaren valde dock att stödja sin argumentation på the Defamation Act 1996.[96] Här stagas att förmedlaren kan hållas ansvarig för förtal i de fall ett *primärt ansvar* för informationen kan utrönas.[97] Bestämmelsen har vidare tolkats så att förmedlaren har bevisbördan för att denne inte hade uppsåt till spridningen av det olagliga meddelandet.[98]

---

[92] Informations- und Kommunikationsdienste Gesetz
[93] Anonym källa på Justitiedepartementet
[94] Case No: 1998-G No 30, Royal Courts of Justice Strand, London, WC2A 2LL, 1999-03-26
[95] Se närmare redogörelse i avsnitt 7.1.
[96] Åsikter har framförts om att den brittiska regleringen, till skillnad mot den amerikanska, gör lite för att erkänna Internet som ett nytt medium. Lagen är vidare utformad utan samarbete med operatörer. Tanken är dock att lagen skall vara dagsaktuell och oberoende av vilken teknologi som används. Lagen är således tillämplig även på material publicerat på Internet.
[97] Defamation Act 1996, section 1 ”Respnsibility for publication”
[98] Jämför exempelvis med USA där denna bevisbörda läggs på användaren.

Demon Internet ansågs ha haft ett primärt ansvar då de faktiskt haft möjlighet att utplåna aktuella meddelanden.[99] Förmedlares ansvar utvidgas här avsevärt eftersom domstolen menar att ett primärt ansvar omfattar sådant som tredje man har gjort. Demon Internet lyckades inte heller visa att de inte hade uppsåt till det olagliga meddelandet. Hänvisningen till det amerikanska rättsfallet var alltså utan framgång. Enligt domaren illustrerade detta fall endast skillnaderna i angreppssätt mellan de båda rättsordningarna.[100] Frågan är om denna skillnad kan vidhållas i brittisk rättspraxis eftersom e-handelsdirektivet till stor del har utformats mot bakgrund av amerikansk rätt. En anpassning till e-handelsdirektivet måste således ske. Av denna anledning inkom inte heller Demon Internet med någon överklagan. Ett prejudikat grundat på oförändrad lagstiftning var inte önskvärt. På grund av förväntningarna om en ändring av rättsläget kan detta fall troligtvis inte tillmätas något framtida prejudikatvärde.[101]

6.2 COMPUSERVE GMBH[102]

Även tysk rättspraxis visar exempel på att förmedlare kan ådömas ansvar på ett betungande sätt. I detta fall ålades verkställande direktör för Compuserve GmbH, Felix Somm ett *straffrättsligt* ansvar då barnpornografi förekommit på dess servrar. Compuserve GmbH försåg tyska användare med access till det amerikanska moderbolaget Compuserve Incs newstjänster. Somm fick 1995 meddelande om att det förekom barnpornografi på flera av newstjänsterna. Han kontaktade då moderbolaget och bad dem avlägsna eller förhindra åtkomst till aktuella tjänster. Åtgärder vidtogs snabbt. Först gick man till och med så långt att åtkomst förhindrades till *alla*, 282, newstjänster. Då inte alla hade innehållit barnpornografi bestämde man sig emellertid för att öppna övriga newstjänster igen. För säkerhets skull försågs även tyska användare med tekniskt filtreringssystem vilket möjliggjorde för föräldrar att blockera aktuellt innehåll. Systemet fungerade dock inte tillfredsställande och barnpornografi dök återigen upp

[99] Domskälen p 35
[100] Domskälen p 40
[101] BBC NEWS, http://news.bbc.co.uk/hi/english/sci/tech/newsid_364000/364261.stm
[102] Amstgericht Munchen 8340 Ds 465 Js 173158/95, 28 Maj 1998

på servrarna.[103] Somm dömdes till fängelse för spridande av barnpornografi. Domaren ansåg att han, tillsammans med moderbolaget, avsiktligen underlåtit att radera material innehållande barnpornografi. Uppsåtet låg i att det de facto funnits barnpornografi på newstjänsterna.[104] Enda sättet att undvika ansvar hade enligt domaren varit att stänga ner servrarna helt alternativt blockera all access till dem.[105] Ett misslyckat försök kunde således inte fria från ansvar.

Domaren valde att tillämpa Multimedialagen. Förmedlares ansvar berörs i artikel 1, ”Teledienstgesetz” (TDG).[106] I 5 § TDG stadgas att förmedlare endast har ett uttryckligt ansvar för *eget material*.[107] Vid förmedling av information har man istället valt att införa en ansvarsbegränsning relaterad till uppsåt. Ansvar kan således inte göras gällande för andras innehåll som förmedlaren tillgängliggör om inte vetskap finns om detta innehåll. Ett utkrävande av ansvar kräver vidare att det skall finnas teknisk möjlighet att blockera innehållet.[108] Domaren ansåg att Somm hade vetskap om det olagliga innehållet. För rena accesstjänster går förmedlaren helt fri från ansvar.[109] Domslutet kan således ifrågasättas då det även går att argumentera för att Compuserve GmbH endast tillhandahöll access. Osäkerhet om var skiljelinjen mellan eget material och annans material skall dras tycks föreligga. I detta fall fanns inte newstjänsterna på Compuserve GmbH:s servrar varför inte heller innehållet borde kunnat härledas till dem. Domen överklagades och i högre domstol frikändes Felix Somm.

6.3 ALTERN

[103] Det är oklart om bristerna i filtreringen kan hänföras till själva systemet eller om de som lade ut barnpornografiskt material visste ett sätt att ta sig runt filtreringen.
[104] Ett brott mot spridning av barnpornografi, sektion 184(3)Tyska Brottsbalken
[105] Nathrath, ”Criminal liability of Internet Providers in Germany: Conviction of a Compuserve Executive”, artikel från Journal of Internet Law
[106] TDG är inlagd som en del av Multimedialagen.
[107] 5 (1)
[108] 5 (2)
[109] 5 (3)

Det franska fallet Altern rörde nakenbilder på en modell, Estelle Hallyday. Bilderna som fanns att hitta på en av Alterns 47 000 fria webbsidor hade lagts dit av en användare.[110] Då bilderna ansågs kränkande stämde Hallyday Alterns ägare, Valentin Lacambre. Lacambre ålades att betala skadestånd samt blockera tillgången till bilderna. Domstolen motiverade sitt ställningstagande med att förmedlare har en skyldighet att garantera moralen hos sina användare.[111] Domen antyder att en förmedlare är ansvarig för allt material på tjänsten oavsett omständigheterna i det enskilda fallet.[112] Ingen eftergift gavs efter överklagan. Med tilläggsmotiveringen att tjänsten tillät helt anonyma meddelanden fastslog således Paris Court of Appeals det tidigare domslutet.[113] Betydelsen av denna motivering, kan enligt vår mening, starkt ifrågasättas eftersom användarens identitet lätt kunde röjas. Detta uppmärksammades dock inte från något håll utan ansvarsfrågan riktades enbart mot förmedlaren. Vi ställer oss vidare frågande till varför Hallyday valde att enbart rikta sig mot Altern istället för att stämma den person som lagt ut bilderna.

Till skillnad från föregående två fall fanns här ingen lagstiftning anpassad till Internet. Frankrike har tidigare över huvud taget inte engagerat sig för att skapa någon nationell lagstiftning på detta område.[114] Först i juni 2000 antogs en lag, the Freedom of Communications Bill, för reglerande av förmedlares ansvar. Lagen undantar access providers helt från ansvar. Deras enda skyldighet är att erbjuda användare tillgång till tekniska möjligheter, utarbetade i syfte att förhindra åtkomst till specifika webbsidor. Även för hosting service providers begränsas ansvaret. Ansvar kan endast utkrävas i de fall de underlåter att, i enlighet med domstols beslut, blockera access till Internetsiter alternativt underlåter att avlägsna material tredje man anmält såsom olagligt.[115]

6.4 E-HANDELSDIREKTIVET ARTIKLARNA 12-15

[110] ”Court cases regrding ISP liability”, http://webreview.com/wr/pub/1999/04/23/platform/cases.html
[111] http://www.cyberlaw.se/swedish/elaw-1.htm
[112] ”Court cases regrding ISP liability”, http://webreview.com/wr/pub/1999/04/23/platform/cases.html
[113] http://www.cyberlaw.se/swedish/elawi-10.htm
[114] Mayer, ”Europé and the Internet The Old World and the New Medium””, artikel från European Journal of International Law
[115] Linklaters & Alliance, s 5

Artiklarna 12-15 fastslår begränsningar i förmedlares ansvar. Ansvarsbegränsningarna är utformade så att de är relaterade till specifika aktiviteter/funktioner, såsom tillhandahållande av teknik för vidarebefordran (mere conduit), automatisk, temporär och mellanliggande lagring (caching) samt varaktig lagring (hosting service), snarare än aktörskategorier.[116] En aktör som tillhandahåller en stor mängd tjänster, av vilka endast ett fåtal faller inom definitionerna i artiklarna 12-15, kan följaktligen fortfarande dra viss fördel av ansvarsbegränsningarna. Detta gäller dock endast i förhållande till de tjänster som är uttryckligen undantagna från ansvar. Ett exempel för att förtydliga: En förmedlare erbjuder Internet access, lagring och en sökmotor. Ansvarsbegränsning kan då ges för tillhandahållandet av access samt lagringstjänster men inte för tillhandahållandet av länkar genom sökmotorn.[117] Erbjudandet av sökmotorer faller i dagsläget inte inom något av de undantag som e-handelsdirektivet ställer upp.[118] Att söktjänster inte omfattas beror troligtvis på att tjänsten är helt automatisk utan att någon kontroll av innehållet sker. Användaren får genom söktjänsten endast tillgång till material som redan är utlagt på nätet. Förmedlarens tjänst tillför således inte något nytt innehåll. Det tycks förutsättas att medlemsstaterna inte ålägger förmedlare ansvar i sådana situationer. Möjligen har det av denna anledning ansetts onödigt att reglera denna tjänst i e-handelsdirektivet.[119]

Ansvarsbegränsningarna har tillkommit då ett för tungt ansvar på förmedlaren anses medföra orimliga krav på denne vad gäller kostnad i tid och pengar. Dessa kostnader riskerar sedan att övervältras på användarna vilket i sin tur kan hämma den tekniska utvecklingen.[120] Förmedlarnas ansvar begränsas till en nivå som är i överensstämmelse med deras roll på marknaden samt deras praktiska möjligheter till kontroll. Förmedlare skall inte heller åläggas en skyldighet att förhandsgranska alla de meddelanden som tillgängliggörs genom tjänsten.[121]

---

[116] Även LEA är utformad i relation till specifika aktiviteter/funktioner.
[117] Vinje och Paemen, "The European Union's Electronic Commerce Directive: New rules on On-line Advertising, E-contracting, ISP Liability and Dispute Resolution", s 251, artikel från World Intellectual Property Report
[118] Artikel 21 uppmärksammar dock avsaknaden av reglering vad gäller ansvaret för leverantörer av hypertextlänkar, sökverktyg etc. och ambitionen är att en harmonisering skall ske även här framöver.
[119] Källa: Mattias Klang, vik adjunkt.
[120] Kelleher, "IT-law in EU", s115
[121] I Sverige åläggs förmedlare med stöd av 4 samt 5 §§ LEA en skyldighet att förhandsgranska allt material som förmedlas via deras tjänster. Se utförligare redogörelse i avsnitt 3.3.4.2.

