Rapport fra møderækken om håndhævelse af ophavsretten på internettet.

Kulturministeriet 25. juni 2009

Jour.nr.: 2004-16736-214

KULTUR MINISTERIET

23. juni 2009

Indholdsfortegnelse:

1. Baggrund

I januar 2007 nedsatte Økonomi- og Erhvervsministeriet en tværministeriel arbejdsgruppe, som fik til opgave at analysere mulighederne for at styrke indsatsen mod piratkopiering på immaterialretsområdet. I marts 2008 afgav arbejdsgruppen sin rapport[1].

En af de problemstillinger, som beskrives i rapporten, er håndhævelse af ophavsretten på internettet, herunder særligt i forhold til ulovlig fildeling og downloading, hvor det blandt andet drøftes, om de nuværende håndhævelsesmuligheder er tilstrækkelige.

Det fremgår af rapporten, at arbejdsgruppen har set på, hvorvidt der er behov for, at internetudbyderne får en mere aktiv og udfarende rolle i kampen mod piratkopiering, end det er tilfældet i dag. I den forbindelse blev mulighederne for at forpligte internetudbyderne til at lukke brugernes internetforbindelser, når der gentagne gange konstateres ulovlig fildeling eller downloading, nævnt.

Arbejdsgruppen nævner i sin rapport, at en sådan forpligtelse rejser nogle umiddelbare betænkeligheder i relation til borgernes retssikkerhed, herunder spørgsmål om utilsigtede konsekvenser for den enkelte forbrugers kommunikationsmuligheder.

Arbejdsgruppen anbefalede, at man følger igangværende initiativer i blandt andet Frankrig, Sverige og EU.

Arbejdsgruppen anbefalede endvidere, at der gennemføres en analyse af de nuværende og fremtidige tekniske løsninger til at blokere for hjemmesider og fildelingssystemer samt vurdere de mulige konsekvenser heraf, herunder ved en belysning af udviklingen i Frankrig, Sverige og EU.

Den 8. maj fremsatte Socialdemokratiet og SF forslag til Folketingsbeslutning om oprettelse af et klagenævn for ophavsrettigheder på internettet (B 137). Beslutningsforslaget gik efter sin ordlyd ud på at "pålægge regeringen inden udgangen af 2008 at oprette et klagenævn, der kan vurdere mulige ophavsretskrænkelser på internettet og eventuelt pålægge telekommunikationsindustrien at blokere links til internetsider, der muliggør krænkelse af ophavsrettigheder".

I forbindelse med Folketingets behandling af beslutningsforslag B 137 tilkendegav kulturministeren, at "Kulturministeriet som opfølgning på rapporten gennemfører en møderække for bl.a. at få identificeret og analyseret de tekniske løsninger til at lukke ulovlige hjemmesider og fildelingssystemer yderligere. Vi vil samtidig følge udviklingen i andre lande. Det er vigtigt at få afdækket alle de praktiske, økonomiske og retssikkerhedsmæssige konsekvenser af forskellige modeller, hvor internetudbydere pålægges særlige forpligtelser til at blokere for hjemmesider." På den baggrund tilkendegav ministeren afslutningsvist, at "det er for tidligt på nuværende tidspunkt at træffe

[1] Rapport fra arbejdsgruppen om en styrket indsats mod piratkopiering, marts 2008
http://www.dkpto.dk/udvikling/RapportPiratkopiering.pdf

beslutning om nedsættelse af et nyt nævn, der skal vurdere krænkelser på internettet." Beslutningsforslaget blev ikke vedtaget.

På denne baggrund påbegyndte Kulturministeriet i maj 2008 en møderække med deltagelse af de væsentligste aktører på området.

I møderækken deltager: IFPI, Forlæggerforeningen, Samrådet for ophavsret, Dansk Skuespillerforbund, Telekommunikationsindustrien i Danmark, herunder repræsentanter fra ITB, TI samt DI ITEK, Forbrugerrådet, Advokatsamfundet, Justitsministeriet, IT- og Telestyrelsen, samt Økonomi- og Erhvervsministeriet, herunder Patent- og Varemærkestyrelsen, samt Kulturministeriet (formand).

Nærværende rapport udgør møderækkens afrapportering til kulturministeren.

Den 26. september 2008 blev kulturministeren kaldt i samråd i Folketingets Europaudvalg med henblik på at redegøre for regeringens holdning til Kommissionens meddelelse om kreativt online-indhold på det indre marked, herunder kommentere det aftalememorandum, der i efteråret 2007 blev indgået i Frankrig mellem musik- og filmproducenter, internetudbydere og den franske regering. Ministeren tilkendegav her, at regeringen finder, at piratkopiering på internettet er et stort problem, og at regeringen finder det relevant at se nærmere på problemstillingen omkring ulovlige downloads og fildeling. I første omgang sker dette i form af en møderække under Kulturministeriet, hvor de involverede interessenter afdækker det faktuelle grundlag for problemstillingen, herunder de engelske og franske initiativer. Derved får politikerne et grundlag for at vurdere, om der er behov for yderligere initiativer.

Den 28. november 2008 besvarede kulturministeren et § 20 spørgsmål fra medlem af Folketinget Mogens Jensen (S) vedrørende Ministerrådets behandling af Kommissionens meddelelse om online-indhold,hvor der blev spurgt: "Hvad har ministeren tænkt sig at gøre for at følge op på disse rådskonklusioner om kreativt indhold, bl.a. bekæmpelse af piratkopiering, der er behandlet på rådsmødet den 20.- 21. november 2008, for at sikre, at målsætningerne i dokumentet bliver nået?" Kulturministeren svarede hertil blandt andet følgende: " Det fremgår af rådskonklusionerne, at det er vigtigt, at alle relevante parter går sammen i dialog om at bekæmpe piratkopiering. I den forbindelse kan jeg nævne, at Kulturministeriet i maj 2008 nedsatte en møderække med særlig fokus på ulovlig downloading og fildeling af ophavsretlig beskyttet materiale. Når vi har fået konklusionerne fra møderækken, vil regeringen overveje, om det system, vi har i dag, fungerer godt nok, eller om der er behov for at se nærmere på yderligere tiltag. Jeg forventer at orientere ordførerne nærmere herom, og indbyde til brede politiske drøftelser, såfremt der er behov for yderligere tiltag."

2. Møderækkens formål og fokusområder

Møderækkens hovedformål er som nævnt at undersøge de tekniske muligheder for at identificere ophavsretskrænkelser på internettet samt de tekniske muligheder for at

blokere for disse krænkelser. Samtidig har det – i forlængelse af kulturministerens tilkendegivelser til Folketinget i forbindelse med behandlingen af B 137 - været relevant at redegøre for de retsregler, som regulerer området og – så vidt det har været realistisk muligt indenfor møderækkens rammer – at skabe et overblik over de praktiske, økonomiske og retssikkerhedsmæssige overvejelser, som det vil være relevant at foretage i forbindelse med drøftelser af eventuelle initiativer. Endelig har møderækken haft til formål at indhente relevante erfaringer fra andre lande.

Det er i den forbindelse vigtigt at understrege, at møderækken ikke har haft i opdrag at fremkomme med konkrete anbefalinger til eventuelle yderligere initiativer i relation til håndhævelse af ophavsretten på internettet. Møderækkens rapport har således udelukkende karakter af en faktuel udredning og indeholder ikke konkrete anbefalinger eller initiativer. Møderækkens deltagere har selvsagt derfor heller ikke taget stilling til hensigtsmæssigheden af de mulige håndhævelsestiltag, der faktuelt omtales i rapporten.

2.1 Rapportens opbygning

Rapporten indledes med en præsentation af møderækkens formål og fokusområder, herunder en nærmere beskrivelse af rapportens opbygning. Herefter redegøres for omfanget af ulovlig fildeling i Danmark i afsnit 3. I afsnit 4 beskrives de konkrete typer af ophavsretskrænkelser, som møderækken har drøftet.

Af fremstillingstekniske hensyn inddeles behandlingen af ophavsretslige krænkelser i to overordnede faser: efterforskning/bevissikringsfasen samt reaktionsfasen. I de følgende afsnit vil disse faser blive behandlet særskilt. Først beskrives efterforskning/bevissikring i afsnittene 5 – 8, herefter beskrives reaktionsfasen i afsnit 9 - 12.

Systematikken, som anvendes til at behandle de to faser, er følgende: en beskrivelse af de tekniske muligheder som efterfølges af et afsnit om gældende regler. Herefter beskrives relevant dansk retspraksis. Disse beskrivelser sammenholdes i et særskilt opsamlingsafsnit, hvorefter der redegøres for de retssikkerhedsmæssige betragtninger, som vil være relevante i forhold til drøftelser om fremtidige tiltag.

Som led i arbejdet med denne rapport har møderækken undersøgt, hvilke erfaringer andre lande har på dette område. Resultatet af disse forespørgsler findes i afsnit 13. Møderækkens deltagere har herudover fundet det relevant, at kigge på en række overvejelser om bl.a. retssikkerhed. Disse overvejelser fremgår af afsnit 13.1.

3. Omfanget af ulovlig fildeling i Danmark

Forbrugerrådet gennemførte i februar 2009 en undersøgelse blandt 1.101 forbrugere om digital adfærd. Undersøgelsen spørger ind til forbrugernes vaner i forbindelse med kopiering og download af musik i fysisk og digital form. Herudover spørger undersøgelsen fra 2009 ind til forbrugernes holdninger til kopispærringer på musik og film.

Undersøgelsen fra 2009 viser, at lovlig kopiering, så som kopiering af egne cd'er til sommerhuset, er udbredt blandt mere end halvdelen af forbrugerne, men at ulovlig kopiering også finder sted, fx har en tredjedel af forbrugerne kopieret fysiske cd'er, de har lånt fra biblioteket eller venner.

Hver femte forbruger angiver at have kopieret musik, de selv har købt til personer udenfor deres husstand. Næsten hver anden forbruger har modtaget kopier af musik fra personer udenfor deres husstand. Begge tendenser er på niveau med Forbrugerrådets undersøgelse fra 2007[2], hvor lignende spørgsmål blev stillet til forbrugerne.

Ifølge undersøgelsen fra 2009 finder den ulovlige tilgængeliggørelse og fildeling via internettet sted i mindre omfang end den ulovlige kopiering af fysisk materiale. Ifølge undersøgelsen har meget få af de adspurgte erfaring med at up- eller downloade musik fra fildelingshjemmesider. Dette kan dog formentlig forklares ved, at forbrugere i alderen 18-30 år er underrepræsenteret i undersøgelsen.

I Forbrugerrådets undersøgelse fra 2007 angav 13 % af forbrugerne, at de havde erfaring med at downloade værker fra hjemmesider, mens 2 % af de adspurgte angav selv at have stillet musik til rådighed for andre på fildelingshjemmesider. I 2007 angav 5 % af de adspurgte endvidere, at de havde sendt digitale kopier af musik eller videoklip til andre via e-mail, mens kun 0,8 % af de adspurgte havde solgt digitale kopier af musik. Disse tal siger dog ikke noget om, hvorvidt der er tale om ulovlig fildeling.

Download og tilgængeliggørelse af filer på fildelingshjemmesider er ikke nødvendigvis ulovligt. Lovlig tilgængeliggørelse og eksemplarfremstilling af beskyttet materiale kræver, at brugeren indhenter tilladelse fra rettighedshaveren til brugen. Den ulovlige kopiering finder sted i alle aldersgrupper, men særligt i de yngre grupper og både hos mænd og kvinder. Det er mere udbredt at tage ulovlige kopier til sig selv, end det er at tage ulovlige kopier til personer uden for sin husstand. Det til trods har over halvdelen af de adspurgte selv modtaget hjemmebrændte kopier af musik fra andre.

En meningsmåling fra august 2008 foretaget af Greens Analyseinstitut[3] indikerer, at hver femte dansker har hentet ulovlige musikfiler på internettet. Meningsmålingen indikerer også, at antallet af danskere, der downloader ulovlig musik, er vokset med fem procentpoint på et halvt år.

Der findes på nuværende tidspunkt ingen statistisk oversigt over det faktiske omfang af piratkopiering i form af ulovlige downloads og fildeling. OECD offentliggør i løbet af foråret 2009 en undersøgelse af problemerne med digital piratkopiering.

Denne undersøgelse har i første omgang til formål at identificere, hvilke markeder, der er berørt af digital piratkopiering. Herudover har undersøgelsen til formål at beskrive brancheinitiativer og gældende lovgivningsmæssige rammer.

---

[2] http://www.forbrugerraadet.dk/emner/internet/alle/digitalerettigheder/musikdownload2007

[3] Jf. artikel af Susan Grønbech, Børsen d. 26. august 2008.

En egentlig klarlæggelse af omfanget af problemet med digital piratkopiering vanskeliggøres af, at der er tale om ulovlige aktiviteter, som ikke systematisk registreres nogen steder. Dette er også påpeget af OECD, som henviser til, at den begrænsede tilgængelighed af troværdig information vedrørende digital piratkopierings kvantitative omfang har betydet, at en planlagt beskrivelse af det faktiske omfang af digital piratkopiering ikke gennemføres på nuværende tidspunkt[4].

Desuden er der forskel på digital og fysisk piratkopiering, idet myndighederne har mulighed for til en vis grad, at kontrollere og tilbageholde mistænkelige fysiske produkter, når disse krydser landegrænser. Den samme mulighed eksisterer ikke ved ulovlig fildeling, hvor filerne transporteres via internettet.

Rapporten fokuserer på, at udfordringerne i forbindelse med digital piratkopiering på en række punkter adskiller sig fra piratkopiering af fysiske produkter. Rapporten beskriver de særlige karakteristika ved digitale markeder.

Nogle af de punkter OECD-rapporten udpeger som særegne for det digitale marked er fx, at grænsen mellem forbruger og udbyder af materiale ikke er særlig skarp. I et fildelingssystem vil brugeren således ofte både downloade og tilgængeliggøre materiale. Hertil kommer at de brugere, der tilgængeliggør værkerne, ofte ikke har et økonomisk incitament for tilgængeliggørelsen. Brugerne opererer efter helt andre parametre, som fx social anerkendelse i en gruppe af fildelere eller som gengæld i forhold til andre brugere, der også tilgængeliggør værker gratis.

Modsat markedet for fysiske kopier, skal rettighedshaverne på det dynamiske marked ikke kun konkurrere med kopi-produkter, der sælges til en lavere pris end originalen. På det digitale marked skal rettighedshaverne konkurrere med kopi-produkter der tilbydes gratis. Det er OECD's vurdering, at ikke-økonomiske faktorer, som fx lovlighed, tilgængelighed og kvalitet derfor er særligt vigtige for de udbydere der, med rettighedshavernes tilladelse, stiller digitale værker til rådighed mod betaling.

Ifølge OECD, opfatter størstedelen af de brugere der tilgængeliggør ulovligt materiale, ikke sig selv som pirater. På trods af at størstedelen af brugerne er klar over, at digitalt pirateri er ulovligt, bliver de ulovlige handlinger ikke opfattet som uetiske, fordi brugerne ikke opfatter de ulovlige handlinger som tabsgivende for rettighedshaverne. OECD peger på, at antallet af brugere, der tilgængeliggør ulovligt materiale, er vokset eksplosivt. Det er derfor OECD's vurdering, at det er blevet langt sværere og mere omkostningstungt for rettighedshaverne at håndhæve deres rettigheder. Hertil kommer, at brugerne opererer på et globalt plan, det vil sige i forskellige lande, hvor lovgivningen vedrørende ophavsrettigheder er forskellig. Brugerne er meget fleksible, og kan forholdsvis hurtigt flytte ulovlige aktiviteter til lande med en svag ophavsretslovgivning.

Herudover fremhæver OECD, at produktions- og leveringsomkostninger er væsentlig lavere ved digital piratkopiering end ved fysisk piratkopiering. Dette gør det særligt

[4] OECD, Phase II, Piracy of digital content, forventes offentliggjort i foråret 2009.

attraktivt at dele digitale produkter. Teknologi, som fx peer-to-peer-systemer, hjælper brugerne med at dele digitalt materiale på en nem og hurtig måde, og internettets struktur gør det let at finde kilder til digitalt materiale. Hertil kommer, at det digitale marked på internettet har et kæmpemæssigt potentiale på grund af internettets globale natur.