Skyldighet att kontrollera och bevaka kunders material i förväg anses utgöra ett orimligt krav på förmedlaren.[122]

Genom artiklarna 12-14 söker man underlätta möjligheterna för förmedlare att utforma sin verksamhet så att de på ett effektivt sätt kan förebygga olagliga meddelanden på sin tjänst. Ett exempel på detta är notice and takedown, vilket regleras i artiklarna 13 och 14. Tillvägagångssättet möjliggör för användare att påtala brottsliga meddelanden. Användaren meddelar förmedlaren, via en lättillgänglig kontaktperson, om det olagliga materialet varefter det kan avlägsnas alternativt blockeras utan dröjsmål. Idén är att artiklarna skall ligga till grund för utarbetande av snabba, tekniska förfaranden vid avlägsnande av sådana meddelanden. E-handelsdirektivet hindrar emellertid inte förmedlarna från att själva utveckla och använda tekniska system för skydd och identifiering.[123]

6.4.1 ARTIKEL 12 (Enbart vidarebefordran (”mere conduit”))

1. Medlemsstaterna skall se till att en tjänsteleverantör som levererar en informationssamhällets tjänst bestående av överföring i ett kommunikationsnät av information som lämnats av tjänstemottagaren, eller tillhandahållande av tillgång till ett kommunikationsnät, inte skall vara ansvarig för den överförda informationen under förutsättning att tjänsteleverantören

a) inte initierat överföringen

b) inte valt ut mottagaren av den överförda informationen, och

c) inte valt ut eller ändrat den information som överförts

2. Överföringen och tillhandahållande av sådan tillgång som avses i punkt 1 omfattar automatisk, mellanliggande och tillfällig lagring av den vidarebefordrade informationen, i den mån lagringen enbart görs för att utföra överföringen i kommunikationsnätet och under förutsättning att informationen inte lagras längre än vad som rimligtvis krävs för överföringen.

3. *Denna artikel skall inte påverka möjligheten för en domstol eller administrativ myndighet att i enlighet med medlemsstaternas rättssystem kräva att tjänsteleverantören upphör med eller förhindrar överträdelse.*

Artikel 12 fastslår att medlemsstaterna inte får ålägga förmedlare straff- eller skadeståndsrättsligt ansvar för sådan information som de inte själva kan kontrollera.[124] Undantaget omfattar endast fall där förmedlarens verksamhet är begränsad till den tekniska processen och där det alltså enbart sker en vidarebefordran av information. Då förmedlarens uppgift endast är att effektivisera överföringen av information är det inte heller möjligt för denne att ha någon kännedom eller kontroll över informationen.[125] Denna artikel överensstämmer med 2 § LEA i det avseendet att network/accessproviders även här är undantagna från ansvar. Artikeln får

[122] ETNO Reflection Document on Jurisdiction and Applicable Law in E-Commerce, RD108 11/99
[123] Preambel p 40, e-handelsdirektivet
[124] Prop 99/00:86

således mindre betydelse för svensk rätt då ansvarsfrihetsgrunden redan är inskriven genom undantaget i LEA. Endast för brott som inte omfattas av LEA kan artikeln få relevans.

Artikel 12 är inte tillämplig då förmedlaren handlat med uppsåt i förhållande till eventuellt olaglig information. Är förmedlaren på något sätt aktiv, genom att t ex kontrollera vidarebefordrat material, samt handlar med uppsåt medger e-handelsdirektivet att nationell lagstiftning föreskriver ansvar.

6.4.2 ARTIKEL 13 (Caching)

1. *Medlemsstaterna skall se till att en tjänsteleverantör som levererar en informationssamhällets tjänst bestående av överföring av information som tillhandahållits av tjänstemottagaren på ett kommunikationsnät inte skall vara ansvarig för den automatiska, mellanliggande och tillfälliga lagring av informationen som ägt rum enbart för att effektivisera vidare överföring av informationen till andra tjänstemottagare på deras begäran, under förutsättning att*

a) *tjänsteleverantören inte ändrar informationen,*
b) *tjänsteleverantören uppfyller villkoren för tillgång till informationen,*
c) *tjänsteleverantören följer regler för uppdatering av informationen, vilka fastställts på ett sätt som är allmänt vedertaget och använt inom branschen,*
d) *tjänsteleverantören inte ingriper i den lagliga användningen av den teknik som är allmänt vedertagen och som används inom branschen för att få fram data om hur informationen används, och*
e) *tjänsteleverantören handlar utan dröjsmål för att kunna avlägsna den information han har lagrat eller göra den oåtkomlig så snart han fått kännedom om att den information som ursprungligen överfördes har avlägsnats från nätet eller gjorts oåtkomlig, eller att en domstol eller administrativ myndighet har bestämt att den skall avlägsnas eller göras oåtkomlig.*

2. *Denna artikel skall inte påverka möjligheten för en domstol eller administrativ myndighet att i enlighet med medlemsstaternas rättssystem kräva att tjänsteleverantören upphör med eller förhindrar överträdelse.*

Kortfattat utgör caching en automatisk, tillfällig och mellanliggande lagring av information som äger rum enbart för att effektivisera vidare överföring. Är exempelvis en site på en amerikansk server populär bland svenska Internetanvändare kan en cache-kopia skapas på en svensk server. Istället för att gå hela vägen över nätverket till den amerikanska servern kan då istället innehållet nås på den svenska. Processen är helt automatisk. Vid ett visst antal träffar skapar servern på egen hand en tillfällig kopia. Någon mänsklig inblandning förekommer inte över huvud taget. Det råder oenighet om cache-kopior kan anses utgöra olaglig exemplarframställning enligt URL.[126] Problemet är idag föremål för en het debatt. En närmare redogörelse faller dock utanför uppsatsens syfte varför vi nöjer oss med att enbart peka på problemet. Oenigheten rör främst om den tidsmässiga längden på lagringen skall tillmätas stor

[125] Preambel p 42, e-handelsdirektivet

betydelse eller om större vikt skall fästas vid om informationen finns kvar eller ej när datorn stängs av. Det råder enighet om att en kopia skapas vid caching men då den endast är tillfällig anser somliga att den är för osjälvständig för att föranleda ett upphovsrättsligt ansvar.

Artikelns betydelse har främst hänförts till det upphovsrättsliga området. För svensk rätts del medför det att artikeln troligen endast kommer aktualiseras om caching omfattas av exemplarframställning och ett upphovsrättsintrång således kan begås.

Skillnaden mellan artikel 13 och artikel 12 markeras i andra punkten i artikel 12. I de fall lagringen varar längre än nödvändigt för överföringen så omfattas denna troligtvis istället av ansvarsbegränsningarna i artikel 13. Ansvarsfrihet enligt artikel 13 förutsätter att ett flertal krav är uppfyllda. Bland annat krävs att förmedlaren genom notice and takedown snarast, efter att ha fått *kännedom* om eventuellt olagligt material, avlägsnar eller blockerar detta. Här förutsätts således, för att artikeln skall bli tillämplig, att förmedlaren handlat utan uppsåt.

6.4.3 ARTIKEL 14 (värdtjänster)

1. Medlemsstaterna skall se till att en tjänsteleverantör som levererar någon av informationssamhällets tjänster bestående av lagring av information som tillhandahållits av tjänstemottagaren inte skall vara ansvarig för information som lagrats på begäran av en tjänstemottagare av tjänsten, under förutsättning att

a) tjänsteleverantören inte hade kännedom om förekomsten av olaglig verksamhet eller olaglig information och, beträffande skadeståndsanspråk, inte var medveten om fakta eller omständigheter som gjort förekomsten av den olagliga verksamheten eller den olagliga informationen uppenbar, eller

b) tjänsteleverantören så snart han fått sådan kännedom eller blivit medveten om detta handlat utan dröjsmål för att avlägsna informationen eller göra den oåtkomlig.

2. Punkt 1 är inte tillämplig om tjänstemottagaren handla under tjänsteleverantörens ledning eller överinseende.

3. *Denna artikel skall inte påverka möjligheten för en domstol eller administrativ myndighet att i enlighet med medlemsstaternas rättssystem kräva att tjänsteleverantören upphör med eller förhindrar en överträdelse, inte heller skall den påverka medlemsstaternas möjlighet att inrätta förfaranden för att avlägsna information eller göra den oåtkomlig.*

Även vid lagring av information under en längre tid, t ex lagring av webbsidor på ett webbhotell eller information på en BBS, föreskriver e-handelsdirektivet ett begränsat max-ansvar. Informationen lagras för användarens räkning och på dennes begäran och förmedlaren fungerar följaktligen som en värd för denna information. Artikeln tar således sikte på samma tillämpningsområde som LEA. Till skillnad från övriga artiklar skiljer man i artikel 14 på det skadeståndsrättsliga och det straffrättsliga ansvaret. Straffrättslig ansvarsfrihet kan således åtnjutas om förmedlaren inte har *kännedom* om eventuella olagligheter. Vidare undgår denne ett

[126] Enligt prop 1996/97:111, s 32 samt 36, tycks detta falla utanför exemplarframställan. En annan åsikt föreligger dock i doktrin där exemplarframställning anses ske så fort information som funnits på servern kan

skadeståndsrättsligt ansvar i de fall han inte är *medveten* om fakta eller omständigheter som medför att olagligheten framstår som uppenbar. Liksom i artikel 13 stadgas i artikel 14 en möjlighet att undgå ansvar genom att avlägsna information. Så fort förmedlaren fått kännedom om eller blivit medveten om en eventuellt olagligt meddelande skall det således avlägsnas eller blockeras. Gör förmedlaren det, så får inte medlemsstaterna föreskriva straff- eller skadeståndsansvar.

6.4.3.1 Notice and takedown

Notice and takedown innebär att användare ges möjlighet att anmäla olagligheter på Internet till förmedlare. Denna anmälan skall sedan föranleda ett snabbt avlägsnande/blockerande av materialet. Tillvägagångssättet har vid bekämpning av brottsliga meddelanden visat sig effektivt och har fått stor genomslagskraft. Amerikansk lagstiftning har tjänat som inspira-tionskälla.[127] Av någon anledning, som inte motiveras någonstans, har dock endast vissa delar av regleringen använts. E-handelsdirektivet fastslår enbart en skyldighet att *avlägsna/blockera* eventuellt olagligt material. Övrig vägledning för hur denna avlägsning/blockering skall gå till saknas således. Vi anser att övriga delar bör beaktas för att ett tillfredsställande resultat skall kunna uppnås.[128] I e-handelsdirektivet finns ej någon bestämmelse som anger hur anmälan skall se ut. Då tydlighet är viktigt för förmedlare bör således meddelandet bl a innehålla vem som utgör anmälare samt vilken lag man anser att informationen bryter mot. Vidare anges inte heller någon begränsning i anmälarkretsen. Blir detta en möjlighet för alla, vilket tycks vara fallet, riskerar förmedlare, enligt vår mening, att överhopas med krav på nedtagande av material.

Möjligen hade det kanske varit lämpligt att låta ett offentligt organ, t ex en reklamationsmyndighet, få ta ansvar för kontakten med förmedlaren.[129] Privatpersoner kunde således vända sig till detta organ för att påtala eventuella olagligheter. Tillvägagångssättet leder till att juridiskt kunniga och följaktligen mer lämpliga personer fattar beslut om ett meddelandes lagenlighet. Förmedlare har inte alltid den juridiska kunskap som krävs för att ta

---

användas för att återskapa ett verk.
[127] Title II 17 U.S.C DMCA, 1998
[128] Exempelvis stadgas i den amerikanska lagstiftningen klara regler för hur anmälan skall se ut, vad den skall innehålla, vem som får anmäla samt vad som händer i de fall en felaktig nedtagning sker.

ställning till om något faktiskt bör tas bort. Vidare kan tyckas att detta organ bör ta på sig såväl förmedlares som anmälares eventuella skadeståndsrättsliga ansvar vid en felaktig nedtagning. E-handelsdirektivet tiger om vad som händer i de fall nedtagningen skett oberättigat. Nackdelen är dock den ökade byråkrati detta förfarande medför, samt ökade kostnader på samhället. Alternativet är att kostnaderna istället, genom lag, läggs på förmedlare som avtalsvägen får begränsa sitt ansvar samt skapa klarhet i situationen. Rimligtvis bör då detta ske genom en ansvarsfriskrivning både gentemot content provider och anmälare. Om anmälare uppmanas att tydligt, i anmälan, förklara sig ta ansvar för en eventuellt felaktig anmälan, och content providers uppmärksammas på detta, undviker förmedlaren ett skadeståndsanspråk. Skadeståndsanspråket riktas istället direkt från content provider till anmälare. Viktigt är dock anmälans tydliga utformning så att det ej kan råda tvekan om anmälares ansvarsåtagande.

Med den osäkerhet som idag föreligger angående förmedlares ansvar intensifieras risken att helt lagenliga meddelanden avlägsnas. I e-handelsdirektivet finns inga begränsningar i förmedlarens skyldighet att avlägsna olagliga meddelanden. E-handelsdirektivet reglerar således varken hur en bedömning av eventuella olagliga meddelanden skall ske eller vem som ansvarar vid en felaktig nedtagning. Frågan vad som gäller när en förmedlare tar ett felaktigt beslut kvarstår således. Då syftet med e-handelsdirektivet är att skapa en gemensam reglering för att öka förutsebarheten för förmedlare kan det tyckas konstigt att inte denna situation har berörts. Det finns alltså ett stort utrymme för medlemsstaterna att ha differentierade regler. Ett generellt stadgande om att förmedlare ej ansvarar för felaktiga nedtagningar som gjorts i god tro skulle sätta förmedlare i en bättre position. Detta påverkar inte heller förmedlares möjligheter till egna, utförligare, ansvarsbegränsningar genom avtal.

6.4.4 ARTIKEL 15 (Avsaknad av allmän övervakningsskyldighet)

1. *Medlemsstaterna får inte ålägga tjänsteleverantörerna en allmän skyldighet att, i samband med tillhandahållande av sådana tjänster som avse i artiklarna 12, 13 och 14, övervaka den information de överför eller lagrar, och inte heller någon allmän skyldighet att aktivt efterforska fakta eller omständigheter som kan tyda på olaglig verksamhet.*
2. *Medlemsstaterna kan fastställa skyldigheter för leverantörer av informationssamhällets tjänster att omedelbart informera de behöriga myndigheterna om påstådda olagliga verksamheter som utförts eller olaglig information som tillhandahållits av mottagarna av deras tjänster eller att till behöriga myndigheter på deras begäran*

[129] Detta tillvägagångssätt har man valt att använda sig av i Finland.

lämna information som gör det möjligt att identifiera de mottagare av deras tjänster med vilka de ingått lagringsavtal.

I denna artikel stadgas att medlemsstaterna inte får ålägga förmedlare en allmän övervakningsskyldighet.[130] En aktiv skyldighet att övervaka information skall endast få förekomma i de fall det är påkallat från domstol eller polismyndighet för att förebygga eller bekämpa brottslig verksamhet.[131] Enligt preambeln får dock medlemsstaterna ålägga förmedlare att ”visa den omsorg som skäligen kan förväntas av dem”.[132] Innebörden av detta är osäker. Formuleringen fanns inte med i det ursprungliga förslaget utan tillkom som en följd av att Sverige krävde att få behålla 4 och 5 §§ i LEA.[133] Möjligen skulle paragraferna kunna falla inom denna vaga formulering och således inte stå i strid med e-handelsdirektivet. Innehållet i artikel 15 har emellertid inte ändrats varför bestämmelsernas båda ordalydelser fortfarande är direkt motstridande.[134] Frågan om svensk lagstiftning är i överensstämmelse med e-handelsdirektivet är i nuläget föremål för debatt. En del hävdar att skyldigheten att förhandsgranska, i 4 och 5 §§ LEA, är tillåten enligt artikel 15 medan andra hävdar motsatsen.[135] Frågan kommer att ställas på sin spets i och med implementeringen av e-handelsdirektivet. En omformulering av LEA, så att övervakningsskyldigheten avlägsnas, borde dock, enligt vår mening, vara nödvändig.

6.5 PROBLEM MED E-HANDELSDIREKTIVET

6.5.1 TILLÄMPNINGSOMRÅDET

Genom e-handelsdirektivet försöker man genom konkreta regler fastställa förmedlares maximala ansvar och således klargöra den osäkerhet som råder angående förmedlaransvaret. Vi ifrågasätter hur stor genomslagskraft e-handelsdirektivet egentligen kommer att få i svensk rätt.

---

[130] Preambel p 47, e-handelsdirektivet
[131] Yng, ”Elektronisk handel –En gemensam rättslig ram för EU:s inre marknad”, s 117
[132] Preambel p 48, e-handelsdirektivet
[133] Enligt anonym källa tillkom formuleringen endast 8 dagar före e-handelsdirektivets antagande.
[134] LEA stadgar, genom att i 4 § ålägga förmedlare att ha viss uppsikt för att kunna fullgöra skyldigheten i 5 §, de facto ett övervakningsansvar vilket, enligt e-handelsdirektivet, inte får åläggas förmedlare.
[135] På Justitiedepartementet och Näringsdepartementet är samtliga vi har pratat med av åsikten att 4 och 5 §§, genom p 48, inte är i strid med e-handelsdirektivet. Marknadens aktörer intar dock motsatt inställning vilket bl a framförts av Patrik Hiselius, jurist på Telia. Vi ifrågasätter därför om man inte av bekvämlighetsskäl intagit den ståndpunkt man gjort på departementen. Denna lösning medför trots allt att implementeringsarbetet underlättas.

Det får troligen större betydelse i de länder där förmedlare, utan klart fastställd grund, de facto ådömts ansvar.[136] I Sverige har vi hittills inte sett några sådana fall. Som redogjorts för ovan är ansvarsbegränsningarna i e-handelsdirektivet inte tillämpliga då förmedlaren handlat med uppsåt. Enligt svensk lagstiftning krävs i princip uppsåt för att någon skall kunna dömas till ansvar. De olika regleringarna kan till viss del tyckas ta ut varandra eftersom ansvarsbegränsningarna endast blir tillämpliga då, till följd av brist i uppsåtet, brott inte föreligger. E-handelsdirektivet kommer emellertid att ha betydelse i ett fåtal specifika fall. I URL stadgas t ex om en ersättningsskyldighet oberoende av uppsåt.[137] Detta ansvar måste ändras och begränsas till följd av e-handelsdirektivet.

Vidare kan e-handelsdirektivet tänkas få viss betydelse på det straffrättsliga området då ett fåtal brott stadgar ansvar redan vid grov oaktsamhet.[138] E-handelsdirektivet stadgar om ansvarsfrihet i *alla* de fall tjänsteleverantören inte har uppsåt till att det finns ett olagligt innehåll. Ansvarsfrihet föreligger följaktligen vid grov oaktsamhet. I praktiken används emellertid rekvisitet grovt oaktsam endast i de fall det är uppenbart att förövaren är skyldig men det inte finns tillräckliga bevis för att styrka uppsåt. Detta rekvisit ligger således väldigt nära uppsåt. Rent teoretiskt medför e-handelsdirektivet dock en faktisk utvidgning av svenska förmedlares möjlighet att gå fria från ansvar. Frågan är emellertid hur stor betydelse vårt resonemang får i praktiken då de subjektiva rekvisiten ligger så nära varandra. Domstolarna väljer även i det huvudsakliga antalet fall att använda sig av uppsåtsrekvisitet snarare än grov oaktsamhet.[139]

6.5.2 KOMPETENSÖVERSKRIDANDE

Det kan ifrågasättas om Kommissionen, vid utformandet av e-handelsdirektivet, har gått utanför sin tilldelade kompetens. E-handelsdirektivet stadgar ansvarsfrihet och indirekt kan

[136] Ansvar har ådömts förmedlare i England, Tyskland samt Frankrike. Se närmare redogörelse i avsnitt 6.1-3.
[137] Se avsnitt 3.4.
[138] Endast 16:10a § BrB, spridning av barnpornografi, 16:10b § BrB, olaga våldsskildring, brott mot BBS-lagen samt brott mot URL är relevanta i det fortsatta resonemanget.
[139] Källa: Advokaten Lars Perhard Cederqvists Advokatbyrå AB. Domstolarnas faktiska tillämpning har dock visat sig ha liten betydelse ur EG-rättslig synvinkel. EU, som intar en väldigt formalistisk syn, godtar oftast inte annat än att *lagstiftningen* är direktivkonform.

detta möjligen ses som ett sätt att reglera ansvar.[140] Det straffrättsliga området ligger idag utanför EG:s kompetens. Gränserna är oklara varför en risk för inkräktande av medlemsstaternas suveränitet aktualiseras. Denna oklarhet har utnyttjats av Gemenskapens institutioner genom ständiga försök att utvidga kompetensen.[141] Möjligen försöker man, genom ansvarsbegränsningarna, att bakvägen reglera vad som är tillåtet och inte. Kommissionen har föga övertygande sökt motivera sitt agerande genom hänvisning till de något vaga formuleringarna rörande e-handelsdirektivets syfte.[142] Vidare pekar man på de konkurrensfördelar USA har, tack vare dess tekniska försprång.[143] Kommissionen har i sin argumentation lagt vikt vid att man inte försöker reglera vad som de facto *är* straffbart utan vad som *inte* är straffbart. Det hävdas att en klar uppdelning av olika rättsområden inte kan ske varför det inte heller går att skilja på olika regler in absurdum. I praktiken påverkar rättsregler på ett område även regler på ett annat.[144] Frågan om Kommissionen får anses ha överskridit sin kompetens är följaktligen inte klar. I sammanhanget får dock inte glömmas bort att e-handelsdirektivet faktiskt är antaget. Det är således upp till EG-domstolen att fälla ett sista avgörande vid en eventuell ogiltighetstalan. Mot bakgrund av detta resonemang kvarstår möjligen osäkerheten angående förmedlares ansvar, trots implementeringen av e-handelsdirektivet. Troligtvis kommer dock samtliga medlemsstater undanta förmedlare från straffansvar i enlighet med e-handelsdirektivet.