OECD kommer på baggrund af rapporten med en række anbefalinger til beslutningstagerne og industrien/rettighedshaverne. OECD påpeger, at problemerne med pirateri på det digitale marked er unikke i forhold til de problemer rettighedshaverne har i forbindelse med fysisk piratkopiering, og at digitalt pirateri kan mangedoble de problemer, piratkopieringen skaber for både beslutningstagere og producenter af digitale produkter.

OECD peger på, at de eksisterende love ofte er meget generelle og ikke i fornødent omfang kan anvendes på problemstillingen, bl.a. på grund af den hurtige teknologiske udvikling. Herudover peger OECD på, at det er vigtigt, at der bliver taget hånd om problemstillingen uden unødig påvirkning af lovlige aktiviteter på nettet, herunder påvirkning af brugernes adgang til internettet som platform for kommunikation, handel og læring. OECD henviser i denne forbindelse til deklarationen fra Seoul fra 2008.[5] Desuden understreger OECD behovet for oplysning og undervisning.

OECD anbefaler, at retshåndhævelse fortsat er en vigtig del af den overordnede strategi vedrørende piratkopiering. Det er dog OECD's opfattelse, at retshåndhævelse på længere sigt ikke vil være effektivt på grund af det store antal af brugere, der krænker ophavsretten. Derfor anbefaler OECD, at der tages andre tiltag i brug, som fx nye typer af sanktioner og undervisning. OECD anbefaler, at sådanne tiltag opretholder en balance mellem rettighedshavers, brugernes og mellemmændenes interesser.

OECD peger herudover i sine anbefalinger på, at brugernes holdning til internetpirateri skal ændres bl.a. gennem information og undervisning og udvikling af lovlige alternative forretningsmodeller. På grund af internettets globale natur anbefaler OECD, at undervisning og information også sker på tværs af landegrænser. OECD anbefaler, at beslutningstagerne målretter informations- og undervisningsarbejdet, så brugerne får hjælp til at finde ud af, hvad der er lovligt og ulovligt på internettet.

Ifølge IFPI kan udviklingen i de lovlige downloads af musik give indikationer for omfanget af piratkopieringen på området. IFPI's tal viser, at der i 2003 på verdensplan var ca. 50 hjemmesider, der lovligt solgte digital musik online. I 2007 var dette tal steget til over 500 hjemmesider.[6] I 2007 downloadede forbrugerne lovligt musiknumre 1,7 milliarder gange på verdensplan, hvilket var en stigning på 53 % i forhold til 2006.[7] I 2008 udgjorde det lovlige online salg af digital musik 20 % af musiksalget på verdensplan, hvilket er en stigning på 5 % i forhold til 2007.[8] IFPI oplyser i Digital Music Report

[5] OECD (2008e)
[6] IFPI, Digital Music Report 2008.
[7] IFPI, Digital Music Report 2008.
[8] IFPI, Digital Music Report 2009.

2009, at salget af lovlige downloads rundede 100 mio. i 2008[9]. IFPI vurderer i samme rapport, at 95 % af den musik der downloades på verdensplan, bliver downloaded uden rettighedshavernes tilladelse, og dermed uden at der betales vederlag til rettighedshaverne.

4. Hvordan sker ulovlig tilgængeliggørelse?

Det overordnede fokusområde for møderækken er den systematiske ulovlige fildeling og ulovlige kopiering af ophavsretligt beskyttet materiale, særligt musik, film og tv-serier, som foregår via internettet.

Ophavsretsloven tildeler ophavsmænd og udøvende kunstnere en række enerettigheder. Ophavsmanden har eneret til at lave eksemplarer af sine værker og til at gøre værkerne tilgængelige for offentligheden, fx via internettet. Rettigheder til musikværker er i mange tilfælde overdraget til andre, fx et plade- eller forvaltningsselskab, der helt eller delvist repræsenterer rettighederne i stedet for eller på vegne af ophavsmanden eller den udøvende kunstner. Der skal indhentes samtykke fra rettighedshaver, inden digitale værker kopieres til andet end personlig brug[10], og inden værker gøres tilgængelige på internettet.

Det ophavsretligt beskyttede materiale, der distribueres via internettet kan omfatte en lang række forskellige produkter, lige fra musik og film, til tv-serier og litterære tekster m.v. Værkerne er beskyttet af ophavsretsloven[11], som bl.a. regulerer adgangen til up- og downloading fra internettet, samt tilgængeliggørelse af de beskyttede værker.

Brugen af ophavsretligt beskyttet materiale på internettet er varieret og ændres dagligt. Der sker en konstant udvikling af mulighederne for fx at se tv live, uploade egne værker og kommentere på andres værker mv. Derudover sker der også en hastig udvikling i mulighederne for at informere andre brugere om eksisterende værker og endda gøre disse værker tilgængelig for andre brugere fx på blogs, via e-mails og via fildeling.

Møderækken har fokuseret på ulovlig tilgængeliggørelse. Ulovlig tilgængeliggørelse dækker den situation, hvor en person selv lægger materiale ud på internettet til fri afbenyttelse uden nødvendigt samtykke fra rettighedshaverne.. Konkret har møderækken drøftet de to fremgangsmåder, som ifølge IT- og Telestyrelsen er dem, der oftest anvendes til organiseret ulovlig tilgængeliggørelse på internettet:

- tilgængeliggørelse via centrale servere og
- tilgængeliggørelse via fildelingsnetværk baseret på peer-to-peer teknologi.

Det kræver en tilladelse fra rettighedshaver, hvis man vil kopiere og dele (tilgængeliggøre) filer, som indeholder ophavsretligt beskyttet materiale fx et musiknummer med

[9] IFPI, Digital Music Report 2009
[10] Ophavsretslovens § 12 indeholder en regel om eksemplarfremstilling til privat brug. Eksemplarfremstilling af digitale værker til privat brug må ske til brug for fremstilleren og dennes husstand.
[11] Lovbekendtgørelse nr. 587 af 20. juni 2008 (lov om ophavsret).

personer udenfor ens husstand.. Har man ikke denne tilladelse, vil det udgøre en krænkelse af ophavsretsloven, hvis filen gøres tilgængelig på internettet eller kopieres. Krænkelse af ophavsretten på internettet kan dermed begås af to typer af aktører:

- En aktør der på uretsmæssig vis gør ophavsretligt beskyttet materiale **tilgængeligt** for andre via internettet.

- En aktør der på uretsmæssig vis anskaffer sig, dvs. downloader og dermed **kopierer** ophavsretligt beskyttet materiale via internettet.

Krænkelse af ophavsretten i form af ulovlig **tilgængeliggørelse** kan teknisk dokumenteres, særligt hvis materialet bliver stillet til rådighed ved brug af fildeling gennem såkaldte peer-to-peer[12] systemer som eksempelvis BitTorrent[13], hvor det eksplicit er muligt at se, hvilket materiale der bliver tilgængeliggjort. Dette beskrives nærmere i afsnit 4.2.

Den anden type krænkelse, den uretmæssige **download/kopiering,** foregår ved en relativt kortvarig og skjult download-aktivitet gennem internettet. Teknisk dokumentation af download/kopiering vil derfor skulle ske på anden måde end ved dokumentation af tilgængeliggørelse. Konkret vil teknisk dokumentation af ulovlig download/kopiering, alene være teknisk muligt, hvis man løbende analyserer indholdet[14] i brugeres internettrafik fra centrale servere eller fra peer-to-peer systemer.

I lyset af mængden af trafik på internettet, samt kompleksiteten heraf, vil en sådan løbende analyse formentlig være så omfattende, at den ikke vurderes at være økonomisk realistisk at implementere. Desuden vil der formentlig være betragtelige retssikkerhedsmæssige udfordringer i at gennemføre en løbende og generel analyse af indholdet i en brugers internetkommunikation.

Møderækken har drøftet de to måder, som ifølge IT- og Telestyrelsen oftest anvendes til organiseret ulovlig tilgængeliggørelse på internettet: tilgængeliggørelse via centrale servere samt via fildelingsnetværk baseret på peer-to-peer teknologi. Nedenfor følger en beskrivelse af, hvorledes den ulovlige tilgængeliggørelse foregår henholdsvis via centrale servere og via fildeling (peer-to-peer teknologi).

---

[12] Peer-to-peer (eller P2P) anvendes oftest som betegnelse for et computernetværk der bruger forskellige tilslutningsmuligheder mellem brugerne i et netværk og anvender brugernes kumulative båndbredde på nettet. Brugerne har ofte begrænsede sendehastigheder (upload) i forhold til modtagehastigheder (download). I stedet for at brugeren henter data fra én central server, hentes i stedet små mængder data fra et utal af andre brugere.

[13] BitTorrent er en peer-to-peer fildelingsprotokol, der bruges til at distribuere store mængder data.

[14] Det er i denne forbindelse vigtigt at være opmærksom på, hvad der skal betragtes som værende 'indhold', og hvad der skal betragtes som værende 'trafikdata' for en brugers internetkommunikation. 'Trafikdata' er alene de data, der specifikt er nødvendige for at kunne fremføre brugerens internetkommunikation. Alle øvrige data skal betragtes som værende 'indhold' af brugerens internetkommunikation.

4.1 Ulovlig tilgængeliggørelse via centrale servere

En central server er hjemsted for såvel tilgængeliggørelse som download/kopiering, idet systematikken bag en central server er som følger:

Den centrale server fungerer som et sted, hvor filer opbevares, eller hvor der kan være henvisninger til filernes placeringer på andre servere.

Internetbrugere, som ønsker at tilgængeliggøre materiale, kan lægge materialet ud på en central server eller lægge et link på en hjemmeside, der er tilknyttet den centrale server. Tilgængeliggørelse af ophavsretligt beskyttet materiale på denne måde er ulovlig, såfremt det sker uden rettighedshavernes samtykke.

Fordelen ved centrale servere for internetbrugere, som vil downloade/kopiere materiale, er, at internetbrugeren kan gå ind på en bestemt hjemmeside (der er knyttet til én central server), søge på en bestemt fil og downloade den direkte fra hjemmesiden eller via henvisningen (link) til andre hjemmesider/servere. Derved får internetbrugeren adgang til et meget bredt repertoire af ophavsretligt beskyttet materiale blot ved at bruge en enkelt hjemmeside.

Denne fordel for internetbrugeren udgør samtidig et særligt problem for rettighedshaverne. Et bredt repertoire af ophavsretligt beskyttet materiale samlet på et sted gør det muligt at foretage et stort antal krænkelser på meget kort tid.

4.2 Ulovlig tilgængeliggørelse via peer-to-peer systemer

Som udgangspunkt er fildeling et lovligt og effektivt teknisk redskab, der kan anvendes til at sende store mængder data til enkelte brugere, fordi man i realiteten deler båndbredde med andre brugere og derved får en bredere internetforbindelse, som kan modtage større mængder data, end hvis man ikke anvendte fildeling.

Fildeling foregår via peer-to-peer teknologi, som kan benyttes til mange legale formål, idet denne teknologi giver en optimal udnyttelse af internettet. Derfor er fildeling en afgørende bestanddel ved fx web-tv, IP-telefoni og anden aktivitet på internettet, hvor store datamængder er i hurtig bevægelse.

Peer-to-peer teknologi kan imidlertid også anvendes til ulovlige formål, nemlig tilgængeliggørelse af ophavsretligt beskyttet materiale uden rettighedshavers samtykke.

Peer-to-peer teknologien består af et netværksprogram, som internetbrugeren selv installerer på sin computer. Netværksprogrammet bruges til at tilgængeliggøre og downloade filer. Denne automatiske dobbeltfunktion er grundstenen i fildelingsnetværket, og derfor beskrives begge funktioner kort nedenfor.

Netværksprogrammet gør det muligt for internetbrugeren at kommunikere direkte med alle andre internetbrugere på netværket. Dermed er det muligt at få et overblik over alle de filer, som ligger tilgængelige på de computere, der er koblet på netværket i hele

verden. Herefter kan internetbrugeren downloade[15] enkelte filer direkte fra andre brugeres computere uden at skulle igennem en central hjemmeside. Det betyder, at en dansk bruger kan få adgang til musikfilerne på fx en australsk brugers computer, hvis begge brugere har installeret det samme netværksprogram. Det betyder også, at internetbrugeren, som har installeret netværksprogrammet ofte[16] vil have gjort alle sine fx musikfiler tilgængelige på internettet for andre netværksbrugere blot ved at være koblet til netværket. Et eksempel på et fildelingsnetværk baseret på peer-to-peer teknologi er "BitTorrent".

Fildelingsnetværk giver, på samme måde som de centrale servere, potentielle krænkere adgang til et bredt repertoire af ophavsretligt beskyttet materiale. Dermed er udfordringen for rettighedshavere, at potentielle krænkere har let adgang til at foretage et større antal krænkelser på kort tid. Samtidig indebærer fildelingsnetværk den særlige udfordring, at de ikke kan blokeres gennem en enkelt blokering, som centrale servere kan.

Strukturen i et fildelingsnetværk er uden en teknisk central. Såfremt rettighedshaver ønsker at stoppe fildelingen i et netværk, må rettighedshaver derfor henvende sig enkeltvis til samtlige brugere af netværket. Dette indebærer en særlig ressourcemæssig udfordring såvel økonomisk som tidsmæssigt.

5 Efterforskning af ulovlig tilgængeliggørelse på internettet

Rettighedshaverne kan bl.a. håndhæve ophavsretten ved at forsøge at få den, der krænker ophavsretten, idømt en straf og/eller pligt til at betale erstatning.

Strafferetlig håndhævelse af ophavsretten sker som udgangspunkt gennem privat påtale. Rettighedshaverne har således mulighed for at rejse straffesag efter reglerne om privat påtale i ophavsretslovens § 76 stk. 1, jf. § 81 stk. 1. Rettighedshaverne kan i stedet vælge at rejse en civil sag med krav om forbud eller erstatning.

Hvis der er mistanke om, at krænkelsen er begået forsætligt og under visse skærpende omstændigheder, er der betinget offentlig påtale[17]. Det betyder, at rettighedshaveren kan fremsætte begæring om offentlig påtale. Herefter behandles sagen på samme måde som andre sager, der er undergivet offentlig påtale. Det er således politiet, der efterforsker sagen.

Hvis almene hensyn kræver det, kan politiet af egen drift efterforske en overtrædelse af de ophavsretlige regler og anlægge en straffesag ved domstolene, uden at rettighedshaver har bedt om det (offentlig påtale[18]). Der foreligger bl.a. almene hensyn, når kræn-

[15] Ved denne download skaber internetbrugeren en kopi – et nyt eksemplar af filen. Det er ulovligt, hvis den fil, som bliver kopieret, er gjort tilgængelig uden rettighedshavers samtykke.
[16] Det er ved visse peer-to-peer systemer muligt at ændre indstillingerne i systemet således, at man har mulighed for at downloade uden at gøre egne musikfiler tilgængelige for andre brugere.
[17] Ophavsretsloven § 82.
[18] Retsplejeloven § 727, stk. 2 samt ophavsretsloven § 82. I visse sager er der altid offentlig påtale jf. § 81, stk. 4 og 5.

kelsen fx vedrører betydelige økonomiske beløb, samfundsmæssige interesser, eller når der er risiko for borgernes sikkerhed og sundhed.

Som udgangspunkt er det rettighedshavers opgave at være opmærksom på eventuelle krænkelser, tage skridt til at dokumentere krænkelsen og indbringe eventuelle krænkelser for domstolene, som herefter træffer beslutning om idømmelse af sanktioner, erstatning, godtgørelse og tilintetgørelse m.v. ud fra de gældende regler i henholdsvis ophavsretsloven og straffeloven.

Rettighedshaverne laver i dag en del opsøgende arbejde for at opspore eventuelle krænkelser. Dette sker bl.a. ved, at rettighedshaveren installerer netværksprogrammer baseret på peer-to-peer teknologi og søger efter konkrete ophavsretligt beskyttede titler, som rettighedshaveren har rettighederne til. Denne søgning sker på lige fod med andre brugere af netværket. Resultatet af søgningen giver rettighedshaveren viden om, hvorvidt en konkret fil bliver tilgængeliggjort via netværket uden rettighedshaverens samtykke.

Når rettighedshaverne har fundet en udbyder af den aktuelle fil, kan rettighedshaverne identificere udbyderens IP-adresse. Udbyderens IP-adresse er offentlig tilgængelig information på netværket og kan identificeres af alle brugere af netværket. Herefter kan rettighedshaveren gå til domstolene for at få udleveret oplysninger fra internetudbyderen om, hvilken abonnent, der brugte IP-adressen på det konkrete tidspunkt. Disse oplysninger kan efterfølgende bruges til at dokumentere en krænkelse ved en senere retssag.

I afsnit 15 gennemgås de tekniske muligheder for at efterforske og foretage bevissikring for uretmæssig tilgængeliggørelse af ophavsretligt beskyttet materiale via peer-to-peer systemer samt via centrale servere på internettet.

I afsnit 6 og 7 præsenteres det relevante regelgrundlag samt nyere dansk retspraksis.

5.1 Tekniske muligheder for efterforskning ved peer-to-peer systemer

Det er muligt at foretage en løbende, manuel undersøgelse af alt det materiale, der bliver tilbudt gennem de forskellige peer-to-peer systemer på internettet med henblik på at dokumentere mulige krænkelser af ophavsretten.

En manuel fremgangsmåde til bevissikring vil imidlertid ikke være en realistisk metode til håndhævelse af ophavsrettigheder på internettet, da disse undersøgelser ofte vil være ressourcetunge både tidsmæssigt og økonomisk. En effektiv dokumentation af mulige krænkelser vil oftest kunne opnås gennem en automatisk undersøgelsesproces i de forskellige peer-to-peer systemer på internettet.

5.1.1 Automatiske undersøgelsessystemer

Et automatisk undersøgelsessystem er baseret på et specielt udviklet softwareprogram. Dette softwareprogram kan installeres på en almindelig PC, der har adgang til inter-

nettet. Systemet fungerer ved, at PC'en automatisk indhenter oplysninger om, hvilket materiale, der tilbydes via peer-to-peer systemer på internettet.

Det automatiske undersøgelsessystem vil alene kunne få adgang til frit tilgængeligt materiale, som brugerne har offentliggjort på internettet via peer-to-peer systemer. Systemet indsamler alene oplysninger, som er offentlig tilgængelige, og som også ville kunne indsamles ved en manuel søgning – på samme måde, som hvis man gik en tur på hovedgaden og kiggede på de varer, som butikkerne udstillede i deres vinduer og noterede, hvad der var i vinduet.

Systemet indsamler bl.a. IP-adresser[19], som er en offentlig og frit tilgængelig oplysning. Udveksling og tilgængeliggørelse af IP-adresser er en forudsætning for teknisk at kunne anvende internettet.

5.1.2 Konstatering af ulovlig fildeling

Et automatisk undersøgelsessystem kan fastslå filnavn og Hash-værdi[20] for filer i et peer-to-peer system. Herudover kan systemet indsamle oplysninger om de IP-adresser[21], som på undersøgelsestidspunktet fremtræder som afsendere af materiale. Disse oplysninger kan være det første skridt på vejen til at dokumentere krænkelser af ophavsretten ved fildeling på internettet.

Det vil være muligt for det automatiske undersøgelsessystem at identificere materiale, som potentielt krænker ophavsretten og som via det ovenfor omtalte peer-to-peer system kan hentes fra konkrete IP-adresser. Identifikationen kan ske ud fra en database med relevante oplysninger om ophavsretligt beskyttet materiale (en såkaldt blacklist).

Det næste skridt på vejen kan være, at det automatiske undersøgelsessystem, via peer-to-peer systemet på internettet, kontakter de konkrete PC'er[22], som på undersøgelsestidspunktet anvendte de pågældende IP-adresser, og anmoder om at få kopier af materiale, som potentielt krænker ophavsretten.

Når dette materiale er blevet modtaget, kan undersøgelsessystemet verificere, hvorvidt det indhentede materiale via peer-to-peer systemet er identisk med et bestemt materiale, som er beskyttet af ophavsretten.

---

[19] Se uddybende forklaring i Annex II "lidt om IP-adresser"

[20] En Hash-værdi er et tal, der populært sagt er et slags 'elektronisk koncentrat' for en fil. Se en uddybende forklaring i Annex I "lidt om Hashværdier".

[21] IP-adressen er PC'ens "navn" på internettet. Teknisk set tildeles en IP adresse til en konkret internettilslutning og ikke selve den fysiske PC. Da flere PC'ere kan anvende den samme internettilslutning kan der sagtens være flere PC'er bag en given IP-adresse. Se uddybende forklaring i Annex II "lidt om IP-adresser"

[22] Denne kontakt sker ved at det automatiske undersøgelsessystem retter henvendelse til en IP-adresse, som automatisk dirigerer henvendelsen videre til den konkrete computer, som anvender den pågældende IP-adresse. Det er ikke muligt for det automatiske undersøgelsessystem at spore denne videredirigering.

Denne proces vil typisk starte med en hurtig sorteringsproces, hvor filnavn eller væsentlige dele af filnavnet og Hash-værdi for det hentede materiale fra peer-to-peer systemet bliver sammenlignet med de tilsvarende oplysninger på listen (databasen) over det materiale, som er ophavsretligt beskyttet.

Sammenfald mellem filnavn (eller dele af filnavn) og/eller Hash-værdi for det materiale, der er hentet fra peer-to-peer systemet og et emne på listen over ophavsretligt beskyttet materiale betyder ikke, at der teknisk set er identitet mellem de to filer. Det konstaterede sammenfald giver alene en formodning om, at der er identitet mellem to filer. Egentlig identitet mellem to filer vil rent teknisk først være etableret, hvis det automatiske undersøgelsessystem efterfølgende via en supplerende og detaljeret analyse af indholdet af det materiale, der er hentet fra peer-to-peer systemet, konstaterer et indholdsmæssigt sammenfald hos de to filer.

Hvis det fastslås, at en konkret fil er identisk med et ophavsretligt beskyttet værk som tilgængeliggøres i peer-to-peer systemet uden rettighedshavers samtykke, vil der foreligge en krænkelse af ophavsretten.

Det automatiske undersøgelsessystem vil på dette tidspunkt have dokumenteret, at en konkret IP-adresse er blevet brugt til uretmæssigt at tilgængeliggøre ophavsretligt beskyttet materiale via et bestemt peer-to-peer system på internettet.

Der vil dog fortsat være nogle uafklarede spørgsmål. For det første er det uafklaret hvilken PC, der i det konkrete tilfælde har anvendt den pågældende IP-adresse. Det er også uafklaret, hvem der har ansvaret for, at PC'en blev brugt i forbindelse med den krænkende handling. Denne personidentitet kan ikke fastlægges ud fra den specifikke viden om IP-adressen. IP-adressen er alene knyttet til internetopkoblingen og ikke til en bestemt PC eller en bestemt fysisk person.

Hvis en PC er udstyret med et trådløst net (ofte kaldet WLAN eller WiFi), og dette trådløse net ikke er tilstrækkeligt beskyttet[23], kan udefra kommende personer misbruge internetforbindelsen og foretage ulovlig fildeling via peer-to-peer systemer via det trådløse netværk. Ulovlige fildelingsaktiviteter vil alene kunne spores tilbage til IP-adressen for det pågældende trådløse netværk. Dette gælder også, selvom den ulovlige aktivitet rent faktisk blev foretaget af udefrakommende personer. Forbrugerrådets undersøgelse fra februar 2009 viste, at kun 0,7 % af de adspurgte, havde skaffet sig adgang til internettet via andres trådløse netværk[24].

En nærmere teknisk undersøgelse af de relevante PC'er i den husstand, institution eller virksomhed, der hører til den pågældende IP-adresse, vil som regel kunne verificere, hvorvidt en bestemt PC har været anvendt i forbindelse med ulovlig fildeling på

[23] Der foreligger ikke statistikker over antallet af ubeskyttet trådløse netværk i Danmark. IT- og Telestyrelsen formoder, at formentlig op mod 1/3 af alle trådløse netværk i Danmark er utilstrækkeligt beskyttet. IT- og Telestyrelsen har dog ikke kendskab til, i hvilket omfang der sker misbrug af disse netværk.

[24] Se Forbrugerrådets undersøgelse spm. 13 (bilag 7)

internettet, herunder om udefrakommende personer har udnyttet et utilstrækkeligt beskyttet trådløst net til ulovlige aktiviteter på nettet.

Virus eller orm kan også føre til, at udefrakommende får adgang til at misbruge en PC. Dette forudsætter blot en almindelig internetforbindelse og ikke, at PC'en er forbundet til et trådløst netværk. En ganske væsentlig del af de vira/orme, der huserer på internettet har til formål at overtage kontrollen med tilfældige PC'er, der er koblet på internettet. Normalt er en sådan overtagelse af en PC usynlig for brugeren. Hackere benytter overtagelsen som en usynlig dør ud til internettet med henblik på at kunne foretage IT-kriminalitet, e-mail spamming og blokering af politiske modstandere på internettet etc., uden at hackerens egen identitet bliver afsløret.

En udefrakommende person kan således benytte en 'overtaget' PC[25] til ulovlig fildeling via peer-to-peer systemer. Derved vil den oprindelige fildeler være helt usynlig, idet alle IT-efterforskningsspor vil pege på den 'overtagne' PC. IT- og Telestyrelsen har under møderækken oplyst, at der endnu ikke kendes konkrete eksempler på, at vira eller orme har været anvendt i forbindelse med ulovlig fildeling.

Sandsynligheden for, at en almindelig PC bliver inficeret med virus eller orm, afhænger fuldstændigt af IT-sikkerhedsniveauet på PC'en. Hvis brugeren har et effektivt IT-sikkerhedssystem på sin PC – og dette IT-sikkerhedssystem holdes fuldt opdateret – vil en infektion med virus eller orm formentlig være højst usandsynlig. Omvendt vil det formentlig være sandsynligt, at en PC bliver inficeret, hvis PC'en ikke er udstyret med et fuldt opdateret IT-sikkerhedssystem.

Det er ikke nødvendigt, at internetbrugeren opsøger hjemmesider og trykker på de forkerte 'Ja tak' beskeder for, at vira eller orme kan komme ind i en PC. Der har indenfor det seneste år været eksempler på, at pop-up reklamer på meget regulære hjemmesider (større danske aviser, meteorologisk institut m.m.) har været inficeret med virus, der havde til formål at overtage kontrollen med tilfældige PC'er. Brugeren skulle således ikke klikke på noget på en hjemmeside for at få de pågældende vira over i sin PC - brugeren skulle blot besøge hjemmesiden.

Dette forhold betyder, at selv om en PC ikke er udstyret med trådløst net, er det alligevel muligt, at den tilknyttede IP-adresse kan være blevet brugt til ulovlig fildeling på internettet af personer udenfor husstanden.

Et automatisk undersøgelsessystems dokumentation for, at en bestemt IP-adresse har været benyttet til ulovlig fildeling på internettet, kan således ikke i sig selv dokumentere, at den ulovlige fildeling er foretaget af bestemte personer fx i en husstand.

Retsplejelovens kapitel 57a giver mulighed for, at der kan gennemføres detaljerede IT-tekniske undersøgelser med henblik på bevissikring i forbindelse med krænkelse af ophavsretten på internettet. Retsplejelovens regler er beskrevet nedenfor i kap. 6.

[25] Med 'overtaget' menes en PC der er inficeret med en virus eller orm, der betyder at PC'en kan kontrolleres af eksterne parter ude på internettet.

Brugen af avanceret undersøgelsessoftware sammen med bestemmelserne i retsplejelovens kapitel 57a kan formentlig gøre det teknisk muligt at etablere entydig og sikker dokumentation i forbindelse med krænkelser af ophavsretten ved ulovlig fildeling på internettet via peer-to-peer systemer. Det vil dog fortsat ikke være teknisk muligt at koble IP-adressen til en bestemt krænker i en husstand, men blot at koble IP-adressen til husstanden som helhed. Problemstillingen er beskrevet med eksempler fra retspraksis nedenfor i kap. 7.

5.2 Tekniske muligheder for efterforskning ved centrale servere

Ud over peer-to-peer fildeling forekommer der også uretmæssig tilgængeliggørelse af ophavsretligt beskyttet materiale via centrale servere på internettet. I modsætning til fildeling via peer-to-peer systemer vil alt det materiale, der bliver delt via en central server, være placeret på én enkelt server. En eventuel krænkelse af ophavsretten kan derfor modvirkes ved at blokere for brugernes adgang til den centrale server.

Ved tilgængeliggørelse via en central server vil afsenderen (dvs. kilden) af materiale, der krænker ophavsretten, rent teknisk være ligeså usynlig som modtageren, idet selve afsendelsen af materialet til serveren foregår ved en relativt kortvarig og skjult uploadaktivitet gennem internettet. Det vil derfor ofte ikke være praktisk muligt at identificere selve afsenderen (kilden) af materialet.

6. Gældende regler

En række regler regulerer rammerne for rettighedshavernes efterforskning og bevissikringsmuligheder. Disse regler findes blandt andet i persondataloven[26], e-handelsloven[27] og retsplejeloven[28] samt de relevante EU-direktiver.

I forbindelse med overvågning af internettet har rettighedshaverne mulighed for at finde frem til de IP-adresser, der står bag fx ulovlig fildeling. Ofte vil rettighedshaverne ikke selv have mulighed for at finde frem til oplysninger om indehaveren af en bestemt IP-adresse uden teleudbydernes hjælp, da det er teleudbyderen, der ligger inde med oplysninger om de forskellige abonnenter. Der er således tale om to forskellige problemstillinger, for det første rettighedshavernes indsamling af oplysninger og for det andet teleudbydernes videregivelse af oplysninger. Begge problemstillinger er beskrevet nedenfor i afsnittet om persondataloven.

E-handelsloven regulerer spørgsmålet om udbydernes ansvar, når deres abonnenter distribuerer ulovligt materiale via udbydernes netværk. Udgangspunktet er, at teleudbyderne ikke ifalder ansvar for ren videreformidling og caching. Udbyderne kan dog i visse tilfælde ifalde ansvar for medvirken ved transmission af ulovligt indhold. Disse regler er beskrevet nærmere nedenfor under afsnittet om E-handelsdirektivet.

---

[26] Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer.
[27] Lov nr. 227 af 22. april 2002 om tjenester i informationssamfundet, herunder visse aspekter af elektronisk handel.
[28] Lovbekendtgørelse af 594 af 20. juni 2008 om rettens pleje.

I ophavsretslovens kap. 2 beskrives en række indskrænkninger i ophavsmandens eneret. § 11 a indeholder en indskrænkning i ophavsmandens eneret til at fremstille eksemplarer af et værk. Bestemmelsen vedrører midlertidig eksemplarfremstilling og giver teleudbyderne adgang til at fremstille flygtige eller tilfældige kopier af værker, hvis eksemplarfremstillingen udgør en integreret og væsentlig del af en teknisk proces, der udelukkende har til formål at muliggøre transmission af værker i et netværk mellem tredjemænd. Eksemplarfremstillingen må ikke have en selvstændig økonomisk-værdi.

Ophavsretsloven opstiller i § 11, stk. 3, et krav om lovligt forlæg. Hvis rettighedshaverne har givet tilladelse til anvendelsen af et værk, eller hvis anvendelsen af værket er omfattet af en af undtagelsesbestemmelserne i loven, vil forlægget være lovligt. Bestemmelsen finder anvendelse på § 11 a. Det betyder, at en teleudbyder, der spreder materiale, der krænker ophavsretten, foretager en retsstridig handling, og at rettighedshaverne herefter kan anvende retsplejelovens regler til at få nedlagt forbud og derigennem bl.a. få teleselskaberne til at forhindre adgangen til hjemmesider[29].

Rettighedshaverne har mulighed for at anvende retsplejelovens regler om edition til at få en retskendelse, som pålægger teleudbyderen at udlevere oplysninger om abonnenter bag IP-adresser, som rettighedshaverne forbinder med ulovlig fildeling. Rettighedshaverne har således mulighed for at anvende domstolssystemet for at få udleveret abonnentsoplysninger fra teleudbyderne til brug for en senere retssag. Reglerne er beskrevet nedenfor i afsnittet om retsplejeloven.

6.1 Persondataloven

Persondataloven regulerer behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling.[30] Loven regulerer behandling af alle personoplysninger, uanset om oplysningerne er fortrolige eller offentligt tilgængelige fx på en hjemmeside. I forbindelse med fildeling er persondataloven relevant, når teleudbyderne eller rettighedshaverne indsamler oplysninger om andres færden på nettet.

Persondatalovens definition af personoplysninger er meget bred. Alle oplysninger kan således være personoplysninger, såfremt de kan knyttes til en fysisk person.