6.6 IMPLEMENTERING

Då e-handelsdirektivet kommer att få betydelse för regleringen av förmedlaransvaret anser vi det nödvändigt att i denna framställning beröra implementeringen av artiklarna 12-15. Någon

---

[140] Då detta problem aktualiserades vid utformandet av e-handelsdirektivet var även den svenska straffrättsenheten med och förhandlade, något som vanligtvis inte sker.
[141] Se t ex C-203/80 Casati samt C-271/82 Auer där EG-domstolen uttalat att regler för den fria rörligheten inte får vara beroende av att straffrätt ligger utanför EG:s kompetens. Fallen rör dock situationer där enskilda åberopat rättigheter enligt regler i direktiv för att undgå straffrättsligt ansvar. Resonemanget kan således inte här tillämpas i sin helhet.
[142] Formuleringarna som bl a finns att hitta i p 1, 2 samt 40 rör det framväxande behov av gemensam reglering som finns enligt Gemenskapsinstitutionerna. Skillnader i medlemsstaternas rättssystem anses skapa osäkerhet för operatörer vilket anses hämma utvecklingen av tjänster på Internet samt hindra en inre marknad från att fungera smidigt.
[143] Kelleher, ”IT-law in the EU”, s 93

större vikt kommer dock inte att läggas vid implementeringsfrågorna. Vi avser endast att kort redogöra för de alternativ som är föremål för diskussion. Det råder i dagsläget inte full enighet om hur man på bästa sätt implementerar e-handelsdirektivets artiklar 12-15. Det föreligger emellertid två huvudalternativ för hur man skulle kunna inkorporera e-handelsdirektivet i svensk lagstiftning.

Inkorporera e-handelsdirektivet i en ny lag

Det första alternativet innebär att man kopierar e-handelsdirektivet och inför det i en helt ny *lag för informationssamhällets tjänster*. Denna lag ges företräde framför konkurrerande svensk lagstiftning. Tillvägagångssättet är emellertid ovanligt, (PUL är ett undantag). Då e-handelsdirektivet kanske kan tyckas svåranpassat till svensk rätt kan dock detta möjligen utgöra ett tänkbart alternativ. Detta alternativ är minst tidskrävande. Det finns även tecken på att övriga medlemsstater kommer att implementera e-handelsdirektivet på detta sätt.[145]

Ändringar i relevant lagstiftning

Det andra alternativet, som enligt vår mening utgör det mest lämpliga, innebär att man går in och gör ändringar i olika aktuella lagrum. Detta alternativ är mer arbetskrävande men samtidigt skapar det ett mer enhetligt, tydligt och tillämparvänligt regelsystem. Ansvars-begränsningarna utgör endast en del av e-handelsdirektivet. Att implementera dem enligt ovan medför, anser vi, att e-handelsdirektivets klargörande syfte går förlorat. Att fastställa ansvar respektive ansvarsbegränsningar i skilda lagar förefaller högst omotiverat. Det riskerar att bli aktörerna på marknaden som tvingas göra relevanta kopplingar till annan svensk lagstiftning. Rättsläget blir klarare om svensk lag ändras i de fall den inte harmoniserar med e-handelsdirektivets regler. Man bör även ta itu med terminologiproblematiken. Exempelvis är, som ovan nämnts, begreppet informationssamhällets tjänster vidare än elektroniska tjänster i LEA.

En av de tydligaste diskrepanserna mellan e-handelsdirektivet och svensk lag utgör den allmänna övervakningsskyldigheten i LEA. Att se preambeltexten som en medelväg

---

[144] Anonym källa på Justitiedepartementet

[145] Efter kontakt med Närings- och Justitiedepartementet, vid ett flertal tillfällen, verkar detta alternativ i dagsläget vara det man beslutat sig för. Det färdiga förslaget väntas läggas fram, enligt senaste uppgift från anonym källa på Näringsdepartementet, någon gång i januari 2001.

innebärande att 4 och 5 §§ är i överensstämmelse med e-handelsdirektivet kan ifrågasättas då den faktiska ordalydelsen i artikel 15 klart uttalar motsatsen. Ett annat exempel där den svenska lagstiftningen inte överensstämmer med e-handelsdirektivet utgör de tidigare berörda ersättningsreglerna i URL 54 §. Då ansvarsbegränsningarna omfattar samtliga aktiviteter där förmedlaren inte har uppsåt kan fortsättningsvis inte stadgas ett strikt skadeståndsansvar. Vi anser således att dessa regler måste omformuleras alternativt tas bort. Vidare bör de oklarheter som råder angående det subjektiva rekvisitet i Brottsbalken samt i URL:s straffrättsliga bestämmelser beaktas. Då man här, i motsats till e-handelsdirektivet, ålägger förmedlare ansvar redan vid grov oaktsamhet krävs att bestämmelserna ändras. Det måste vara klart för förmedlare i vilka fall ett eventuellt ansvar kan aktualiseras. Sådan klarhet uppnås, menar vi, först då ansvarsfrihetsreglerna inkorporeras direkt i ansvarsreglerna.

7 USA

I ovanstående redogörelse över svensk rätt har ett försök att definiera rådande osäkerhetsmoment på området gjorts. En fullständig utredning av förmedlaransvaret kräver att hänsyn tas till utländska tendenser då dessa kan få betydelse för svensk rättstillämpning.[146] Med sin rikliga praxis på området samt den långt framskridna utvecklingen av lagar anpassade till Internet får USA en framträdande plats. Utvecklingen av ansvarsregler för förmedlare påbörjades tidigt i USA. Utländsk praxis har inte något prejudikatvärde i Sverige. Dess betydelse kan dock av olika anledningar ändå inte uteslutas.

Frågan om förmedlaransvar har uppkommit vid främst två typer av brott. Den första typen benämns i det följande *förargelseväckande brott* och inbegriper exempelvis spridande av barnpornografi samt förtalsbrott. Den andra gruppen hänför sig till *upphovsrättsliga brott*. Ansvarsfrågan har reglerats olika beroende på till vilken av dessa grupper brottet kan hänföras. För att underlätta för läsaren utgår följande redogörelse från nämnda uppdelning av brott. Då mängden fall är stort har endast ett fåtal relevanta fall valts ut.

---

[146] Se t ex ansvarsbegränsningarna i e-handelsdirektivet, som är direkt influerade av amerikansk lagstiftning och praxis.

7.1 FÖRARGELSEVÄCKANDE BROTT

För förargelseväckande brott har amerikanska domare visat en viss benägenhet att göra analogier till medier inom den pappersbaserade världen. Man har ålagt förmedlaren olika ansvar beroende på om förmedlaren kan hänföras till en passiv distributör och således jämställas med exempelvis ett bibliotek, eller om förmedlaren istället kan liknas vid en aktiv förläggare. Benägenheten har varit att ålägga förmedlaren ett större ansvar i de fall han kunnat jämställas med en förläggare. Jämställs han istället med en distributör är det mest sannolikt att han går helt fri från ansvar.

Rättspraxis på området började utformas redan i början av 1990-talet. Regler fick etableras i praxis eftersom det inte fanns någon lag som reglerade förmedlares ansvar. I *Cubby v. Compuserve*[147] ålades en förmedlare för första gången ett uttryckligt ansvar. Fallet rörde ett meddelande i ett nyhetsbrev på Compuserves tjänst. Innehållet i meddelandet utgjorde, enligt Cubby, ett förtalsbrott varpå anspråk riktades mot Compuserve, såsom ansvarig för tjänsten. Domstolen fastslog att en förmedlare faktiskt har ett ansvar för förmedlade uttalanden innehållande förtal. Detta ansvar är dock inte strikt. Vidare uttalades att en förmedlare endast kan bli ansvarig i de fall han har uppsåt. I föreliggande fall jämställdes Compuserve med en distributör, varför ansvar inte förelåg.[148]

I *Stratton Oakmount Inc v. Prodigy Services Company*[149] jämställdes förmedlaren med en förläggare. Prodigy förestod en välbesökt elektronisk anslagstavla. Ett meddelande innehållande nedvärderande uppgifter om Stratton föranledde process om utkrävande av ansvar för förtal. I jämförelse med föregående fall intog förmedlaren en mer aktiv roll. Prodigy vidtog aktiva åtgärder för att förhindra spridandet av olagliga meddelanden. Bl a användes ett mjukvaruprogram vilket med automatik rensade bort meddelanden innehållande ett opassande språk. Vidare hade Prodigy anställd personal som övervakade tjänsten. Omständigheterna

[147] 776 F. Supp. 135 (S.D.N.Y.) 1991
[148] En jämförelse kan här göras med artikel 12 i e-handelsdirektivet som även bygger på detta resonemang. Ansvar får ej göras gällande om förmedlaren kan ses endast som ett ”verktyg”.
[149] [1995] WL 323710 (N.Y. Sup. Ct. 1995)

ledde sammantaget till att Prodigy inte kunde anses passiv i sin förmedlarroll. Prodigy jämställdes med en förläggare och ansvar för förtal kunde således utkrävas.

The Federal Communications Decency Act

Prodigy-fallet tillsammans med andra fall föranledde att ytterligare steg togs för att handskas med problematiken. 1996 infördes the Federal Communications Decency Act.[150] Syftet med denna lag är att skydda användare mot oanständigt material innebärande brott som t ex förtal och barnpornografi. Internet skall styras av samma regler till skydd för förtalsbrott etc som finns i andra telekommunikationer. Lagen innehåller bl a regler om undantag från ansvar för förmedlare. § 230 tillkom specifikt som en följd av domen mot Prodigy. Förmedlare som arbetar aktivt för att få bort skadligt material skall enligt bestämmelsen inte kunna straffas för detta. En liknelse med förläggare skall således inte göras i sådana fall.[151] Genom lagen har förmedlares ansvar alltså begränsats avsevärt. Endast i undantagsfall kan ansvar utkrävas, av förmedlare, för denna typ av brott. Detta har upprätthållits i efterföljande praxis. Ett exempel utgör *Zeran v. America Online, Inc*[152] (AOL). Även i detta fall rörde det sig om ett förtalsbrott. Zerans telefonnummer hade lagts ut, av en okänd person, på AOL:s BBS. Genom att ringa detta nummer skulle man kunna köpa t-shirts med upprörande slogans. Det ursprungliga meddelandet togs bort efter anmälan från Zeran. Liknande meddelanden fortsatte dock att dyka upp. Zeran argumenterade då för att AOL hade en plikt att, såsom förläggare, omedelbart avlägsna material man visste innehöll förtal. Mot bakgrund av Federal Communications Decency Act dömde domstolen till AOL:s fördel. Man poängterade att § 230 var skapad för att minimera myndigheters inblandning samt att en förmedlare omöjligt kunde kontrollera alla de miljontals meddelanden som gick över dess servrar varje dag.