Loven omhandler både behandling af følsomme og ikke-følsomme oplysninger. Der stilles generelt strengere krav til behandlingen af følsomme oplysninger end til behandlingen af ikke-følsomme oplysninger. Persondatalovens §§ 7 og 8, omhandler følsomme personoplysninger. Følsomme oplysninger kan fx være oplysninger om etnisk baggrund, politisk eller religiøs overbevisning. Oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold bliver også betragtet som følsomme. Oplysningskategorier, som ikke er nævnt i persondatalovens §§ 7 og 8, er omfattet af lovens § 6 og bliver betragtet som ikke-følsomme oplysninger.

[29] Se afsnit 11; Tele2/AllofMp3
[30] Jf. persondataloven § 1, stk. 1

Rettighedshavernes behandling af ikke-følsomme personoplysninger, fx. oplysninger om navn, adresse og IP-adresse, skal ske i overensstemmelse med persondatalovens § 6. Det betyder, at den registrerede som udgangspunkt skal give udtrykkeligt samtykke til, at behandlingen kan finde sted.[31] Herudover kan behandling af ikke-følsomme oplysninger finde sted, hvis behandlingen er nødvendig for, at den dataansvarlige eller tredjemand kan forfølge en berettiget interesse, og hensynet til den registrerede ikke overstiger denne interesse[32].

Private må behandle følsomme oplysninger om strafbare forhold[33], hvis den registrerede har givet sit udtrykkelige samtykke hertil. Herudover kan behandling ske, hvis det er nødvendigt til varetagelse af en berettiget interesse, og denne interesse klart overstiger hensynet til den registrerede. Bestemmelsen opstiller meget snævre rammer for, hvornår der kan ske behandling af følsomme personoplysninger uden samtykke. Bestemmelsen giver mulighed for, at en privat virksomhed kan behandle oplysninger om strafbare forhold med henblik på indgivelse af politianmeldelse.

Behandling af personoplysninger skal ske i overensstemmelse med lovens grundlæggende principper[34]. Det betyder,[35] at indsamling af oplysninger skal ske til udtrykkeligt angivne (saglige) formål, og at behandlingen skal være rimelig og lovlig. Registrerede personer skal have mulighed for at få kendskab til en behandlings eksistens og få nøjagtige og fyldestgørende oplysninger med hensyn til de nærmere omstændigheder ved indsamlingen af information.[36]

Enhver behandling af personoplysninger skal ske i overensstemmelse med god databehandlingsskik. Heri ligger ifølge lovens forarbejder, at behandlingen skal være rimelig og lovlig. Behandling af personoplysninger må derfor som udgangspunkt kun finde sted, hvis behandlingen er nødvendig for at forfølge en legitim interesse. Håndhævelse af ophavsrettigheder vil typisk blive betragtet som et sagligt formål i henhold til loven.

De indsamlede oplysninger skal slettes snarest muligt, det vil sige senest, når sagen er afsluttet hos politiet eller domstolene. Hvis retsforfølgning opgives eller ikke indledes inden rimelig tid, skal oplysningerne slettes umiddelbart. Der vil i hvert enkelt tilfælde være tale om en konkret vurdering af, hvornår en oplysning skal slettes.

Anvendelse af internettet giver udbyderne mulighed for at indsamle oplysninger, uden at de personer, som oplysningerne handler om, bliver bekendt hermed. I forbindelse med indsamlingen af oplysninger har rettighedshaverne og teleudbyderne en oplysningspligt overfor den registrerede.

---

[31] Jf. § 6, stk 1, nr. 1
[32] Jf. § 6, stk. 1, nr. 7
[33] Jf. persondatalovens § 8, stk. 4.
[34] Jf. persondataloven § 5
[35] Ifølge lovens forarbejder
[36] Dette følger af reglerne om oplysningspligt i persondatalovens §§ 28 og 29

Behandling af følsomme oplysninger kræver som udgangspunkt, at behandlingen anmeldes til Datatilsynet inden databehandlingen påbegyndes. For private databehandlere fremgår anmeldelsespligten af persondatalovens §§ 48 og 49.

6.1.1 Rettighedshavernes indsamling af oplysninger

I forbindelse med indsamling af oplysninger på internettet foretager rettighedshaverne både behandling af følsomme og ikke-følsomme personoplysninger. Inden indsamlingen af oplysninger indledes, skal rettighedshaverne anmelde indsamlingen til Datatilsynet med henblik på at få generel tilladelse til at indsamle og behandle oplysningerne[37].

Datatilsynet kom i 2003[38] med en udtalelse om Antipiratgruppens håndtering af personoplysninger. Tilsynet udtalte i denne forbindelse, at sammenhængen mellem en IP-adresse og abonnentens navn og adresse er oplysninger af beskyttelsesværdig karakter, der skal betragtes som personoplysninger, og som derfor skal behandles i henhold til persondatalovens regler.

Antipiratgruppens behandling af oplysninger om bl.a. strafbare forhold blev af Datatilsynet anset for nødvendig, fordi ophavsretskrænkelserne som hovedregel er undergivet privat påtale. Hvis rettighedshaverne ikke har mulighed for at behandle personoplysninger, vil det i praksis være umuligt at håndhæve ophavsretten. Efter Datatilsynets opfattelse var behandlingen af oplysningerne således nødvendig for, at Antipiratgruppens retskrav kunne fastlægges, gøres gældende og forsvares.

Datatilsynet udtalte, at Antipiratgruppen med hjemmel i persondataloven kan behandle oplysninger om strafbare forhold med henblik på at vurdere, hvorvidt der bør indgives politianmeldelse eller iværksættes privat påtale for overtrædelse af ophavsretslovgivningen.

I det omfang rettighedshaverne behandler oplysninger, som de er kommet i besiddelse af gennem offentligt tilgængelige kilder, eller som er modtaget ved en lovlig videregivelse, f.eks. i medfør af retskendelse, vil behandlingen ifølge Datatilsynet ikke være i strid med god databehandlingsskik.

6.1.2 Teleudbydernes videregivelse af oplysninger

I modsætning til rettighedshaverne har teleudbyderne teknisk mulighed for at registrere meget detaljerede oplysninger om brugernes færden på internettet. Ved at registrere trafikdata har teleudbyderne mulighed for at følge kommunikationen i de elektroniske netværk og se, hvem deres abonnenter kommunikerer med, hvornår kommunikationen har fundet sted m.v.

Videregivelse af oplysninger fra teleudbyderen til rettighedshaverne er omfattet af reglerne i persondataloven.

---

[37] Jf. persondatalovens kap. 12

[38] Datatilsynets udtalelse af 20. november 2003 i sag 2002-219-0135

Persondataloven[39] tillader udlevering af ikke-følsomme oplysninger, som fx oplysninger om abonnenten bag en IP-adresse, hvis behandlingen er nødvendig for, at tredjemand kan forfølge en berettiget interesse, og hensynet til den person, som oplysningerne omhandler, ikke overstiger denne interesse.

I den ovennævnte udtalelse om Antipiratgruppen, udtalte Datatilsynet, at rettighedshaverne har en berettiget interesse i at få oplysninger fra internetudbyderne. Udlevering af oplysningerne kan dog få betydelige konsekvenser for den person, som oplysningerne omhandler, fordi personen risikerer at ifalde strafansvar. Herudover bør der efter Datatilsynets opfattelse tages hensyn til, at teleudbydernes kunder kan have en berettiget forventning om, at oplysninger om deres kundeforhold ikke tilgængeliggøres uden en retskendelse.

Det klare udgangspunkt er derfor, at udlevering af oplysninger om abonnenten bag en IP-adresse kræver en retskendelse. Datatilsynet lagde i udtalelsen om Antipiratgruppen vægt på, at udlevering af IP-oplysninger i praksis skete på baggrund af en retskendelse.

Promusicae-sagen[40]
Sagen vedrørte forelæggelse af et præjudicielt spørgsmål ved EF-Domstolen i anledning af en tvist mellem den spanske rettighedshaverorganisation Promusicae og Telefónica, en spansk tele- og internetudbyder.

Promusicae anlagde i 2005 sag mod Telefónica med henblik på foreløbige foranstaltninger. I den forbindelse begærede Promusicae udlevering af navne og adresser på abonnenter, hvis IP-adresser ifølge Promusicae var blevet anvendt til ulovlig fildeling på fildelingstjenesten KaZaa. Promusicae ønskede at anvende oplysningerne til retsforfølgning gennem civile søgsmål. Telefónica nægtede at følge rettens kendelse om udlevering af oplysningerne under henvisning til, at pligten til at udlevere sådanne oplysninger ikke gjaldt under en civil retssag eller som foreløbig foranstaltning i forbindelse med en sådan retssag.

Den spanske domstol forelagde herefter spørgsmålet om, hvorvidt EU-retten tillader, at medlemsstaterne i national ret begrænser internetudbyderens pligt til at opbevare og udlevere data om elektronisk kommunikation, således at pligten kun gælder i straffesager eller sager om beskyttelse af den offentlige sikkerhed og det nationale forsvar, men ikke i civile retssager, for EF-domstolen.

Sagen omhandlede bl.a. afvejningen af hensynet til privatlivets fred overfor hensynet til en effektiv håndhævelse af ophavsretten. Denne problemstilling er reguleret i en række forskellige EU-direktiver bl.a. Databeskyttelsesdirektivet, E-handelsdirektivet og Infosoc-direktivet. Det er første gang, at Domstolen har foretaget en undersøgelse af forholdet mellem håndhævelsen af ophavsretten og persondataretten.

---

[39] Jf. persondatalovens § 6.
[40] Dom af 29. januar 2008 i sag C-275/06, dommen er endvidere omtalt af Søren Sandfeld Jakobsen i Juristen nr. 10, 2008

Domstolen fastslog, at IP-adresser skal betragtes som persondata. Herudover fastslog domstolen, at man ikke af EU-retten kan udlede en pligt for internetudbyderne til at udlevere oplysninger til rettighedshaverne. De enkelte medlemsstater er dog ikke afskåret fra at indføre en sådan pligt, forudsat at en sådan regel afspejler en afvejning mellem hensynet til kommunikationshemmeligheden og hensynet til en effektiv håndhævelse af ophavsretten og andre lovfæstede formuerettigheder og i øvrigt iagttager almindelige fællesskabsretlige principper, særligt proportionalitetsprincippet.

6.2 E-handelsdirektivet[41]

Det er indholdsudbyderen, der har ansvaret for, at det indhold, der lægges ud på internettet, er lovligt. Det betyder, at den som uploader indhold skal sørge for at indhente de nødvendige tilladelser ved upload af ophavsretligt beskyttet materiale. Teleudbyderne kan videreformidle abonnenternes kommunikation på nettet, men har som udgangspunkt ikke indflydelse på indholdet af den information, der formidles.

E-handelsdirektivet fritager derfor i visse tilfælde teleudbyderne for ansvar for den information, de transmitterer gennem deres netværk. Ansvarsfritagelserne omfatter kun tilfælde, hvor tjenesteudbyderens aktivitet er udelukkende teknisk, automatisk og passiv. Det betyder, at tjenesteudbyderen for at være ansvarsfri ikke må have hverken kendskab til eller kontrol over de informationer, der transmitteres eller oplagres. Det betyder også, at tjenesteyderen ikke må ændre de informationer, der bliver videreformidlet[42].

Ansvarsfritagelserne for teleudbyderne findes i e-handelslovens §§ 14 – 16[43], som vedrører tjenesteudbydere, der foretager videreformidling, caching og oplagring[44]. Fælles for disse tre ydelser er, at de vedrører behandling af information, som ikke stammer fra tjenesteudbyderen. For at teleudbyderne kan undgå at ifalde ansvar, skal de ovenfor anførte betingelser være opfyldt. Er betingelserne ikke opfyldt, kan udbyderen gøres ansvarlig for medvirken til en ulovlig handling efter de almindelige erstatningsretlige eller strafferetlige regler.

Det følger af e-handelsdirektivet, at medlemsstaterne ikke må pålægge teleudbyderne en generel forpligtelse til at overvåge den information, der transmitteres eller oplagres i udbydernes netværk. Teleudbyderne må heller ikke pålægges en generel forpligtelse til aktivt at undersøge forhold eller omstændigheder, der tyder på ulovlig virksomhed. Medlemsstaterne kan derimod godt kræve, at teleudbyderne straks underretter de kompetente offentlige myndigheder om påståede ulovlige aktiviteter eller information, der udøves eller leveres af tjenestemodtageren[45]. Herudover kan medlemsstaterne

[41] Direktiv 2000/31/EF, implementeret i dansk ret ved E-handelsloven jf. lov nr. 227/2002.
[42] Det ændrer dog ikke på udbyderens ansvarsfrihed at foretage tekniske manipulationer, der finder sted i løbet af transmissionen, og som ikke ændrer i det materielle indhold af den transmitterede information.
[43] E-handelsdirektivets art. 12-14.
[44] De forskellige tjenester er indgående beskrevet i Straffelovrådets betænkning om kriminalisering af generelle opfordringer til selvmord. Betænkning nr. 1462 fra 2005 s. 14 ff.
[45] E-handelsdirektivet art. 15, stk. 2

kræve, at teleudbyderne på anmodning giver de kompetente myndigheder oplysninger, som gør det muligt at identificere de abonnenter, som teleudbyderen har oplagringsaftaler med[46]. Bestemmelsen i direktivets artikel 15 vedrører kun udlevering af oplysninger til de kompetente myndigheder. Teleudbyderne har således ikke en generel pligt til at underrette rettighedshaverne om ulovlige aktiviteter, herunder udlevere oplysninger om de abonnenter, der står bag disse aktiviteter.

Det fremgår af bemærkningerne til direktivet[47], at hensigten var at skabe grundlag for udarbejdelse af hurtige og pålidelige ordninger, som skulle gøre det muligt at fjerne ulovlig information og hindre adgangen til denne information.

Ifølge bemærkningerne bør sådanne ordninger fremmes af medlemsstaterne og udarbejdes ved frivillige aftaler mellem alle de berørte parter. Der henvises til, at alle de parter, som deltager i levering af informationssamfundstjenester, har interesse i at vedtage og anvende sådanne ordninger.

Det fremgår også af bemærkningerne til direktivet[48], at bestemmelserne om ansvarsfritagelse ikke bør være til hinder for, at de forskellige berørte parter udvikler og faktisk gennemfører tekniske beskyttelses- og identifikationssystemer samt tekniske overvågningsinstrumenter, som er muliggjort af den digitale teknik med respekt for de europæiske regler om beskyttelse af personoplysninger[49].

6.3 Retsplejeloven

Som anført ovenfor er udgangspunktet, at teleudbyderne kun må udlevere oplysninger om abonnenten bag en IP-adresse, når de er pålagt det i en retskendelse. Efter retsplejelovens regler om optagelse af bevis mv. i civile sager kan rettighedshaverne få en retskendelse, som pålægger teleudbyderne at udlevere oplysninger, som fx navn og adresse på abonnenter bag IP-adresser, der kan sættes i forbindelse med ophavsretskrænkelser.

Det er anerkendt i retspraksis[50], at retsplejelovens regler om isoleret bevisoptagelse[51] sammenholdt med reglerne om edition[52] kan anvendes til at pålægge f.eks. teleudbydere at udlevere oplysninger, der er nødvendige for, at en rettighedshaver kan finde ud af, hvem man skal anlægge sag mod.

Efter reglerne i retsplejelovens kapitel 57 a om bevissikring ved krænkelse af immaterialrettigheder mv. kan fogedretten på rettighedshavernes anmodning træffe afgørelse om, at der skal foretages en undersøgelse med henblik på at sikre bevis for bl.a. kræn-

---

[46] Disse regler er fuldt implementeret i den danske e-handelslovs §§ 14-16.
[47] Direktivets præambel punkt 40
[48] Direktivets præambel pkt. 40
[49] Der henvises i præamblen til, at systemerne skal være indenfor grænserne fastsat i direktiv 95/46/EF om beskyttelse af personoplysninger i EU samt direktiv 97/66/EF om behandling af personoplysninger og beskyttelse af privatlivets fred inden for telesektoren.
[50] Se U2003.2263.Ø og U2005.1410.V.
[51] Retsplejelovens § 343,stk. 1, 1.pkt.
[52] Retsplejelovens § 299, stk. 1.jf. §§ 169-172. samt § 299 stk. 2.

kelse af ophavsretsloven. Bestemmelserne giver mulighed for uanmeldt og tvangsmæssig undersøgelse af en formodet krænkers lokaler og genstande, herunder også af computere, med henblik på at sikre bevis for krænkelserne samt omfanget af disse. Undersøgelsen kan ske, hvis rettighedshaverne overfor fogedretten kan sandsynliggøre, at der foregår krænkelser af immaterialrettigheder, såsom ulovlig tilgængeliggørelse eller eksemplarfremstilling af ophavsretligt beskyttet materiale fx fra den formodede krænkers computer.

Rettighedshaverne skal senest 4 uger efter undersøgelsens afslutning anlægge retssag vedrørende de krænkelser, som dannede grundlag for, at undersøgelsen kunne foretages. Anlægger rettighedshaverne ikke denne sag, skal de undersøgte genstande leveres tilbage og kan ikke bruges som bevis i en senere retssag.

I tilfælde, hvor teleudbyderne ved transmissionen af værker fremstiller eksemplarer uden lovligt forlæg, falder teleudbydernes eksemplarfremstilling udenfor ophavsretslovens regel om midlertidig eksemplarfremstilling[53]. Det betyder, at den eksemplarfremstilling som teleudbyderne foretager, udgør en krænkelse af rettighedshavernes eneret[54] til eksemplarfremstilling af det beskyttede materiale. Teleudbyderne vil derfor i disse tilfælde, som udgangspunkt kunne mødes med ophavsretlige sanktioner, herunder forbud efter reglerne i retsplejeloven[55]. Ansvarsfritagelserne i e-handelsloven sikrer dog, at der normalt ikke vil kunne rejses et civil- eller strafferetligt ansvar mod teleudbyderne i disse tilfælde[56].

7 Retspraksis fra Danmark

Der har været flere afgørelser om krænkelse af ophavsretten, som illustrerer vanskelighederne med at bevise, hvem der har begået en krænkelse af ophavsretten.

I en række af disse sager har beviserne bestået af en "teknisk bevis-pakke" bestående af en række data om sammenfald mellem den delte fil og den ophavsretligt beskyttede fil samt dokumentation til identifikation af IP-adresser samt for tidspunktet, hvor tilgængeliggørelse af det ophavsretligt beskyttede materiale skete. Derudover er disse tekniske beviser ofte suppleret af vidneforklaringer og i visse tilfælde af tilståelser fra sagsøgtes side. De ovenfor omtalte regler i retsplejelovens kap. 57 a har ikke været anvendt i nedenstående sager.

Vanskelighederne for rettighedshaverne ved at bevise, hvem der har begået krænkelser, illustreres bl.a. af 4 landsretsafgørelser fra efteråret 2008:

Østre Landsret, dom af 5/9 – 2008

[53] Ophavsretsloven § 11a.
[54] Jf. ophavsretsloven § 2.
[55] Se fx U2007.1474H
[56] Adjunkt phd Clement Salung Petersen har i sin artikel "Netværksoperatørernes rolle i bekæmpelsen af ophavsretskrænkelser på internettet" bl.a. beskrevet denne problemstilling.

Sagen vedrørte en ankesag fra Glostrup byret, hvor A blev frikendt for at have foretaget ulovlig fildeling.

Under ankesagen oplyste A, at hun havde trådløs router. Forbindelsen var ikke sikret med et password. A kunne ikke udelukke, at computeren nogen gange var tændt, når familien ikke var hjemme, men hun var sikker på, at det ikke var tilfældet på det tidspunkt, hvor krænkelsen skulle være sket.

Under ankesagen blev der afgivet vidneforklaring af en systemudvikler fra et internetfirma, som foretager bevissikring for rettighedshaver. Dette vidne forklarede, at hvis en trådløs router ikke var sikret, ville en person, der befandt sig i en vis nærhed af routeren, kunne misbruge den pågældende IP-adresse.

Rettighedshaverne gjorde under sagen gældende, at bevisbyrden burde vendes, så det måtte påhvile A at sandsynliggøre, at krænkelserne ikke var sket fra hendes husstands computere. I forhold til internetudbyderen havde A pligt, jf. abonnementsvilkår, til at sikre sin internetforbindelse mod misbrug, herunder ophavsretskrænkelser. Derfor burde det ifølge rettighedshaverne være A's ansvar at sikre sig mod disse misbrug. Såfremt retten lagde til grund, at andre kunne have foretaget krænkelserne, måtte A, ifølge rettighedshaverne, bære et ansvar for krænkelserne i medfør af hendes status som indehaver af internetforbindelsen, og fordi hun ikke havde sikret forbindelsen.

A gjorde gældende, at internetudbyderens abonnementsvilkår ikke kunne pålægge A et ansvar i forhold til andre end internetudbyderen. A bestred, at nogen fra hendes husstand havde foretaget krænkelserne og henviste til, at det var muligt at hacke en usikret forbindelse.

Landsretten udtalte, at bevisbyrden påhvilede rettighedshaverne. Ifølge landsretten skulle A derfor ikke bevise, at hun ikke havde foretaget krænkelserne. Landsretten fandt, at rettighedshaverne ikke havde bevist, at A selv havde foretaget krænkelserne, eller at A havde handlet culpøst i forbindelse med, at andre måtte have foretaget krænkelserne.

Østre Landsret, dom af 5/9 – 2008

Sagen vedrørte en ankesag fra Helsingør byret, hvor A var blevet frikendt for at have foretaget ulovlig fildeling. Indholdsmæssigt lignede sagen den ovenfor beskrevne sag.

A forklarede under sagen, at de tre computere var koblet til internettet via hendes telefonforbindelse. Hun vidste ikke hvem, der havde downloaded på det konkrete tidspunkt.

En teknisk ekspert afgav vidneforklaring, hvorunder han oplyste, at han ikke havde kendskab til, at det automatiske undersøgelsesprogram, som rettighedshaver anvendte til bevissikring, nogen sinde skulle have identificeret en forkert IP-adresse, men teoretisk var det muligt, at internetudbyderen kunne have givet en forkert oplysning.

Rettighedshaverne gjorde også under denne sag gældende, at bevisbyrden burde vendes, så det måtte påhvile A at sandsynliggøre, at krænkelserne ikke var sket fra hendes husstands computere. I forhold til internetudbyderen havde A pligt, jf. sine abonnementsvilkår, til at sikre sin internetforbindelse mod misbrug, herunder ophavsretskrænkelser. Derfor burde det ifølge rettighedshaverne være A's ansvar at sikre mod dette misbrug. Såfremt retten lagde til grund, at andre kunne have foretaget krænkelserne, måtte A, ifølge rettighedshaverne, bære et ansvar for krænkelserne i medfør af hendes status som indehaver af internetforbindelsen, og fordi hun ikke havde sikret forbindelsen.

A gjorde gældende, at internetudbyderens abonnementsvilkår ikke kunne pålægge A et ansvar i forhold til andre end internetudbyderen. A bestred, at nogen fra hendes husstand havde foretaget krænkelserne og henviste til, at det var muligt at hacke en usikret forbindelse.

Landsretten frikendte A og stadfæstede dermed byrettens afgørelse. Landsretten lagde den samme vurdering til grund i denne sag, som i den ovenfornævnte sag fra samme dato.

Vestre Landsret, dom af 6/10 – 2008

Sagen vedrørte en ankesag fra Randers byret. A var af byretten blevet dømt for at have foretaget ulovlig fildeling via et peer-to-peer system. Under ankesagen var parterne enige om en række konkrete forhold, bl.a. at:

- routeren / computeren kunne ikke identificeres fra IP-adressen,
- der kunne være tilsluttet mere end én computer til en router, som havde flere udgange eller var trådløs, og
- det var ikke nødvendigt at være på samme adresse, som en trådløs router for at tilslutte sig denne.

A forklarede, at han boede i et boligområde med flere lejlighedskomplekser, og at der i A's kompleks var 32 lejligheder. A var på arbejde det konkrete tidspunkt, hvor krænkelsen skulle være sket. A havde en trådløs internetforbindelse, men opsagde den i den måned, hvor krænkelsen skulle være sket.

Under sagen afgav en syns- og skønsmand forklaring. Han oplyste, at man ikke kan se, hvad der er tilsluttet en router. Hvis en trådløs forbindelse er ubeskyttet, kan enhver tilslutte sig. Hvis forbindelsen er beskyttet, kræver tilslutning en dygtig hacker. Syns- og skønsmanden oplyste, at det var muligt at sidde et andet sted end på adressen og søge efter trådløse forbindelser i nærområdet. Hvis en uvedkommende brugte en trådløs forbindelse, ville det blive registreret som om, det var ejeren af den pågældende IP-adresse, der var på nettet.

Rettighedshaverne gjorde gældende, at A, som indehaver af internetforbindelsen, var ansvarlig for de skete krænkelser, uanset om disse var foretaget af andre.

Landsretten fandt det bevist, at der gennem A's internetforbindelse var blevet stillet 1897 musikfiler ulovligt til rådighed for andre. Under hensyn til, at A havde en usikret trådløs forbindelse, og at han boede i et lejlighedskompleks, kunne det ifølge landsretten ikke udelukkes, at andre havde misbrugt A's IP-adresse. Landsretten bemærkede, at det ikke kunne anses for ansvarspådragende, at A ikke havde sikret sin internetforbindelse. Landsretten frifandt herefter A.

Vestre Landsret, dom af 20/10 – 2008

Sagen vedrørte en ankesag fra Aalborg byret. A var af byretten blevet dømt for at have foretaget ulovlig fildeling via peer-to-peer systemet DirectConnect. Under ankesagen forklarede A, at han ofte arbejdede om aftenen og havde en computer, som var koblet til internettet via en fastnetforbindelse og et modem. A havde ikke firewall på sin computer, men et antivirusprogram. Han brugte ikke kodeord, og computeren var derfor ubeskyttet. A havde en router, men den var ikke trådløs. A havde oplyst, at han havde brugt DirectConnect uden at gøre sig klar, hvad dette indebar.

Under sagen afgav en syn- og skønsmand forklaring. Han oplyste, at ved en ubeskyttet fastnetforbindelse med et modem og en router, som ikke var trådløs, var det kun personer, som havde adgang fra hjemmet, der kan komme ind på computeren. Hvis computeren var tændt og inde på DirectConnect, kunne andre udefra godt gå ind og foretage fildeling, men skønsmanden kendte ikke det konkrete program godt nok til at kunne svare på, om disse udefrakommende ville kunne bruge A's alias.

Landsretten fandt det bevist, at den konkrete IP-adresse på det pågældende tidspunkt tilhørte A og alene blev anvendt af A. Landsretten fandt det også bevist, at de konkrete filer blev ulovlig delt fra A's computer, og at A derfor krænkede ophavsretslovens § 2. A blev derfor dømt til at betale erstatning og vederlag på i alt 160.000 kr. samt slette de ulovlige filer fra sin computer.

Sagen er med procesbevillingsnævnets tilladelse anket til Højesteret d. 23. januar 2009.

7.1 Opsummering på afsagte domme

De fire nævnte domme viser, at bevissikring i forhold til hvilken person, der har foretaget den ulovlige fildeling er kompliceret og vedrører en række aspekter, herunder evt. ansvar for andres brug af internetforbindelsen.

De to domme fra september viser, at domstolene i disse konkrete sager har vurderet, at en indehaver af en internetforbindelse ikke er ansvarlig for andres brug af internetforbindelsen. Samtidig viser de første tre domme, at domstolene har været tilbageholdende med at idømme et ansvar for ophavsretlige krænkelser via en internetforbindelse, når internetforbindelsen er trådløs og usikret, og der er tvivl om, hvem der i husstanden eller udenfor kunne have foretaget krænkelserne.

Ud fra de fire nævnte domme, kan det konstateres, at domstolene ikke dømmer indehavere af internetforbindelser alene på baggrund af teknisk identifikation af IP-adresser og teknisk sammenfald mellem filer. Der skal foreligge yderligere tekniske beviser, som

knytter de krænkende handlinger til bestemte personer, hvis dette ikke kan bevises ved vidneforklaring eller på anden måde. I den sidstnævnte sag forelå der netop en sådan erkendelse fra A's side af at have brugt peer-to-peer systemet samtidig med, at de tekniske forhold gjorde det mindre sandsynligt, at udefrakommende havde misbrugt internetforbindelsen.

8 Opsamling på efterforskning af ulovlig tilgængeliggørelse på internettet

Som det fremgår af de foregående afsnit, indebærer rettighedshavernes efterforskning af ulovlig fildeling i dag brug af automatiske undersøgelsessystemer, som indsamler offentligt tilgængeligt data. Denne indsamling og behandling af oplysninger blev i 2003 vurderet af Datatilsynet som værende i overensstemmelse med god databehandlingsskik, såfremt indsamlingen er sket gennem offentligt tilgængelige kilder eller ved lovlig videregivelse, og behandlingen af oplysningerne er nødvendig for at håndhæve rettighedshavernes ophavsrettigheder.

Når rettighedshaverne i dag gennem brugen af de automatiske undersøgelsessystemer har indsamlet oplysninger om, hvilken IP-adresse, der på et givent tidspunkt har tilgængeliggjort konkret ophavsretligt beskyttet materiale, kan rettighedshaverne rejse sag ved domstolene med krav om, at internetudbyderen pålægges at udlevere navn og adresse på den abonnent, som på det pågældende tidspunkt anvendte den identificerede IP-adresse[57].

Når rettighedshaver har abonnentoplysningerne, kan der efterfølgende anlægges en civil retssag mod den abonnent, som rettighedshaver mener at kunne dokumentere har foretaget de formodede ophavsretlige krænkelser.

Det nuværende system indebærer, at domstolene involveres både ved udleveringen af abonnentoplysninger samt i den senere civile retssag. Dermed sikres borgernes retssikkerhed ved, at personoplysninger ikke udleveres direkte til rettighedshaver, uden at en domstol har vurderet, hvorvidt det foreliggende bevismateriale kan sandsynliggøre, at der foreligger en krænkelse. Involveringen af domstolene indebærer visse ressourcemæssige omkostninger for såvel rettighedsindehaver som internetudbyderne.

Civile retssager føres indenfor forhandlingsmaksimens rammer. I sager, hvor rettighedshaverne kræver, at internetudbyderne afbryder forbindelsen til fx en central server, kan forhandlingsmaksimen få den betydning, at domstolene kun foretager en materiel prøvelse af sagen, i det omfang teleudbyderne forsvarer sig[58]. I tilfælde, hvor teleudbyderne ikke forsvarer sig, fx fordi de ikke møder op i retten, påser domstolen af egen drift, om reglerne er overholdt. Intensiteten af denne prøvelse er begrænset, da sagsøgers ønsker i udeblivelsessager som udgangspunkt imødekommes, med mindre det strider mod ufravigelig lovgivning.

---

[57] Jf. Retsplejeloven §§ 299 og 343.

[58] Adjunkt phd Clement Salung Petersen har i sin artikel "Netværksoperatørernes rolle i bekæmpelsen af ophavsretskrænkelser på internettet" bl.a. beskrevet denne problemstilling.

Den nuværende anvendelse af automatiske undersøgelsessystemer, kombineret med brugen af retsplejelovens regler, særligt §§ 299 og 343, der kan føre til udlevering af abonnentoplysninger, samt lovens kapitel 57 a om bevissikring, betyder, at rettighedshaver kan foretage efterforskning og bevissikring, som kan føre til domfældelser.

Der ligger en stor udfordring for rettighedshaverne i at bevise, hvilken fysisk person, der har anvendt en trådløs usikret forbindelse. Denne bevismæssige udfordring beror formentlig ikke på mangler i de nuværende regler om bevissikring og efterforskning. I stedet skyldes udfordringen formentlig, at det kan være **teknisk** umuligt at foretage en fuldstændig identifikation af, hvilken fysisk person, der har anvendt en trådløs usikret internetforbindelse.

9 Reaktionsmuligheder ved ulovlig tilgængeliggørelse på internettet

Når rettighedshaverne har identificeret en eventuel krænkelse og foretaget den indledende bevissikring, vil de skulle anmode retten om tilladelse til yderligere bevissikring, og/eller påstå nedlæggelse af foreløbige forbud og idømmelse af sanktioner såsom bøde eller fængselsstraf.

I dette afsnit gennemgås de tekniske muligheder for at blokere for ulovlig tilgængeliggørelse på centrale servere samt via peer-to-peer systemer.

I afsnit 10 og 11 præsenteres de relevante regler for sanktioner og forbud samt nyere retspraksis.

9.1 Teknisk blokering af centrale servere på internettet

Teknisk blokering af centrale servere på internettet kan foretages på forskellige måder. For flertallet af de forskellige blokeringsstrategier gælder det imidlertid, at blokeringen ikke vil være fuldstændig effektiv, men forholdsvist let kan omgås af IT-kyndige brugere.