Samma slutsats drogs i *Lunney v. Prodigy Services Company*[153]. Här postades på Prodigys BBS, av okänd användare, hotfulla mail riktade mot en tredje man. Meddelandena var skrivna i Lunneys namn. Lunney stämde Prodigy för förtal. Han hade dock ingen framgång med sitt åtal.

---

[150] 47 U.S.C.A., § 230 får anses mest intressant i sammanhanget.
[151] Weiner, ”Negligent publication on Electronic Bullentin Boards: Is there any liability left after Zeran?”, artikel från Santa Clara Law Review, s 929
[152] 958 F. Supp. 1124 (E.D.Va. 1997) appeal 129 F. 3d 327 (4th cir. 1997)
[153] 683 N.Y.S.2d 557 (A.D.2Dept. 1998), appeal 723 N.E.2d539 (N-Y.Ct.App 1999)

Även här tillämpade domstolen § 230 med motiveringen att en förmedlare inte skall behöva övervaka de alla de meddelanden som ständigt passerar dennes tjänst. Detta fall har även haft betydelse vid utformandet av e-handelsdirektivet.[154] Möjligen har domstolens argumentation tjänat som inspirationskälla vid införandet av artikel 15.

7.2 UPPHOVSRÄTTSLIGA BROTT

På det upphovsrättsliga området har utvecklingen i USA, liksom för de förargelseväckande brotten, gått mot ett mer begränsat ansvar. I de fall förmedlaren endast utgör ett *passivt verktyg* skall ansvar således inte kunna utkrävas. Det upphovsrättsliga skyddet är starkt i USA. Till skillnad från svensk rätt faller caching och annan mellanliggande lagring uttryckligen inom det upphovsrättsliga skyddet.[155] Det är dock osannolikt att man i USA skulle ålägga förmedlare ansvar som gärningsman i ett fall då kopiering sker mekaniskt och utan egentlig kontroll. Intressant i detta avseende är *Religious Technology Centre v. Netcom On-line Communication Services, Inc.*[156]. Netcom tillhandahöll en newstjänst vid vilken postades upphovsrättsligt skyddat material. Netcoms datorer lagrade sedan detta material under en kort period så att andra Usenet datorer skulle kunna kopiera och sprida innehållet över hela världen. Mot bakgrund av detta ansåg upphovsrättsinnehavarna att Netcom gjort sig skyldiga till upphovsrättsintrång. Domstolen var dock inte av samma åsikt. Netcom ansågs inte vara direkt ansvarig eftersom de kopierade verken lagts in av en tredje part. Trots att lagringen varat i elva dagar utkrävdes inget ansvar. Netcom ansågs ha varit passiv i sin roll och liknades således vid ett verktyg. Man poängterade dock att ansvar kunde uppkomma i de fall förmedlaren intar en mer aktiv roll.[157]

I *Playboy Enterprises, Inc. V. Russ Hardenburgh, Inc.*[158] ansågs förmedlaren ha handlat aktivt. Det användes bl a en policy som uppmuntrade användare att ladda upp pornografiska bilder på servern. Vidare granskade de anställda granskade bilder samt flyttade dem från

[154] Anonym källa på Justitiedepartementet
[155] Cahoy, ”Comment: New legislation regarding on-line liability for copyright infringement: a solution in search of a problem?”, artikel från The Journal of Law and Technology, s 338 ff
[156] 37 U.S.P.Q.2d (BNA)
[157] Se även här likheterna med ansvarsbegränsningarna i e-handelsdirektivet.
[158] 1997 WL 709747, 45 U.S.P.Q.2d (BNA)

uppladdningsfilen till en, för användare, mer lättillgänglig fil. Förmedlaren dömdes för upphovsrättsintrång.[159]

Mot bakgrund av dessa rättsfall kan vi således sluta oss till att det i praxis framvuxit ett begränsat ansvar för upphovsrättsintrång. Förmedlaren åläggs endast gärningsmannaansvar i de fall han varit *aktiv* i den brottsliga gärningen. Förmedlaren kan dock fortfarande drabbas av ett medverkandeansvar. Vid medverkandeansvar föreligger inte samma aktivitetsrekvisit. Ansvarsfrihet kan endast åtnjutas fram till tidpunkten då vetskap nås om eventuella brottsligheter.[160] Efter det att kännedom nåtts om intrånget kan förmedlaren inte vara passiv utan måste handla aktivt för att förhindra fortsatt brottslighet.[161]

7.2.1 DIGITAL MILLENIUM COPYRIGHT ACT

Som en följd av krav på en klar och enhetlig reglering på detta område tillkom 1998 the US Online Copyright Infringement Liability Limitation Act. Lagen utgör en del av den s k Digital Millennium Copyright Act och är utformad i samarbete mellan olika parter på marknaden.[162] En mer marknadsanpassad lösning har således skapats. Som redan nämnts har denna lag haft stort inflytande vid utformningen av e-handelsdirektivet. Till skillnad från e-handelsdirektivet riktar den sig endast mot upphovsrättsliga brott och således inte mot brott i allmänhet.

Genom detaljerade regler fastslås i lagen olika begränsningar i förmedlares ansvar.[163] Det bakomliggande syftet är att tillhandahållande av enbart teknik för överföring av information inte skall medföra ansvar. Under samma förutsättningar som anges i artikel 12 i e-handelsdirektivet kan förmedlaren alltså frias från ansvar. Vidare anges att tillfällig lagring, caching, ligger utanför det upphovsrättsliga ansvarsområdet. Trots att en sådan lagring i och för sig anses omfattas av upphovsrättens regler om mångfaldigande och således utgöra ett intrång, väljer man att undanta detta förfarande från förmedlarens ansvarsområde.[164] En likartad

[159] Här ser vi således en skillnad i rättsutvecklingen gentemot anständighetsbrotten.
[160] Detta har framkommit i bl a *Fonovisa, Inc. v. Cherry Auction, Inc.,* 76 F. 3d 259, 264, 37 U.S.P.Q2d (BNA) 1590, 1595 (9th Cir. 1996)
[161] Cahoy, ”Comment: New legislation regarding on-line liability for copyright infringement: a solution in search of a problem?”, artikel från The Journal of Law and Technology, s 347
[162] Carlinsky och Conciatori, ”DMCA charts safe harbors in a wired world”, artikel från New York Law Journal
[163] Section 512 (a-i) US Copyright Act
[164] Section 512 (a) US Copyright Act

inställning tillämpas vid lagring av information. Begränsningar i ansvaret stadgas även för söktjänster. [165]

Notice and takedown

DMCA:s regler om notice and takedown utgör förlagan till artiklarna 13-14 i e-handelsdirektivet. Då syftet i avsnitt 6.4 samt 6.5 är att poängtera de brister som föreligger i utformandet av dessa artiklar görs här endast en generell beskrivning av detta förfarande. I det följande ges således en mer detaljerad redogörelse. Utöver den faktiska skyldigheten att plocka ned ett meddelande stadgar DMCA att förmedlare skall tillhandahålla en lättillgänglig kontaktperson samt att en anmälan endast kan göras av vissa personer. Här finns således skyldigheter åt båda håll. Endast en *rättighetsinnehavare* eller *dennes agent* kan göra anmälan. Anmälan skall vara skriftlig, med vissa ytterligare formkrav.[166] Efter att anmälan har skett åläggs förmedlaren att snabbt avlägsna eller blockera access till materialet. Det har vidare intagits en följdreglering vilken ytterligare begränsar ansvaret. En åtgärd som förmedlare åtagit i *god tro* skall således aldrig föranleda ansvar även om avlägsnandet/ blockerandet skett felaktigt. På användares begäran skall dock materialet läggas tillbaka på tjänsten. Detta sker genom att användaren skickar en ”counter notification” till förmedlaren. Materialet skall därefter vara tillgängligt igen inom 10-14 dagar efter delgivandet av en sådan ”counter notification”.[167]

Napster

Frågan om DMCA:s tillämpningsområde aktualiserades i det uppmärksammade målet mot Napster i USA. Napster tillhandahöll en central server gentemot vilken användare kunde ladda upp sig för att utbyta mp3-filer med varandra. Systemet var unikt på så sätt att musiken aldrig fanns på Napsters centrala server utan istället hemma hos användarna. Napster utgjorde således ingen traditionell förmedlare då inget lagringsutrymme tillhandahölls. Kopieringen skedde inte av Napster. Utbytet av mp3-filer hade emellertid inte kunnat ske utan deras

[165] Title II 17 U.S.C DMCA, 1998
[166] Den måste vara tydlig på så sätt att förmedlaren lätt kan lokalisera det brottsliga materialet. Det måste även uttryckligen stadgas att anmälan är utformad i god tro samt innehålla en bekräftelse under straffansvar att informationen är riktig.
[167] Detta gäller dock inte om rättighetsinnehavaren meddelat förmedlaren att denne påtalat brottet i domstol.

medverkan. Det enda som krävdes av användaren var egentligen att denne tryckte på en knapp för att nedladdning skulle ske till hårddisken. Vidare tillhandahöll Napster ett register vilket användare kunde söka i för att få kontakt med varandra. Brott mot upphovsrätten aktualiserades och flera stora skivbolag valde att gemensamt driva ansvarsfrågan gentemot Napster. Frågan om Napster kunde anses utgöra förmedlare eller inte aktualiserades.