Den eneste form for blokering, der er fuldstændigt effektiv, er at få lukket serveren fysisk i dens opholdsland. Rent praktisk kan en sådan fysisk nedlukning dog vise sig at være vanskelig at få gennemført via det lokale retssystem i serverens opholdsland. Servere, der primært benyttes til ulovlig tilgængeliggørelse af ophavsretligt beskyttet materiale, er som regel bevidst placeret i lande, hvor ophavsretten til elektronisk materiale såsom film, musik og lignende ikke er genstand for effektiv håndhævelse. Hertil kommer, at materialet nemt og hurtigt kan flyttes og tilgængeliggøres fra en anden server.

Af denne årsag kan man i stedet vælge at blokere for internetbrugernes adgang til bestemte servere med et generelt indhold af ulovligt materiale. Dette kan ske ved rent teknisk at blokere for brugernes internettrafik til de pågældende servere.

Der er flere måder at foretage en teknisk blokering på. Disse måder beskrives nedenfor.

Som det fremgår af det følgende, har en teknisk blokering af internettrafik til bestemte servere den fordel, at den tekniske blokering kan foretages i internetbrugernes hjemland eksempelvis Danmark, også selvom den pågældende server er placeret i et andet land.

Ulemperne ved en teknisk blokering af internettrafik til bestemte servere er, at de mere enkle blokeringsstrategier relativt nemt kan omgås teknisk, samt at de mere effektive blokeringsstrategier vil kræve betydelige økonomiske investeringer fra internetudbydernes side. Derudover medfører en række af de nedenfor beskrevne blokeringsmuligheder en række retssikkerhedsmæssige overvejelser, jf. afsnit 13.1.

En teknisk blokering af internetbrugerne mod udvalgte servere med et generelt indhold af ulovligt materiale kan ske via:

- URL blokering.
- IP-adresse blokering[59].
- Port-blokering.
- Protokol-blokering.
- Indholdsblokering.

De fem mulige blokeringsstrategier bliver nærmere beskrevet i det efterfølgende.

9.1.1 URL blokering (DNS-spærring)

På internettet benyttes IP-adresser til at fremføre al trafik mellem de forskellige servere og PC'er, der er tilsluttet til internettet. IP-adresser er meget vanskelige at huske og vil let blive indtastet forkert af mennesker. Derfor er der blevet indført en særlig nem måde at angive en internetadresse på – en såkaldt Uniform Ressource Locator (URL).

Et eksempel på en URL er internetadressen: www.kum.dk. En sådan adresseangivelse er nem at huske, men den kan ikke umiddelbart benyttes på internettet til at skabe kontakt mellem en brugers PC og den server, der er identificeret ved denne URL. Til dette formål er det altså nødvendigt at kende IP-adressen for serveren bag ved URL'en www.kum.dk.

En URL bliver automatisk oversat til den tilhørende IP-adresse af et særligt databasesystem hos brugerens internetudbyder. Dette databasesystem kaldes Domain Name Service (DNS). Dette foregår ved, at PC'en, når brugeren indtaster adressen www.kum.dk i sin browser, spørger DNS-databasen hos internetudbyderen om, hvad IP-adressen er for denne URL. DNS databasesystemet hos udbyderen svarer derefter

---

[59] En PC, der er forbundet til internettet, bliver identificeret på nettet ved hjælp af den tildelte IP-adresse. En IP-adresse er en éntydig identifikation og er konkret en kombination af 4 tal mellem 0 og 255. Selv om IP-adresser således gemmes som binære tal, vises de sædvanligvis i menneske-læsbare tekster som eksempelvis www.hav-en-god-dag.dk. Læs eventuelt mere om IP-adresser i annex II Lidt om IP-adresser.

brugerens PC, at den ønskede IP-adresse er 123.456.789.012. Derefter starter brugerens PC sin kommunikation med serveren på den oplyste IP-adresse.

Hvis man forestiller sig, at en internetudbyder fjerner sammenknytningen mellem en bestemt URL og den tilhørende IP-adresse i sin DNS database, vil brugerne hos denne internetudbyder ikke umiddelbart være i stand til at kommunikere med den server på internettet, der netop har denne URL, idet URL'en ikke kan blive oversat til den nødvendige IP-adresse.

Denne type af teknisk blokering af brugernes kommunikation med en bestemt server på internettet kaldes en URL blokering (eller DNS-spærring).

En URL blokering er den mest simple form for teknisk blokering, hvis man ønsker at forhindre brugernes adgang til bestemte servere på internettet. Blokeringen indføres i internetudbyderens DNS-database.

Omkostningerne ved at udføre en URL blokering er relativt begrænsede, men blokeringen kan forholdsvist nemt omgås af IT-kyndige brugere.

9.1.2 IP-adresse blokering

Ved en IP-adresse blokering forhindrer man en brugers PC i at kommunikere med en server på internettet med en bestemt IP-adresse. Denne type blokering er mere effektiv end URL blokering, men også mere omkostningskrævende at indføre.

Der er dog et væsentligt problem forbundet med IP-adresse blokering. Problemet hænger sammen med den måde, som internettrafik bliver håndteret på. Når en internetudbyder skal sende trafik til en server eller en PC udenfor udbyderens eget net – altså til en fremmed IP-adresse – bliver trafikken alene sendt ud fra en viden om det autonome system[60], som IP-adressen er en del af.

Kommunikation til servere og PC'er, der er udenfor udbyderens eget net, men som har IP-adresse indenfor samme autonome system, bliver behandlet ens af udbyderens tekniske systemer og bliver sendt videre til den server, der er næste led i kommunikationskæden på internettet.

Som internettet er specificeret, vil det således ikke være muligt for en internetudbyder at gøre noget særligt ved trafikken mod en bestemt server med en bestemt IP-adresse udenfor udbyderens eget net.

Indføring af IP-adresse blokering mod servere eller PC'er udenfor udbyderens eget net forudsætter, at internetudbyderen indfører særligt udstyr, der specifikt identificerer

[60] I forbindelse med internettets eksplosive vækst måtte Internet Engineering Task Force IETF allerede i starten af 90'erne erkende, at en given server ikke længere ville være i stand til at kende en vilkårlig anden server på internettet. IP-adresserne blev derfor opdelt i 65.536 forskellige blokke kaldet 'autonome systemer'. Indenfor hvert 'autonom system' kan der fortages en videre opdeling af IP-adresser i underblokke kaldet 'subnet'.

udvalgte IP-adresser og fjerner kommunikation mod disse adresser. Dette er teknisk muligt, men medfører en meromkostning for internetudbyderen.

IT- og Telestyrelsen anslår, at omkostningerne for den danske internetbranche ved at indføre og drive et sådant system vil være op mod 200 mio. kr.[61]. Det vil endvidere være meget enkelt for den IT-kyndige bruger at modvirke den form for blokering. Effektiviteten og nyttevirkningen ved blokering af IP-adresser vil derfor, ifølge IT og Telestyrelsen, formentlig være meget lille.

9.1.3 Port blokering

Når en server eller PC sender information via internettet til en anden server eller PC, oplyser afsenderen, at informationen skal føres frem til en særlig intern "forbindelse" (mere præcist et program) i den modtagende server eller PC. Oplysningen til modtageren om den korrekte interne "forbindelse" er det såkaldte port-nummer. Port-nummeret er et tal mellem 0 og 65.535.

Ideen med port blokering er, at internetkommunikation med bestemte port-oplysninger bliver blokeret. Fremgangsmåden er ikke særligt hensigtsmæssig, idet information om port-nummer ikke giver nogen entydig identifikation af en konkret aktivitet på internettet.

Mange forskellige internet aktiviteter benytter de samme port-numre. Port-nummeroplysninger kan således ikke benyttes som et korrekt og retvisende grundlag for blokering af bestemte, uønskede aktiviteter.

Det bør desuden understreges, at port-nummer oplysninger ikke er trafikdata. Et portnummer er derimod en specifik indholdsinformation, der vedrører de to kommunikationsparter[62]. Port-nummeroplysninger befinder sig endvidere på et dybere niveau i internetkommunikationen end de ovenfor omtalte IP-oplysninger. Omkostningerne for den danske internetbranche ved at foretage port blokering vil derfor være endnu højere end de tidligere omtalte omkostninger ved at foretage IP-adresse blokering. IT- og Telestyrelsen vurderer, at omkostningerne i forbindelse med port blokering vil nærme sig en milliard.

Samlet kan det konkluderes, at port blokering formentlig ikke vil hindre de uønskede aktiviteter.

9.1.4 Protokol blokering

---

[61] Det pågældende udstyr er ikke standardudstyr, hvilket i sig selv har en væsentlig indflydelse på omkostningerne. Endvidere skal det pågældende udstyr fungere sammen med det eksisterende udstyr hos udbyderen uden at belaste trafiksituationen – altså uden at reducere brugernes oplevede kvalitet.

[62] Data, der specifikt og alene benyttes til at overføre information fra en afsender til en modtager i et kommunikationsnet, kaldes **trafikdata** – et eksempel på trafikdata er en IP-adresse. Den nytteinformation, der overføres fra en afsender til en modtager, kaldes **indholdsdata**. Rent praktisk minder det om informationerne på et almindeligt postkort: modtagerens navn og adresse er trafikdata, mens selve beskeden på postkortet er indholdsdata.

Ved protokol blokering går man et skridt dybere ind i internetkommunikationen, og blokerer for den kommunikation, der forgår med en bestemt bruger-til-bruger protokol[63].

Denne strategi har de samme ulemper som port blokering og ingen supplerende fordele.

Med protokol blokering vil det formentlig ikke være muligt at stoppe for den uretsmæssige tilgængeliggørelse af ophavsretligt beskyttet materiale[64]. Implementerings- og driftsomkostningerne i forbindelse med protokol blokering vil formentlig være endnu højere end de tilsvarende omkostninger ved port-blokering.

9.1.5 Indholdsblokering

Ved indholdsblokering går man skridtet længere end protokol blokering, idet man blokerer for kommunikation med særligt indhold. Eksempler på særligt indhold kunne være dele af musik, film eller lignende, hvor der er rettighedsmæssige forhold, der ikke tillader den pågældende kommunikation.

Denne strategi har præcis de samme ulemper som port blokering og protokol blokering, blot er omkostningerne formentlig endnu højere.

Indholdsblokering vil formentlig ikke kunne stoppe uretsmæssig tilgængeliggørelse af ophavsretligt beskyttet materiale[65]. Implementerings- og driftsomkostningerne vil formentlig udgøre adskillige milliarder for den samlede danske internetbranche.

9.2 Teknisk blokering ved peer-to-peer systemer

Fildeling via peer-to-peer systemer er den vanskeligste krænkelse af ophavsretten at imødegå ved teknisk blokering, idet sådanne systemer ikke er afhængige af en central server på internettet, der blot skal blokeres for derved at hindre krænkelsen. Det er derfor formentlig ikke muligt at foretage en generel teknisk blokering af et helt peer-to-peer system. I stedet må man tage juridiske skridt mod den enkelte deltager i netværket, såfremt man kan dokumentere omfanget af deltagerens tilgængeliggørelse af ophavsretligt beskyttet materiale.

10 Gældende regler om sanktionering af ophavsretskrænkelser efter privat påtale

På ophavsrettens sanktionsområde inddeles krænkelser i tre kategorier:

---

[63] En bruger-til-bruger protokol er en protokol, der alene benyttes til at udveksle data direkte mellem de to parter i kommunikationen. En bruger-til-bruger protokol benyttes således ikke til at styre kommunikationen på internettet. Som et eksempel på en bruger-til-bruger protokol kan nævnes http-protokollen, der benyttes ved visning af hjemmesider

[64] Det er muligt at skjule den krænkende adfærd som værende en legitim adfærd på internettet. Visse IP-telefonisystemer benytter eksempelvis port 80 (almindelig internetbrowsing) for at slippe igennem en virksomheds firewall

[65] Det meste af denne trafik er sendt i særlige komprimeringsformater (eksempelvis WinRAR eller ZIP), der som regel er krypteret med AES-algoritmen med en nøglestørrelse på 256 bit, og kan derfor ikke identificeres af en internetudbyder eller en tilsvarende virksomhed.

- **Simple krænkelser**: Omfatter forsætlige krænkelser af mindre omfang samt alle groft uagtsomme krænkelser.
- **Grove krænkelser**: Forsætlige overtrædelser under skærpende omstændigheder.
- **Særligt grove krænkelser**: Forsætlige overtrædelser under særligt skærpende omstændigheder.

Sanktionsbestemmelser for simple og grove krænkelser findes i ophavsretsloven. Særligt grove krænkelser er reguleret i straffeloven.

Der er mulighed for at rejse straffesag for simple krænkelser efter reglerne om privat påtale, jf. ophavsretslovens § 76, stk. 1, jf. § 81, stk. 1. Det vil sige, at sager om forsætlige krænkelser af mindre omfang samt alle groft uagtsomme krænkelser kan rejses som straffesager efter privat påtale. Sanktionen er bødestraf. Den nævnte straffebestemmelse kan anvendes i sager, der anlægges mod fysiske eller juridiske personer[66], som har foretaget ulovlig eksemplarfremstilling og/eller tilgængeliggørelse[67].

Udover disse sager har rettighedshavere indenfor de senere år anlagt enkelte sager mod internetudbyderne. Konkret har rettighedshaverne nedlagt påstand om at pålægge internetudbyderne en pligt til at blokere for adgangen til konkrete hjemmesider eller på anden måde blokere for en fortsat ulovlig tilgængeliggørelse. Disse sager starter som forbudssager ved fogedretten og reguleres derfor af retsplejelovens kapitel 57.

10.1 Retsplejelovens kapitel 57

Retsplejelovens kapitel 57 indeholder retsplejelovens almindelige regler om fogedforbud.

Bestemmelserne betyder, at fogedforbud kan nedlægges, hvis det kan godtgøres eller sandsynliggøres at[68]

- de handlinger, der søges forbudt, strider mod rettighedshavers ret,
- at den, som fogedforbudet retter sig imod, vil foretage handlingerne som søges forbudt,
- at formålet vil forspildes, såfremt rettighedshaver henvises til at gøre sin ret gældende gennem en almindelig rettergang.

I det omfang der nedlægges fogedforbud, skal forbudet justificeres under en senere retssag.

---

[66] Ophavsretslovens § 80.

[67] Der er i øvrigt mulighed for offentlig påtale af forsætlige grove krænkelser, jf. ophavsretslovens § 76, stk. 2, jf. § 82, og forsætlige særligt grove krænkelser, jf. straffelovens § 299b. Straffferammerne går op til henholdsvis 1 ½ års fængsel og 6 års fængsel.

[68] Jf. Retsplejelovens § 642

Retsplejelovens kapitel 57 er på ophavsrettens område særlig relevant i forhold til rettighedshavernes mulighed for at kunne nedlægge fogedforbud over for mellemmænd, hvis tjenester anvendes af tredjemand til at krænke ophavsretten. Det fremgår af det nedenfor beskrevne Infosoc-direktiv, at det i EU-medlemsstaterne skal være muligt for rettighedshaverne at få nedlagt sådanne forbud. Forbudsbestemmelserne er blandt andet brugt i to retsafgørelser fra 2006[69].

I dag deltager internetudbyderne ikke i at afklare, hvordan og i hvilket omfang, der er tale om en krænkelse. Dette afklares mellem rettighedshaveren og den påståede krænker, evt. under en retssag (om straf og/eller erstatning). I det omfang retten har pålagt internetudbyderne at afbryde internetforbindelser eller blokere adgangen til konkrete hjemmesider, har internetudbyderne efterlevet dette.

10.2 Infosoc-direktivet

Ifølge direktiv 2001/29/EF af 22. maj 2001 om harmonisering af visse aspekter af ophavsret og beslægtede rettigheder i informationssamfundet (infosoc-direktivet) [70] skal medlemsstaterne sikre, at rettighedshaverne kan kræve nedlagt forbud over for mellemmænd, hvis tjenester anvendes af tredjemand til at krænke ophavsrettigheder eller beslægtede rettigheder.

Infosoc-direktivet blev gennemført i dansk ret ved lov af 17. december 2002[71]. Det fremgår af lovens forarbejder, at direktivets krav[72] om mulighed for at kunne nedlægge fogedforbud over for mellemmænd ikke kræver særskilt lovændring, da denne mulighed er til stede ved anvendelse af de almindelige forbudsbestemmelser i retsplejelovens kapitel 57[73]. Det er Kulturministeriets vurdering, at de gældende regler i tilstrækkelig grad balancerer hensynet til en effektiv håndhævelse af ophavsrettigheder i forhold til internetbrugernes muligheder for at udnytte internettjenester til legale formål.

11 Retspraksis fra Danmark

Som det fremgår ovenfor vil teknisk blokering af centrale servere ofte nødvendiggøre, at internetudbyderne inddrages, da de reelt vil være de eneste, som kan foretage blokeringen.

---

[69] Jf. afsnit 11
[70] Infosoc-direktivet artikel 8 (3)
[71] Lov nr. 1051 af 17. december 2002 (lov om ophavsret)
[72] Jf. direktivets artikel 8 (3)
[73] Adjunkt phd Clement Salung Petersen har i sin phd-afhandling "immaterialrettigheder og foreløbige forbud" fra 2008 anført, at de almindelige regler om forbud i RPL kapitel 57 efter hans opfattelse ikke er velegnede til at håndtere de tilfælde, hvor der ifølge infosoc-direktivets art. 8(3) skal kunne nedlægges forbud over for en mellemmand.

I dag sker blokering i Danmark, efter en domstol har fastslået, at der eksisterer en krænkelse samt i hvilket omfang, der er behov for, at internetudbyderne foretager blokering.

De senere år er der i Danmark afsagt enkelte afgørelser, som omhandler dette spørgsmål:

Københavns Byret, afgørelse fra 2006[74] (allofmp3-sagen)
IFPI anlagde fogedforbudssag mod Tele2 A/S. Påstanden var, at Tele2 A/S medvirkede til andres ulovlige tilgængeliggørelse og eksemplarfremstilling ved at give sine kunder adgang til den russiske hjemmeside www.allofmp3.com.

Retten lagde til grund, at den flygtige og tilfældige fiksering af musikværker, som Tele2 A/S foretog i forbindelse med transmissionen af musikken fra hjemmesiden til kunderne, udgjorde en eksemplarfremstilling. Denne midlertidige eksemplarfremstilling var ulovlig, fordi fremstillingen skete på grundlag af en ulovlig musikfil fra hjemmesiden. Tele2 A/S's transmission af musikværkerne til kunderne udgjorde derfor en ulovlig eksemplarfremstilling og tilgængeliggørelse, som objektivt krænkede IFPI's rettigheder.

Retten forbød derfor Tele2 A/S at medvirke til andres tilgængeliggørelse og eksemplarfremstilling ved at give sine kunder adgang til den russiske hjemmeside. Tele2 A/S skulle derfor foretage de nødvendige skridt for at forhindre adgangen til den russiske hjemmeside www.allofmp3.com. Dette betød i praksis, at Tele2 A/S blev pålagt at blokere adgangen til den konkrete hjemmeside[75].

Højesteretsafgørelse fra 2006[76] (TDC-sagen)
TDC ankede en landsretskendelse, som forbød TDC at transmittere ophavsretligt beskyttede værker fra to servere uden rettighedshavers samtykke. Sagen drejede sig om to abonnenter hos TDC, som havde udbudt ulovlige musikfiler gennem to FTP-servere.

En FTP-server kan benyttes til at stille en af brugeren valgt mængde datafiler på computeren til rådighed for andre brugere, der kan downloade og uploade datafiler til og fra FTP-serveren. Den information, der ligger på FTP-serveren, er således tilgængelig for offentligheden eller en udvalgt kreds af internetbrugere. FTP-servere benyttes til en lang række legitime formål, hvor brugere af Internettet har behov for at udveksle information og filer af forskellig art men også til ulovlig udveksling af ophavsretligt beskyttede filer.

Landsretten havde i sin kendelse pålagt TDC at blokere trafikken til og fra disse to servere ved at blokere servernes IP-adresser. TDC gjorde gældende overfor Højesteret, at dette ikke var muligt.

---

[74] Sag nr. F1-1512/2006
[75] Dommen pålægger ikke Tele2 a/s at anvende en bestemt teknisk løsning til den blokering.
[76] Kendelse af 10. februar 2006, sag 49/2005

IP-adresser identificerer en computer og sætter denne i stand til at kommunikere med andre computere på Internettet. En IP-adresse kan enten være statisk eller dynamisk. I sidstnævnte tilfælde tildeles computeren en ny IP-adresse, hver gang den tilsluttes Internettet.

I den pågældende sag var der tale om dynamiske IP-adresser, og derfor kunne Landsrettens forbud ikke effektueres, da blokering af de to identificerede IP-adresser ikke blokerede trafikken fra serverne, da disse konstant skiftede IP-adresser. Det blev lagt til grund, at TDC i sine abonnementsvilkår forbeholdt sig retten til at afbryde en internetforbindelse, hvis abonnenten krænker tredjemands ophavsrettigheder.

Højesteret stadfæstede landsrettens kendelse med den præcisering, at landsrettens forbud skal forstås som sigtende til de servere, som var tildelt de to konkrete IP-adresser. Konkret betød dette, at TDC afbrød internetforbindelsen til de konkrete abonnenter.

Østre Landsret, dom afsagt 26. november 2008 (Piratebay-Sagen)
Østre Landsret stadfæstede den 26. november 2008 en kendelse fra fogedretten på Frederiksberg af 29. januar 2008.

Fogedrettens kendelse pålagde det daværende DMT 2 A/S (nuværende Telenor) at foretage de nødvendige skridt til at forhindre adgangen for DMT 2's kunder til hjemmesiden www.thepiratebay.org samt tilhørende undersider og subdomæner.

Denne kendelse blev indbragt til Østre Landsret, som stadfæstede kendelsen, idet landsretten bl.a. lagde til grund, at DMT 2 A/S ved at give sine kunder adgang til www.thepiratebay.org medvirkede til ulovlig tilgængeliggørelse og eksemplarfremstilling af ophavsretligt beskyttet materiale.

Sonofon har 24. april 2009 fået Procesbevillingsnævnets tilladelse til at anke sagen til Højesteret.

11.1 Opsummering på afsagte domme
Det fremgår af de nævnte domme, at domstolene i disse konkrete sager har vurderet, at teleudbyderne kunne pålægges at stoppe den fortsatte transmission af ophavsretligt beskyttet materiale fra hhv. to FTP servere samt blokere adgangen til hjemmesiderne www.allofmp3.com samt www.thepiratebay.org.

Teleselskaberne efterlevede de to afgørelser vedrørende blokering af hjemmesider ved at blokere for sine abonnenters adgang til hjemmesiderne ved hjælp af en DNS-spærring, mens Højesterets afgørelse om de to FTP servere betød, at teleselskabet afbrød de to abonnenters internetforbindelse.

12 Opsamling på de civilretlige reaktionsmuligheder

Når rettighedshavere i dag bliver opmærksomme på mulige ophavsretskrænkelser på internettet og har foretaget den efterforskning og bevissikring, som rettighedshaver vurderer er tilstrækkelig, har rettighedshaver i dag følgende muligheder for at iværksætte en reaktion: Rettighedshaver kan anlægge en sag ved retten med henblik på at få krænkeren idømt en strafferetlig sanktion eller erstatning. Derudover følger det af retsplejelovens kapitel 57, som gennemfører Infosoc-direktivets artikel 8, at rettighedshaverne kan kræve nedlagt forbud over for mellemmænd, hvis tjenester anvendes af tredjemand til at krænke ophavsrettigheder eller beslægtede rettigheder. I praksis er dette sket i enkelte sager, hvor internetudbydere er blevet pålagt at blokere for adgangen til konkrete hjemmesider samt for trafikken til eller fra konkrete servere. Denne reaktionsmulighed ses anvendt i de tilfælde, hvor den ulovlige tilgængeliggørelse sker via en central server.

Rettighedshaverne har i flere tilfælde anvendt domstolssystemet til, via editionsreglerne, at få udleveret abonnentoplysninger med henblik på at sende erstatningskrav direkte ud til de abonnenter, som rettighedshaverne mener krænker ophavsretten.

13 Erfaringer fra andre lande

Møderækken har indhentet erfaringer fra en række lande med henblik på at redegøre for situationen i disse lande. Konkret har følgende lande været kontaktet: Norge, Sverige, Finland, Storbritannien, Frankrig, Tyskland, Belgien, Holland, USA og New Zealand[77].

De adspurgte lande har alle bekræftet, at de, på linie med den danske ophavsretslov, har bestemmelser i deres nationale lovgivning, som gør det ulovligt at tilgængeliggøre ophavsretligt beskyttet materiale uden rettighedshavers samtykke samt at foretage eksemplarfremstilling af dette materiale.

England, Holland, Sverige, Norge, Finland har oplyst, at de har igangværende drøftelser mellem rettighedshavere og internetudbydere med henblik på at udvikle samarbejde og løsninger til at begrænse og håndtere den ulovlige fildeling.

I **Sverige** har man i flere år haft en offentlig debat om ulovlig fildeling, idet der i Sverige eksisterer en stærk kultur for at foretage ulovlig fildeling på internettet fx via hjemmesiden www.thepiratebay.org, som blev etableret af initiativtagere fra Sverige. Som følge af denne debat bad den svenske regering i 2006 Cecilia Renfors om at udarbejde en rapport om ulovlig fildeling. Den såkaldte Renfors-rapport[78] blev offentliggjort i 2007. Denne rapport indeholder en redegørelse for udviklingen samt forslag til initiativer rettet mod ulovlig tilgængeliggørelse af ophavsretligt beskyttet materiale. Samtidig indeholder rapporten også forslag til at stimulere udviklingen af lovlige internettjenester.

[77] Svarerne fra disse lande er vedlagt som bilag 6.
[78] Ds 2007:29.

Renfors-rapporten peger bl.a. på, at der er behov for at informere forbrugerne om ophavsretten, herunder hvilken betydning ophavsretten har for samfundet. Renfors-rapporten påpeger, at udbuddet af lovlige online tjenester er utilstrækkeligt, og at der derfor bør iværksættes initiativer på dette område. Endelig påpeges det i rapporten, at internetudbyderne har potentiale til at spille en central rolle i forhold til håndhævelse af ophavsrettighederne i forbindelse med ulovlig tilgængeliggørelse. Derfor foreslås det i rapporten, at internetudbyderne pålægges at medvirke til håndhævelse af ophavsretten. Konkret blev det i rapporten foreslået at indføre en ny bestemmelse i den svenske ophavsretslov, som skulle forpligtige internetudbyderne til at opsige abonnementer, som blev anvendt til systematiske ophavsretskrænkelser, såfremt en domstol vurderede, at der var tilstrækkelige beviser herfor. Bestemmelsen er ikke indført i den svenske lovgivning, da der ikke har været politisk flertal for dette.

De svenske myndigheder har sideløbende hermed implementeret retshåndhævelsesdirektivet[79], som bl.a. danner grundlag for, at domstolene kan forpligte internetudbyderne til at videregive personoplysninger om konkrete abonnenter til rettighedshaverne[80]. Direktivet er implementeret i svensk ret ved en lov vedtaget d. 1.april 2009.

Stockholms Tingsrätt afsagde den 17. april 2009 dom i den svenske Piratebay sag. De 4 tiltalte blev straffet med fængsel i 1 år for omfattende ophavsretskrænkelser i forbindelse med fildeling på hjemmesiden www.thepiratebay.org. Herudover besluttede retten, at de tiltalte skal betale 30 mio. sek. i erstatning til rettighedshaverne.

Den svenske ophavsretslovgivning åbner op for fængsel i indtil 2 år. Retten lagde ved strafudmålingen til grund, at de tiltalte havde handlet som et "team" i samarbejdet om Piratebay:

> "De har på olika sätt bidragit till verksamheten med tjänsten och samtidigt varit medvetna om varandras roller. Det har funnits ett gemensamt syfte att driva och utveckla tjänsten."

Retten fandt herefter, at straffen til de tiltalte skulle være den samme. Retten henviste konkret ved strafudmålingen til følgende strafskærpende omstændigheder:

- at fildelingen havde haft omfattende karakter
- at fildelingen var sket over en længere periode
- at hjemmesiden havde mange brugere
- at fildelingen havde ført til store tab for rettighedshaverne

Retten kommer med nogle betragtninger om, hvorvidt straffen skal lempes, idet de tiltalte ikke selv foretog eksemplarfremstillingen, men blot gjorde brugernes eksem-

[79] Direktiv 2004/48/EU, som blev implementeret i Danmark i 2005.
[80] Implementeret i den danske retsplejelov § 306.

plarfremstilling mulig. Retten fandt ikke, at denne omstændighed kunne tillægges strafnedsættende betydning. Dommen er anket til højere retsinstans.

I **Finland** har man i september og oktober 2008 afholdt branchesamtaler med deltagelse af rettighedshavere, internetudbydere samt myndigheder. Konklusionerne på disse branchesamtaler blev offentliggjort i november 2008[81]. Det fremgår af branchesamtalernes konklusioner, at der findes en klar vilje blandt deltagerne i branchesamtalerne til at investere i elektronisk handel med kreativt indhold og udvikle udbuddet af kreativt indhold, herunder forbedre forudsætningerne for lovlig elektronisk handel. Samtidig har branchesamtalerne været en mulighed for kommunikation og dialog mellem rettighedshavere og internetudbydere. De finske myndigheder har fokus på, at fortsættelsen af denne dialog er vigtig,

Som opfølgning på branchesamtalerne har de finske myndigheder oplyst, at man i øjeblikket overvejer, hvorledes man fra myndighedernes side bedst kan støtte op om den fortsatte kommunikation i brancherne samt de hensigter om udvikling af lovlig elektronisk handel og udbud af lovligt indhold, som blev fremsat under branchesamtalerne.

I **Storbritannien** har der gennem nogen tid været arbejdet på at finde en løsning, der kan dæmme op for ulovlig fildeling. Grundlæggende har tilgangen været, at en samarbejdsløsning mellem regeringen, industrien og rettighedshaverne er at foretrække, idet en sådan ikke vil være konkurrenceforvridende, er fair for alle parter - særligt borgerne - og i øvrigt betragtes som den mest effektive tilgang.

Derfor iværksatte regeringen i juli 2008 en proces, der indeholdt flere elementer. For det første blev der iværksat en bred høring med det formål at få belyst spørgsmålene omkring fildeling hos alle relevante interessenter.

For det andet underskrev de seks største internetudbydere, rettighedshaverne og regeringen en frivillig aftale (Memorandum of Understanding) med henblik på at begrænse og forebygge ulovlig fildeling af kreativt online-indhold. Følgende principper dannede grundlag for samarbejdet:

Opmærksomheden omkring ulovlig fildeling øges gennem uddannelse af brugerne.
Lovligt materiale gøres disponibelt online i en række tilgængelige formater. Der skabes et selvregulerende miljø med fokus på information til internetudbydernes brugere om brud på ophavsrettighederne som resultat af fildeling. Den britiske regering deltager som observatør i arbejdsgrupperne.

Parterne forpligtede sig gensidigt til at samarbejde om udvikling af kutyme og regler, understøttet af en lovfæstet pligt for internetudbyderne om at have en effektiv politik på området med henblik på at håndtere problemerne med ulovlig fildeling. I forbindelse med dette samarbejde er der iværksat nogle arbejdsgrupper, som har arbejdet med disse problemstillinger.

[81] Arne Wessbergs rapport: Branschsamtal september – oktober 2008, Undervisningsministeriet.

For det tredje iværksatte man et initiativ, hvor teleudbyderne i en tre måneders prøveperiode i efteråret 2008 har underrettet de enkelte brugere skriftligt om krænkelse af ophavsretslovgivningen. Brugerne er i denne forbindelse blevet orienteret om, hvilke lovlige alternativer der eksisterer i denne sammenhæng. Denne underretning er sket gennem udsendelse af breve til den enkelte bruger.

Der har ikke været tale om en indholdsmæssig overvågning af individuelle brugeres internetaktiviteter. Derimod er det rettighedshaverne, der, når et brud på ophavsretten er blevet observeret, har identificeret den pågældende IP-adresse, hvorefter internetudbyderen er blevet kontaktet for at fastslå abonnentens identitet. I tilfælde af gentagne overtrædelser er mulighederne for at håndtere dette ligeledes blevet undersøgt. Samarbejdet vil afslutningsvis fokusere på udviklingen og gennemførelsen af en oplysningskampagne under ledelse af erhvervslivet, hvor de britiske konkurrencemyndigheder vil agere facilitator.