Domstolen ansåg inte Napster utgöra en förmedlare. Då mp3-filerna inte passerade tjänsten på ett brukligt sätt menade domaren istället att Napster fungerade som en länkläggare, varför det inte kunde åtnjuta ansvarsfrihet enligt någon av de grunder som anges i DMCA.[168] Målet överklagades av Napster då det ansåg sig utgöra en network/access provider. En av parterna, skivbolaget BMG, har under hösten valt att lägga ned sin stämning gentemot Napster. Anledningen är att ett samarbete utvecklats mellan skivbolaget och Napster. Tjänsten är således för tillfället under omarbetande. Användarna är i fortsättningen skyldiga att, till upphovsrättsinnehavaren, erlägga betalning vid utnyttjande av upphovsrättsligt skyddade verk.[169] Övriga stämningar har emellertid inte dragits tillbaka. Problemet kvarstår sålunda för avgörande i högre instans.[170]

8 JURISDIKTION

8.1 DET GRÄNSÖVERSKRIDANDE INTERNET

Framställningen har hittills behandlat förmedlares ansvar på ett nationellt plan. Utgångspunkt har följaktligen tagits i olika länders nationella lagstiftning. Internet utgör emellertid ett globalt, gränslöst medium. Informationen känner inga landgränser. Lagar är däremot nationella och sträcker sig inte utanför det egna landets geografiska gräns. Att endast koncentrera framställningen till en redogörelse på nationell nivå skulle inte ge en rättvisande bild av verkligheten. En webbsida med rasistiska uttalanden skrivna på svenska språket kan t ex ha

[168] Carlinsky och Conciatori, ”DMCA charts safe harbors in a wired world”, artikel från New York Law Journal
[169] Claeson, ”Napster i blåsväder efter samarbete”, artikel från Göteborgsposten

lagts in av en konsult i USA på en server i Portugal. Innehållet på webbsidan kan vara tillgängligt i flera olika länder och strida mot vissa av ländernas lagstiftning samtidigt som det anses lagligt i andra länder. Frågan är vilket lands domstol som anses behörig att pröva en tvist samt vilket lands lag som då skall tillämpas. Vidare föreligger problem med verkställigheten av domen. Naturligtvis är det meningslöst att utverka en dom i Sverige som ålägger ett amerikanskt företag att betala skadestånd, om domen varken kan verkställas i USA eller i Sverige.

Problemet med jurisdiktion tillhör ett av de mest svårlösta i den internationella samvaron. Problemet är inte nytt utan existerar sedan länge. Den ökning av internationell kontakt som Internet möjliggör medför att detta problem intensifieras. Att göra en mer djupgående redogörelse av nämnda problem samt den materiella rätt som gäller skulle spränga ramen för denna framställning. Följande redogörelse begränsas därför till ett konkret fall där problemet aktualiseras.

Cyberspace likställdes tidigare med ett eget ”virtuellt” land som låg utanför traditionella staters räckhåll. Det hävdades att det inte fanns något enskilt land som ägde jurisdiktion över det gränslösa Internet. Synsättet är nu det rakt motsatta. Idag kan istället samtliga stater tänkas ha jurisdiktion. Problematiken kring jurisdiktionsfrågor får koncentreras till om det föreligger tillräckliga anknytningsmoment till domstolsstaten. Liksom övriga regler på detta område är traditionella beprövade anknytningsmoment, som bygger på geografiska anknytningspunkter såsom gärningsorten, avtalsorten, skadeorten mm, svåra att tillämpa på Internet.[171] Vid en bedömning över om jurisdiktion föreligger borde nätverksservens placering få väldigt liten betydelse eftersom det inte finns några omständigheter, tekniska eller praktiska, som talar för en viss placering. Valet av lagringsplats styrs av pris samt av tillgång till ledig kapacitet. Detta får till följd att faktorer som är styrande vid fastställande av jurisdiktion framstår som helt slumpmässiga och irrelevanta. Att försöka komma runt svensk lagstiftning *enbart* genom att lägga en sida på en utländsk server är således inte möjligt.[172] En samlad bedömning måste i stället göras utifrån omständigheterna i varje enskilt fall.

---

[170] Dom väntas komma inom en snar framtid.
[171] Bogdan, ”Jurisdiktions- och lagvalsfrågor på Internet”, s 7-8
[172] Carlén-Wendels, Nätjuridik, s 45

Yahoo[173]

I maj i år av dömdes det amerikanska portalbolaget Yahoo av fransk domstol att förhindra franska användare tillgång till vissa siter.[174] Genom att tillåta försäljning av föremål med nazistanknytning på den amerikanska siten www.yahoo.com ansågs Yahoo ha brutit mot fransk lagstiftning.[175] Försäljningen som var helt lagenlig i USA var således otillåten i Frankrike. På den franska yahooportalen (www.yahoo.fr) förekom inte någon sådan försäljning. Genom ett enda klick med musen hade dock användare möjlighet att förflytta sig till www.yahoo.com. Med motiveringen att den aktuella sidan var baserad i USA, där försäljningen var tillåten, samt de tekniska svårigheter som aktualiserades, i samband med ett uteslutande av endast franska användare, överklagades domen av Yahoo. Det hävdades att en blockering av de aktuella siterna mot enbart franska användare var tekniskt omöjlig. I syfte att utreda de tekniska frågor som förelåg tillkallade den franske domaren en expertgrupp. Denna grupp konstaterade, efter en omfattande utredning, att det finns teknisk möjlighet att förhindra tillgång för ca 70 procent av de franska användarna. Avgörande är om man har en fransk förmedlare eller inte. För övriga 30 procent, som har utländska förmedlare, är det dock mycket svårare.[176] Till följd av detta fastställdes tidigare domslut.[177] Yahoo säger sig ha för avsikt att följa domslutet men hävdar samtidigt att det finns stora möjligheter att komma runt en sådan teknisk blockering. Argumentation förs även kring svårigheten att effektivt utesluta just franska användare från access till siten. Det anses, mot bakgrund av att franska användare kan använda utländska förmedlare samtidigt som icke franska medborgare kan använda sig av franska förmedlare svårt, att lokalisera de franska användarna. Vidare pekar man på de problem med teknisk filtrering som redan nämnts i framställningen. Sålunda riskerar helt lagligt material, som t ex historiska siter om andra världskriget, att sållas bort. Yahoo har några månader på sig att anpassa sig till domslutet. Alternativt har de också möjlighet att överklaga domen eller föra

[173] Domen finns att läsa på http://www.juriscom.net/txt/jurisfr/cti/yauctions.htm
[174] Bolaget dömdes även att betala böter till de två antirasistiska grupper som stämt dem.
[175] Otillåtet enligt franska brottsbalken artikel R.645-2 samtidigt som det ansågs grovt förolämpande mot det judiska folket.
[176] CNN.com technology, "Experts testify in French Yahoo! Case over Nazi memorabilia", November 6, 2000
[177] Domen kom 21 november 2000. Den nya lagen rörande förmedlaransvar, se avsnitt 6.3, tillämpades inte.

saken i amerikansk domstol.[178] Väljer de det senare alternativet är chansen stor att domslutet blir ett helt annat. Frågan är hur man väljer att agera då.

Trots att sidan är baserad i USA och i överensstämmelse med amerikansk rätt ansåg den franske domaren att Yahoo genom att visa sidorna i Frankrike begått ett brott på det franska territoriet och att fransk lag var tillämplig. Det kan dock ifrågasättas om avgörandet överensstämmer med e-handelsdirektivet och dess ansvarsbegränsningar. Europeisk rättsutveckling går mot ett mer amerikanskt synsätt. Genom e-handelsdirektivet söker man begränsa ansvaret för förmedlare. Läsaren bör göras påmind om de rättsfall som utgjorde bakgrunden till en reglering av detta område. I rättsfallen fastställdes omfattande ansvar för förmedlare. Det är denna utveckling som ansvarsbegränsningarna i e-handelsdirektivet syftar till att hejda. Ett domslut innebärande en utvidgning av ansvaret förefaller gå emot e-handelsdirektivets syfte. Följden av Yahoo-domen blir att förmedlare nu riskerar att ansvara enligt lagarna i samtliga länder där en aktuell tjänst tillhandahålls.[179] Frågan är hur väl detta korresponderar med Internets karaktär av världsomspännande medium. Det finns mer än 180 länder i världen och om alla större förmedlare är tvungna att följa lagarna i samtliga dessa länder faller, menar vi, hela tanken bakom Internet. Varje lands nationella lagstiftning kan inte ensamt reglera ett globalt Internet. Frågan är således vilka maktmedel Frankrike har att ta till för att genomdriva domen i det fall Yahoo vägrar att följa den.

9 AVSLUTANDE KAPITEL

9.1 INLEDNING

Internet medför helt nya möjligheter för kommunikation och spridning av material. Här sker en ständig förmedling av information. Förmedlingsprocessen involverar ett flertal olika aktörer som kan indelas i fyra olika kategorier; network provider, access provider, content provider och hosting service provider. Ansvarsbilden varierar beroende på vilken aktörskategori som är för handen.

[178] CNN.com technology, "Yahoo! Anger at French Nazi auction ban", November 21, 2000
[179] CNN.com, "Web worries over French site ban", November 21 2000

Förmedlares ansvar kan delas in i ett straffrättsligt och ett skadeståndsrättsligt ansvar. Det skadeståndsrättsliga ansvaret, gentemot användare och content provider, regleras ofta genom avtal. Skadeståndsanspråk från tredje man är även det oftast reglerat i avtalet mellan förmedlare och content provider och förmedlare undviker på så sätt ansvar. Det straffrättsliga ansvaret delas upp i ett allmänt, främst BrB och URL, och ett specialstraffrättsligt ansvar, LEA. Det råder idag problem att klart definiera förmedlares ansvar. Osäkerheten hänför sig främst till det specialstraffrättsliga området och LEA. Förmedlares ansvar utvidgas enligt LEA till att omfatta handlingar där någon annan agerat. Förmedlaren är således skyldig att avlägsna ett meddelande om det uppenbart strider mot något av de i lagen uppräknade brotten. För att undgå ansvar krävs även att förmedlaren *förhandsgranskar* allt material som aktualiseras på dennes tjänst. LEA är otydligt utformad och ger upphov till olika tillämpningsproblem. Klara riktlinjer angående centrala begrepp saknas samtidigt som förarbetena i flera avseenden är motsägelsefulla.

I anslutning till de tillämpningsproblem som aktualiseras angående LEA framträder ett annat centralt problem; frågan om yttrandefriheten på Internet. Denna fråga är föremål för debatt och ingen kan idag klart uttala i vilken omfattning yttrandefrihet råder. Såväl YGL:s som TF:s tillämpningsområde är begränsat. Grundlagarna kan endast tillämpas i undantagsfall. Samtidigt som detta område är oklart stadgar LEA en skyldighet för förmedlare, att under straffrättsligt ansvar, ingripa mot eventuellt olagliga meddelanden. Då förmedlaren tvingas avgöra informationens lagenlighet leder detta till en sorts privat bedömning av yttrandefrihetens omfattning. Åsikter har framförts om att detta medför att förmedlarna istället för grundlagen sätter gränserna.

Den osäkerhet som råder angående förmedlares ansvar har uppmärksammats utomlands. Förmedlare har ådömts ett långtgående ansvar i ett antal europeiska länder. Detta ledde fram till ett behov av reglering på gemenskapsnivå. I syfte att klargöra och begränsa förmedlares ansvar utformades e-handelsdirektivet 2000/31/EG. Amerikansk rätt har tjänat som huvudsaklig inspirationskälla.[180] Det amerikanska synsättet kännetecknas av ett begränsat ansvar för förmedlare. Den amerikanska influensen framträder tydligt i e-handelsdirektivets

[180] DMCA, med bl a regler om notice and takedown, har här haft störst inflytande.

ansvarsbegränsningar. Förmedlarnas ansvar begränsas till en nivå motsvarande deras praktiska möjligheter till kontroll.

Genom självreglering har förmedlarna själva möjlighet att öka förtroendet på markanden samt till viss del begränsa sitt ansvar. Självreglering bygger på samarbete mellan branschens olika parter och är mer flexibel än vanlig lagstiftning då den snabbt kan anpassas till den tekniska utvecklingen. Det går dock inte att bortse från det samband som föreligger mellan lagstiftning och självreglering. Självregleringen utgör ofta ett komplement till lagstiftningen då den bidrar till ett mer substantiellt innehåll av densamma. Självreglering kan ske genom information och frivillig påverkan. I de flesta fall sker dock självreglering genom mer ingripande åtgärder, att användare stängs av från tjänsten är t ex vanligt.

Vidare har förmedlare möjlighet att rent tekniskt ingripa mot olagligt innehåll. Såväl teknisk som social filtrering används. Här föreligger emellertid vissa begränsningar varför denna åtgärd endast får anses fungera som ett komplement till lagstiftning och självreglering.

9.2 ANALYS OCH SLUTSATSER

Frågan vem som bör ansvara för visst förmedlat material kan inte entydigt besvaras. Då möjligheterna att identifiera en content provider ofta är begränsade är det svårt att i praktiken utkräva ansvar. Förmedlaren tillgängliggör det aktuella materialet och det kan därför tyckas naturligt att denne också bör ha ett visst ansvar för detsamma.

Det är idag inte heller möjligt att definiera ett klart avgränsat ansvarsområde för förmedlare. Oklarheterna hänför sig huvudsakligen, som redan påpekats, till LEA och dess otydliga utformning. Detta kan tyckas underligt med tanke på att nämnda lagstiftning utformats i syfte att klargöra ansvaret.

Svensk lagstiftning

LEA har ännu inte prövats i svensk domstol. Lagen tjänar främst ett förebyggande syfte på så sätt att flertalet aktörer de facto beaktar den. Flera avtal är utformade mot bakgrund av bestämmelserna i lagen. Oklarheterna i lagen kan emellertid inte negligeras. Förarbetena bidrar genom sin motsägelsefulla utformning till ett förstärkande av rådande osäkerhet. Frågan är hur

detta överensstämmer med förarbetenas funktion som klargörande rättskälla. Den förvirring som råder angående definitionen av elektronisk anslagstavla utgör ett tydligt exempel. I förarbetena stadgas uttryckligen att någon klar definition inte kan fastställas. Samtidigt görs dock enligt vår mening diverse inkonsekventa försök att avgränsa begreppet.[181]

Vidare är skyldigheten att förhandsgranska oklar. Lagtexten stadgar en uttrycklig skyldighet samtidigt som man i förarbetena anger motsatsen. Oklarheterna förstärks ytterligare genom införandet av e-handelsdirektivet som också är motsägelsefullt. E-handelsdirektivets förbud mot övervakningsskyldighet står i klar strid mot svensk lagstiftning. Trots de motstridiga ordalydelserna råder det i dagsläget oenighet om den svenska lagstiftningen står i överensstämmelse med e-handelsdirektivet. Det hävdas att preambeltextens utformning etablerar möjligheter att bortse från förbudet varför svensk lag står i överensstämmelse med ordalydelsen.

Ovanstående analys visar på svårigheterna för förmedlare att förutse eventuella konsekvenser av sitt agerande. LEA kan inte anses uppfylla grundläggande krav på förutsebarhet. Implementeras e-handelsdirektivet i *oförändrad* lydelse intensifieras problemet ytterligare. Förbudet mot övervakningsskyldighet är dock inte det enda exemplet där diskrepans råder.[182] En implementering bör, enligt vår mening, istället genomföras på ett mer konsekvent och tydligt sätt. Det sker enklast genom att aktuella motstridigheter avlägsnas genom ändringar i relevant lagstiftning. Då syftet med e-handelsdirektivet är att klargöra rättsläget förefaller det inkonsekvent att fastställa ansvar respektive ansvarsbegränsningar i skilda lagar. Det kan även ifrågasättas vilken lag som skall ges företräde i de fall lagtexterna är motstridiga.

Oberoende av implementeringsproblematiken, bidrar vidare e-handelsdirektivets utformning självständigt till ytterligare oklarheter. Ett flertal brister kan påtalas.[183] Ett tydligt exempel

---

[181] Ett tydligt exempel är att man som avgörande kriterium använder ”sända och ta del av” samtidigt som man även väljer att omfatta webhotel i begreppet elektronisk anslagstavla.

[182] Även ersättningsreglerna i URL står i direkt strid med e-handelsdirektivet. Resonemang kan även föras kring ”grov oaktsamhetsbrott”. Svensk lag stadgar i vissa fall ansvar vid grov oaktsamhet trots att e-handelsdirektivet endast medger ansvar för förmedlare då de haft uppsåt till förekommande olagligheter.

[183] Ansvarsbegränsningarna är t ex enbart tillämpliga i de fall förmedlaren handlat utan uppsåt. Samtidigt fastslår dock svensk lagstiftning huvudsakligen ansvar vid uppsåtliga brott. Begränsningarna förefaller onödiga då bestämmelserna här inte på något sätt påverkar varandra. E-handelsdirektivets klargörande syfte går således förlorat.

utgör det faktum att endast vissa delar av DMCA har använts. En fulländad reglering ställer, enligt vår mening, högre krav på klarhet. Reglerna om notice and takedown innehåller t ex endast en grundläggande struktur. Enbart själva proceduren regleras. Någon vägledning av bl a vem som får göra en anmälan samt konsekvenserna av en eventuellt felaktig nedtagning utelämnas helt.

Anmälningarna kan, som i Finland, handläggas av en offentlig myndighet med juridisk kompetens. Bedömningen av ett meddelandes lagenlighet görs således av juridiskt kvalificerade personer istället för av lekmän. Tar denna myndighet även på sig det skadeståndsrättsliga ansvaret ges klarhet i frågan om skadeståndsansvar för felaktig nedtagning. Nackdelen med detta alternativ är ökad byråkrati samt ökad belastning på skattesystemet. Möjligen är det mer lämpligt att förmedlare med behov av juridiskt kunnande själva anställer jurister. Av stor vikt för förmedlare är också att de klart och tydligt avtalar bort det skadeståndsansvar som kan aktualiseras för dem vid en felaktig nedtagning.

Yttrandefriheten

Två legitima intressen, yttrandefriheten och en effektiv brottsbekämpning, står emot varandra. Förmedlaren hamnar mitt emellan och agerar således inom ett stort osäkerhetsområde. Vi menar det vara av största vikt att förmedlares roll i denna konfliktsituation klargörs. Yttrandefriheten bör regleras on-line och off-line. Valet av medium skall inte påverka i vilken omfattning yttrandefrihet föreligger. Det har framförts åsikter om att det för frågans klargörande är nödvändigt att försöka dra paralleller med vad som gäller i samhället utanför Internet. Genom att försöka fastställa vad som anses lagligt att uttrycka i t ex ett brev som sänds med posten, i ett privat samtal eller i en sluten sammankomst får man vägledning för en bedömning av innehållet på en webbsida. Svårigheten är dock att avgöra vad en tjänsterelaterad webbsida kan jämställas med. Vi ställer oss emellertid frågan om en jämförelse nödvändigtvis måste göras. Idealet, anser vi, borde istället vara att bortse från det aktuella mediets karaktär. Det kan inte anses konsekvent att tillmäta valet av uttrycksmedel så stor betydelse då det i slutändan alltid är en fysisk person som agerar.

Teknik och juridik

Mot bakgrund av ovanstående redogörelse kan man sluta sig till att förmedlaransvaret i såväl svensk som europeisk rätt är oklart. För att ansvar skall kunna rättfärdigas krävs en klar och tydlig reglering. Ansvaret måste stå i proportion till förmedlarens möjligheter att granska servrarnas innehåll. Det är inte möjligt att bortse från de problem som uppstår vid utformningen av teknikrelaterad lagstiftning. Detta framträder tydligt vid en tillämpning av övervakningsansvaret. Vi menar att lagstiftaren inte uppmärksammat samspelet mellan juridik och teknik. Som redan nämnts är informationsflödet på Internet enormt. Möjligheterna för förmedlaren att förhandsgranska all information som vidarebefordras via dennes tjänst är följaktligen minimala. Erfarenheter från förmedlare som använder sig av förhandsgranskning visar vidare att en sådan granskning i praktiken medför en oönskad fördröjning av flödesprocessen.

De utmaningar juridiken står inför kan delas in i två olika områden; kombinationen av juridisk och teknisk sakkunskap samt en tidig integrering av rättsliga lösningar i tekniken. Vi anser inte att det räcker att enbart sammanföra jurister och tekniker då begreppsvärldarna är åtskilda. Risken för missförstånd är stor samtidigt som arbetet kan ta längre tid att slutföra. En helhetsbild där terminologi och synsätt samordnas bör därför eftersträvas. Juridiken bör redan i ett tidigt skede inkorporeras i tekniken. Detaljerade undersökningar av eventuella konsekvenser av en rättslig reglering bör således göras på förhand istället för att utlämnas åt domstolsprövning. Det är följaktligen nödvändigt att söka utröna hur tekniska lösningar på bästa sätt kan anpassas till det rättsliga systemet. Vidare bör hänsyn tas till förmedlares erfarenheter. Detta tillvägagångssätt medför att lagstiftningen lättare kan koncentreras till relevanta praktiska problem och få önskade samhälleliga effekter.

Internationell reglering

Slutligen måste Internets globala karaktär beaktas. Informationen transporteras över gränserna samtidigt som nationell lag idag är geografiskt begränsad. Detta ger upphov till en rad jurisdiktionsproblem. Regleringen bör i möjligaste mån utformas i internationell samverkan.[184]

[184] Yahoo-fallet kan här tänkas bli en accelerator då domslutet knappast kommer accepteras av omvärlden.

Då amerikansk lagstiftning, enligt vår mening, på ett tydligt och proportionerligt sätt reglerar ansvarsproblematiken utgör den en lämplig förebild. Europeiska förmedlare bör ges lika möjligheter, som amerikanska förmedlare, att hävda sig på den Internetrelaterade marknaden.

9.3 PRAKTISKA RÅD

Genom att peka på rådande brister i lagstiftningen vill vi visa att förmedlare idag inte har möjlighet att klart förutse eventuella konsekvenser av sitt handlande.

Vårt första råd till förmedlare är att de bör lägga stor vikt vid utformningen av relevanta avtal. Ansvarsfrågan bör härvid ges en framträdande plats. Det är t ex viktigt att tydligt reglera följderna av att ett meddelande plockas ned felaktigt. Ansvaret bör regleras såväl i förhållande till content provider som till anmälare. Genom att t ex på förmedlarens webbsida tillhandahålla ett standardiserat formulär, för anmälan, utformat som ett avtal, där det skadeståndsrättsliga ansvaret regleras, kan det detta ansvar föras över på anmälaren. Det får dock ej finnas tvivel om avtalets karaktär, rimligtvis kan en acceptklausul tas in i formuläret. Förmedlarens ansvarsreglering i förhållande till användare bör också förklaras i avtalet med content providern.[185] Formuläret bör vidare till viss del reglera anmälans utformning och innehåll. I syfte att underlätta förmedlares bedömning, bör det ställas krav på tydlighet, både med avseende på vem som anmäler samt vad man anser vara lagstridigt.

Vi har tidigare pekat på problemen angående övervakningsskyldighetens överensstämmelse med e-handelsdirektivet. Svårigheten ligger i att kontrollera allt material som passerar på servrarna. I syfte att underlätta en sådan kontroll rekommenderar vi förmedlare att upprätta s k klagomurar. Klagomurarna medför att eventuella olagligheter uppmärksammas på ett tidigt stadium utan att förmedlare själv nödgas övervaka tjänsten aktivt.

Även självreglering och tekniska åtgärder har visat sig vara framgångsrika tillvägagångssätt för brottsbekämpning. Vi anser det vara av vikt för förmedlare att visa ett öppet intresse för minskad brottslighet på Internet. Genom att på både internationell och nationell nivå

[185] Denna klausul kan kompletteras med att förmedlaren alltid förutsätts avlägsna material i god tro i de fall en anmälan ligger till grund för nedtagningen.

samarbeta för att utveckla och förbättra självreglering och tekniska åtgärder skapas ett säkrare Internet. Samarbete samt utväxling av erfarenheter bidrar till ett fortskridande av utvecklingen. Ett öppet intresse för brottsbekämpning skapar likaledes eventuellt möjlighet att vinna lagstiftares och marknadens förtroende vilket medför ökade möjligheter till inflytande.

KÄLLFÖRTECKNING

OFFENTLIGT TRYCK

Offentliga utredningar

SOU 1996:40 Elektronisk dokumenthantering

SOU 1997:49 Grundlagsskydd för nya medier

Propositioner

Prop 1990/91:64 Om Yttrandefrihetsgrundlag mm

Prop 1996/97: 111 Rättsligt skydd för databaser mm

Prop 1997/98:15 Ansvar för elektroniska anslagstavlor

Prop 1999/00:86 Ett informationssamhälle för alla

ÖVRIGT TRYCK

Litteratur

Berggren, Christina, Nätjuridisk guide, Norstedts juridik, 1999

Carlén-Wendels, Thomas, ”Nätjuridik –lag och rätt på Internet”, Norstedts juridik, Stockholm, 1998

Hellner, Jan, ”Skadeståndsrätt”, femte upplagan, Juristförlaget, Gotab Stockholm, 1996

Lehrberg, Bert, ”Praktisk juridisk metod”, 2 upplagan, Graphic Systems AB, Göteborg, 1994

Lindberg, Agne, Westman, Daniel, ”Praktisk IT-rätt”, andra upplagan, Elanders Gotab, Stockholm ,1999

Kelleher, Denis, ”IT-law in the European Union”, Sweet & Maxwell, London, 1999

Periodica

Bogdan, Michael, ”Jurisdiktions- och lagvalsfrågor på Internet, Ny Juridik 4:99

Cahoy, Daniel R, ”Comment: New legislation regarding on-line liability for copyright infringement: a solution in search of a problem?, The Journal of Law and Technology, volume 38, number 2, 1998

Carlinsky, Michael B, Conciatori, Jeffrey A, ”DMCA charts safe harbors in a wired world”, New York Law Journal, Volume 223, Number 108, 2000

Claeson, Daniel, ”Napster i blåsväder efter samarbete”, Göteborsposten 2000-11-01

Josefsson, Dan, ”Fritt fram för rasism och barnporr på nätet i det nya lagförslaget”, Aftonbladet

Linklaters & Alliance, issue 8, Nov 2000

Mayer ,Franz C, ”Europé and the Internet The Old World and the New Medium””, European Journal of International Law 20, Volume 11, 2000

Nathrath, Daniel, ”Criminal liability of Internet Providers in Germany: Conviction of a Compuserve Executive”, Journal of Internet Law,

Palme, Jakob, ”Ett misslyckat lagförslag”, Computer Sweden,

Rosén, Jan, ”Ansvar för utnyttjanden av skyddade prestationer i nätverk”, Svensk juristtidning, 9:2000

Vinje, Thomas C, Paemen, Dieter, ”The European Union’s Electronic Commerce Directive: New rules on On-line Advertising, E-contracting, ISP Liability and Dispute Resolution, World Intellectual Property Report, Volume 14, Number 7, July 2000

Weiner, David, ”Negligent publication on Electronic Bullentin Boards: Is there any liability left after Zeran?”, Santa Clara Law Review, 1999

Wierup, Lasse, ”Flashbacks grundare vägrar backa”, Sydsvenskan

Rapporter

Brinnen, Martin, ”Ansvar och yttrandefrihet i telemedier”, IRI-rapport 1995:2

Post & Telestyrelsen, ”Telelagen och Internet”, Rapport 1999-10-08

Owers, Christoffer, ”Jurisdiktion och lagvalsregler i elektronisk miljö”, IRI-rapport 1997:2, ur Aktuell datarätt, Reprocentralen, Stockholms universitet 1997

Rapport 1998-05-25, ” God etik på Nätet”, En hearing anordnad av IT-kommissionen

Yng, Jörgen, ” Elektronisk handel –En gemensam rättslig ram för EU:s inre marknad”, IRI-rapport 1999:1, ur ”Promemorior IT-rätt”, Institutet för rättsinformatik, Stockholms Universitet, 1999

EG-rättsakter

”Action plan on promoting safe use on the Internet”, Decision No 276/1999/EC

”Green Paper on the protection of minors and human dignity in audiovisual and information services”, COM(96) 483

”Illegal and harmful content on the Internet” COM(1996) 487 COM(1997) 582

Meddelande från Kommissionen till Europaparlamentet enligt artikel 251.2 andra stycket EG-fördraget, 1998/0325 (COD)

RÄTTSFALL MM

Svensk praxis

Justitiekanslerns beslut 1999-08-26, Dnr 2778-99-30

Göta Hovrätt 1998-04-29, dom B 1924/95

Marknadsdomstolens dom MD 1999:18.

NJA 1996 s. 74

NJA 2000 s 292

Svea Hovrätt 1998-09-29, dom DB 101, målnr B 318/97

Utländsk praxis

TYSKLAND

Compuserve GmbH, Amstgericht Munchen 8340 Ds 465 Js 173158/95, 28 Maj 1998

ENGLAND

Laurence Godfrey –and- Demon Internet Limited, Case No: 1998-G No 30, Royal Courts of Justice Strand, London, WC2A 2LL, 1999-03-26

EG-DOMSTOLEN

C-203/80 Casati

C-271/82 Auer

USA

Cubby v. Compuserve, 776 F. Supp. 135 (S.D.N.Y.) 1991

Stratton Oakmount Inc. v. Prodigy Services Company, [1995] WL 323710 (N.Y. Sup. Ct. 1995)

Zeran v.America Online, 958 F. Supp. 1124 (E.D.Va. 1997) appeal 129 F. 3d 327 (4th cir. 1997)

Lunney v. Prodigy Services Company, 683 N.Y.S.2d 557 (A.D.2Dept. 1998), appeal 723 N.E.2d539 (N-Y.Ct.App 1999)

Religious Technology Centre v. Netcom Online Communication Services, Inc., 37 U.S.P.Q.2d (BNA)

Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc., 1997 WL 709747, 45 U.S.P.Q.2d (BNA)

Fonovisa, Inc. v. Cherry Auction, Inc., 76 F. 3d 259, 264, 37 U.S.P.Q2d (BNA) 1590, 1595 (9th Cir. 1996)

INTERNETBASERADE KÄLLOR

”Court cases regarding ISP liability”, http://webreview.com/wr/pub/1999/04/23/platform/cases.html (hämtad 2000-11-09)

ETNO Reflection Document on Jurisdiction and Applicable Law in E-Commerce (Revision of Brussels and Rome Conventions), RD108 11/99, http://www-etno.be/RD/RD108.html (hämtad 2000-09-13)

Europaparlamentets och rådets Direktiv 2000/31/EG av den 8 juni 2000, http://www.infotorg.sema.se/cgi-bin/in…398&docseg=001&hittype=RB&formtype=form.html (hämtad 2000-09-05)

Experts testify in French Yahoo! Case over Nazi memorabilia, November 6, 2000, http://www.cnn.com (hämtad 2000-11-16)

http://www.arl.org/info/frn/copy/band.html (hämtad 2000-09-05)

http://news.bbc.co.uk/hi/english/sci/tech/newsid_364000/364261.stm (hämtad 2000-11-09)

http://www.cyberlaw.se/swedish/elaw-1.htm (hämtad 2000-11-11)

http://www.cyberlaw.se/swedish/elawi-10.htm (hämtad 2000-11-11)

http://www.gcwf.com/articles/journal/jil_nov98_1.html (hämtad 2000-11-09)

http:www.kd.qd.se/safir/ (hämtad 2000-11-08)

http://www.kultur.nu/juridik/itratt_ansvar.html (hämtad 2000-08-31)

http://skolan.presstext.prb.se (hämtad 2000-11-13)

http:// skolan.presstext.prb.se/bin/neta2gate?f=doc&state=25kngv.4.3 (hämtad 2000-11-13)

Web worries over French site ban, November 21 2000, http://www.cnn.com (hämtad 2000-11-22)

Westman, ”MP3-målet i HD –rättsläget kring länkning fortfarande oklart, http://www.juridicum.su.se/IRI/dawe/index.htm (hämtad 2000-09-05)

Yahoo! Anger at French Nazi auction ban, November 21, 2000, http://www.cnn.com (hämtad 2000-11-22)

Användaravtal hämtade på följande företags hemsidor: Altavista, Yahoo Sverige, Everyday.com, Passagen, Utfors AB, HogiaNet, databasen Webbhotellet samt NU Internet.

ÖVRIGA KÄLLOR

Telefonintervjuer samt e-mail med Patrik Hiselius, jurist, Telia

Telefonintervjuer samt e-mail med Jacob Palme, professor i datalingvistik

Intervju samt e-mail med Mattias Klang, vik adjunkt, Göteborgs Universitet

E-mail med Daniel Westman, jur kand, doktorand, Stockholms Universitet

Telefonintervju med Lars Gernhard, advokat, Cederquist Advokatbyrå AB

Telefonintervju med jurist på Post och Telestyrelsen

Telefonintervjuer med flera anonyma källor på Justitie- respektive Näringsdepartementet