Den 29. januar 2009 offentliggjorde de britiske myndigheder deres første konklusioner på den gennemførte høring[82]. Det fremgår af høringssvarene, at de britiske teleudbydere ikke var for en regulering af området. Teleudbyderne ser hellere, at problemet løses ved, at de eksisterende retshåndhævelsesmuligheder kombineres med lovlige tilbud og oplysning. Rettighedshaverne var i deres høringssvar positive overfor en regulering af området, og høringssvarene bar præg af, at rettighedshaverne mente, at teleudbyderne burde tage ansvar i forbindelse med ophavsrettighedskrænkelser, der foregår i teleudbydernes netværk.

De britiske forbrugerorganisationer udtrykte i deres høringssvar bekymring for forbrugernes retssikkerhed, bl.a. i forbindelse med databeskyttelse. Forbrugerorganisationerne fokuserede særligt på, om rettighedshavernes beviser for krænkelserne var pålidelige og fyldestgørende.

De britiske myndigheder udgav i januar 2009 "Digital Britain"[83]; en foreløbig rapport der indeholder 22 konkrete tiltag, der skal fremme briternes position som producenter og forbrugere af digitale produkter.

Den britiske regering har besluttet at arbejde videre ad tre spor. For det første arbejdes der videre med en model, hvor internetudbydere forpligtes til at agere i forhold til abonnenter, når rettighedshaverne orienterer internetudbyderen om mulige krænkelser, som kan være foretaget af den enkelte abonnent. Den britiske regering vurderer, at det med denne fremgangsmåde vil være muligt at reducere omfanget af den ulovlige fildeling væsentligt, måske endda op til 70 %. De britiske myndigheder arbejder således henimod at pålægge internetudbyderne en pligt til at orientere abonnenter om, at deres internettilslutning anvendes til formodede ulovlige aktiviteter.

---

[82] BERR Governement Response, Consultation on legislative options to adress illicit peer-to-peer (P2P) file-sharing. www.berr.gov.uk/consultations/page47141.html

[83] BERR/DCMS Digital Britain, The Interim Report, january 2009.

Initiativet indeholder samtidig et element om, at internetudbyderne forpligtes til at indsamle anonymiserede oplysninger om, hvor mange abonnenter, der gentagne gange er blevet notificeret om mulige krænkelser. Denne information skal indsamles på baggrund af internetudbydernes udsendelser af breve og ikke på baggrund af en overvågning af abonnenternes internetaktivitet. De indsamlede oplysninger kan alene udleveres til rettighedshaverne i tilfælde, hvor en domstol pålægger internetudbyderne at udlevere oplysningerne. Herved vil man opnå, at rettighedshaverne får et solidt bevismæssigt grundlag for at håndhæve deres rettigheder samtidig med, at rettighedshaverne kan målrette håndhævelsen mod personer, der gentagne gange har krænket ophavsretten.

Der er lagt op til, at der bliver gennemført en rammelovgivning, som vil fastlægge, at de nærmere praktiske detaljer i ordningen aftales mellem parterne og godkendes af myndighederne. De britiske myndigheder har derfor pålagt parterne at udarbejde en "Code of Practise", hvori parterne bl.a. skal tage stilling til forhold som bevisernes standard og fordeling af omkostninger.

For det andet indeholder rapporten nogle konkrete tiltag[84] vedrørende brug af værker på internettet, heriblandt et forslag om etablering af et Rights Agency, der skal bringe de involverede parter sammen for at finde ud af, hvordan man kan skabe incitament hos forbrugerne til at anvende lovligt materiale.

For det tredje vil de britiske myndigheder sammen med rettighedshaverne og teleindustrien undersøge mulighederne for nye former for civil retshåndhævelse indenfor rammerne af de eksisterende direktiver på området. I denne forbindelse gør de britiske myndigheder opmærksom på, at det er vigtigt at opretholde balancen mellem behovet for nye lovlige tilbud, der skal imødekomme forbrugernes efterspørgsel, og behovet for, at forbrugerne får de nødvendige oplysninger for at kunne anvende værker med respekt for ophavsretten.

Den foreløbige rapport er suppleret med en endelig rapport fra juni 2009[85]. Rapporten indeholder en handlingsplan for bekæmpelse af piratkopiering, som blandt andet indebærer, at der gennemføres lovgivning, der pålægger internetudbyderne at informere abonnenter, der mistænkes for at krænke ophavsretten.

Herudover vil de britiske internetudbydere blive pålagt at opbevare data, der kan identificere den gruppe af krænkere, der ikke umiddelbart kan stoppes med information alene. Oplysningerne skal hjælpe rettighedshaverne til at målrette deres søgsmål mod personer, der gentagne gange krænker ophavsretten. Oplysningerne udleveres til rettighedshaverne på baggrund af en domstolskendelse.

Rapporten lægger op til, at internetudbyderne og rettighedshaverne inviteres til at deltage i udarbejdelsen af detaljerede retningslinier, der kan understøtte lovgivningen.

[84] Action 11 - 13
[85] Digital Britain, Final Report, june 2009.
http://www.culture.gov.uk/what_we_do/broadcasting/6216.aspx

Formateret: Engelsk (Storbritannien)

Formateret: Engelsk (Storbritannien)

Formålet med den britiske handlingsplan er at reducere ulovlig fildeling med 70-80 %. De britiske myndigheder har derfor åbnet mulighed for at pålægge de britiske internetudbydere at indføre yderligere foranstaltninger mod fildelingen, som fx teknisk blokering af fildelingshjemmesider. De britiske myndigheder vil vurdere effekten af handlingsplanen efter 6 måneder, med henblik på at se på behovet for yderligere tiltag. Effekten vuderes igen efter 12 måneder.

I **Frankrig** indgik rettighedshaverne, internetudbydere samt regeringen en aftale i november 2007. Denne aftale indeholder en række elementer, som har til formål at styrke udviklingen og beskyttelsen af kreativt indhold på internettet. Aftalen indeholder bl.a. en række forpligtelser både for rettighedshavere og internetudbydere.

Rettighedshaverne forpligter sig til at udvide mulighederne for udbuddet af lovligt materiale til download samt begrænse brugen af DRM-systemer for at gøre det lettere at anvende digitalt materiale.

Den franske aftale indeholder en ny model for håndhævelse af ophavsrettigheder i tilfælde, hvor rettighedshaverne får mistanke om krænkelser i form af ulovlig fildeling. Denne model omtales i pressen ofte som "3-strikes-modellen".

Modellen er baseret på, at den franske ophavsretslovgivning indeholder en bestemmelse om abonnentansvar, der gør det muligt at holde abonnenten ansvarlig for de krænkelser, der begås via abonnentens internetforbindelse.

Fremgangsmåden efter "3-strikes-modellen" er følgende; Rettighedshaver identificerer, at en bestemt IP-adresse på et givet tidspunkt er anvendt til en mulig krænkelse og orienterer internetudbyderen herom. Herefter træder følgende i kraft:

1. Internetudbyderen sender en e-mail til den abonnent, som på det pågældende tidspunkt har været tilknyttet IP-adressen, og orienterer om den observerede mulige krænkelse.
2. Observerer rettighedshaver senere en mulig krænkelse fra samme abonnent, orienteres internetudbyderen igen. Denne gang sender internetudbyderen et anbefalet brev til abonnenten.
3. Såfremt der fortsat observeres mulige krænkelser giver den franske "3-strikes-model" mulighed for, at abonnenten pålægges en sanktion i form af en midlertidig afbrydelse af internetforbindelsen.

Denne nye sanktionsmulighed vil alene finde anvendelse, hvis rettighedshaver gentagne gange har identificeret mulige krænkelser fra den samme abonnent, og internetudbyderen gentagne gange har orienteret abonnenten om dette.

Hvis rettighedshaver fortsat konstaterer mulige krænkelser fra denne abonnent, skal rettighedshaver herefter kunne henvende sig til et administrativt organ, der skal være under opsyn af en dommer. Dette administrative organ skal vurdere bevismaterialet fra

rettighedshaver og herefter beslutte, om abonnentens internetforbindelse kan afbrydes i en periode.

Der er ikke tale om en permanent afbrydelse. Hvor lang tid internetforbindelsen skal afbrydes, afgøres ud fra en vurdering af den enkelte sag. Det er det administrative organ, der afgør varigheden af afbrydelsen.. Når internetforbindelsen afbrydes, sættes abonnenten samtidig på en "sortliste". Andre internetudbydere har således forpligtet sig til ikke at oprette et nyt abonnement til personer på "sortlisten".

Den franske aftale er endnu ikke trådt i kraft og er i juni 2009 blevet underkendt af den franske forfatningsdomstol, der betragter adgang til internettet som en basal borgerrettighed og dermed lukning af internetforbindelser på baggrund af en administrativ afgørelse som værende i strid med menneskerettighedskonventionen. Det er således usikkert, hvorvidt loven vil træde i kraft i Frankrig.

I **Norge** skal man i 2009 foretage en grundlæggende revision af ophavsretsloven, og i den forbindelse oplyser de norske myndigheder, at man vil se på, hvorvidt der er behov for at foretage konkrete lovændringer eller andre initiativer med henblik på at begrænse den ulovlige fildeling.

De norske myndigheder oplyser, at de vurderer, at rettighedshavere, afhængig af de nærmere omstændigheder, kan kræve, at fogedretten nedlægger midlertidigt forbud mod en internetudbyder baseret på internetudbyderens medvirken til sine abonnenters krænkelser[86]. Ifølge de norske myndigheder kan de nærmere omstændigheder fx være, hvis internetudbyderen modtager oplysninger fra rettighedshaver om gentagne og vedvarende krænkelser hos en abonnent. I yderste konsekvens kan resultatet af en fogedforbudssag være, at abonnementet skal opsiges. De norske myndigheder understreger dog, at det grundlæggende er op til domstolene at vurdere dette, og spørgsmålet har endnu ikke været prøvet ved en norsk domstol.

I januar 2009 offentliggjorde den norske personværnskommission en udredning om personbeskyttelse i det digitale samfund[87]. Denne udredning har et generelt sigte på personbeskyttelse, men kommer i kapitel 13 konkret ind på personbeskyttelse i forhold til medier. Udredningen fremhæver, at et selvstændigt nævn til at håndtere krænkelser på internettet kunne være et muligt tiltag, særligt i relation til ophavsretsretlige krænkelser på internettet. Udredningen indeholder en uddybende beskrivelse af et sådant nævn. Udredningen er ikke udtryk for, at der i Norge er taget politisk beslutning om at etablere et sådant nævn. Det er alene Personværnskommissionens overvejelser som gengives i udredningen. Det fremhæves dog, at de norske rettighedshavere, teleselskaber samt det norske forbrugerråd som udgangspunkt er positive overfor etableringen af et selvstændigt nævn. Situationen er dog ikke endelig afklaret på nuværende tidspunkt.

---

[86] Jf. tvisteloven § 32-1 tredje led.
[87] NOU 2009:1, side 122 ff. samt vedlagg 2

I **Holland** er der i efteråret 2008 etableret enighed mellem rettighedshavere og internetudbydere samt internetbranchen om et kodeks[88], som beskriver den procedure, som kan anvendes, når rettighedshavere orienterer internetudbyderne mv. om mulige ophavsretskrænkelser på internettet med det formål at få det ulovlige materiale fjernet. (såkaldt "notice and take down" procedure). Kodekset er etableret efter et ønske fra såvel myndigheder som de relevante brancher, idet der har vist sig et behov for at have retningslinier for at foretage "notice and take down" procedurer inden for de eksisterende regelsæt. Dette kodeks etablerer ikke nye lovregler, og deltagelse er frivillig.

Kodekset indeholder en beskrivelse af processen for "notice and take down": Såfremt rettighedshaver ønsker materiale fjernet fra internettet, fordi det krænker rettighedshavers eneret, skal rettighedshaver tage direkte kontakt til de personer, der har placeret materialet på internettet. Ofte vil disse personer være ukendte for rettighedshaver, som derfor har mulighed for at gå et skridt videre og kontakte de ansvarlige for indholdet på hjemmesiden. Hvis dette ikke er muligt, kan rettighedshaver kontakte internetudbyderen, som udbyder serverplads til hjemmesiden.

Et eksempel på "notice and take" down processen, som den er aftalt i Holland: Rettighedshaver opdager en musikfil gjort tilgængelig af en individuel bruger i et chatforum. Rettighedshaver skal forsøge at identificere brugeren og kontakte denne. Såfremt brugeren er anonym eller oprettet under et brugernavn, som ikke umiddelbart kan identificere brugeren, kan rettighedshaver i stedet kontakte den ansvarlige for chatrummet. Såfremt denne ikke kan identificeres, kan rettighedshaver kontakte den internetudbyder, som har udbudt serverplads til chatrummet.

Kodekset beskriver således en trinvis kontaktproces, hvor rettighedshaver i første omgang skal gå direkte til kilden af det ulovlige materiale – hvis ikke det er muligt, kan rettighedshaver gå videre til det næste led i kæden.

I **New Zealand** har man som følge af den teknologiske udvikling valgt at opdatere lovgivningen og har vedtaget en lovændring i 2008.

Et særligt afsnit i den nye ophavsretslov omhandler internetudbydernes ansvar. Under sektion 92 er beskrevet, i hvilket omfang internetudbydere kan stilles til ansvar for brud på ophavsrettigheder. Den nye vedtægt specificerer grænserne for internetudbydernes ansvar under følgende omstændigheder:

- Hvis en person bryder ophavsrettigheder ved at bruge en internetservice, tilbudt af en internetudbyder, kan internetudbyderen ikke drages til ansvar.
- I forbindelse med at pågribe og oplagre ulovligt materiale, hvor internetudbyderen ikke ved eller har grund til at vide, at materialet er ulovligt, og indenfor en rimelig tid efter at have opnået denne viden sletter eller blokerer adgang til materialet, kan internetudbyderen ikke drages til ansvar.

[88] http://www.samentegencybercrime.nl/UserFiles/File/NTD_Gedragscode_Opmaak_Engels.pdf

I sektion 92A er det endvidere specificeret, at en internetudbyder skal have en politik for lukning af internetforbindelser, hvor der er foretaget gentagne ulovligheder. Dette punkt er specifikt inkluderet for at komme ulovlig fildeling til livs og giver mulighed for konkrete tiltag over for personer, der gentagne gange overtræder ophavsretsloven.

Lovændringen trådte i kraft den 31. oktober 2008, dog skulle sektion 92A først træde i kraft den 28. februar 2009. Årsagen til forsinkelsen af ikrafttrædelsen af sektion 92A skyldes, at rettighedshavere og internetudbydere skulle have tid til at nå til enighed om, hvordan lovgivningen bedst muligt kunne implementeres.

Møderækken har i slutningen af marts 2009, fået forlydender om, at den New Zealandske regering har opgivet at gennemføre sektion 92A i dens nuværende form[89]. Disse forlydender kommer ikke fra officielt hold, og er ikke bekræftet overfor Møderækken.

I **USA** indførte man i 1998 "Digital Millenium Copyright Act". Denne indeholder en mulighed for rettighedshaver til at sende en anmodning til internetudbyderen om, at muligt ophavsretskrænkende materiale skal fjernes fra konkrete hjemmesider og gøres utilgængeligt. Internetudbyderen er ikke forpligtet til at efterleve denne anmodning. Dog kan internetudbyderen ikke sagsøges for medvirken, hvis de efterlever anmodningen. Det amerikanske justitsministerium har desuden undersøgt mulighederne for at bekæmpe problemet gennem "digitale audiovisuelle fingeraftryk", hvor det på baggrund af filers dataprofil forsøges at matche disse med ophavsretsbeskyttede produkter. Det amerikanske justitsministerium oplyser, at en anvendelse af sådanne systemer dog ikke synes nærliggende.

13.1 Kommissionens meddelelse om kreativt onlineindhold

Kommissionen udsendte i januar 2008 en høringsmeddelelse om kreativt online-indhold på det indre marked. Målet med meddelelsen var at indlede en fælles europæisk strategi, som tog højde for både eksisterende og kommende udfordringer. Kommissionen fokuserer på fire centrale problemstillinger.

1. Udbuddet af kreativt indhold.
2. Multinational licensering.
3. Tekniske beskyttelsesforanstaltninger.
4. Lovlige tilbud og piratkopiering.

Kommissionen kommer med generelle synspunkter vedrørende piratkopiering i meddelelsens punkt 4. Kommissionen anbefaler blandt andet, at der udvikles lovlige tilbud til forbrugerne, som giver nem og hurtig adgang til lovligt indhold på internettet. Det vil ifølge Kommissionen være hensigtsmæssigt, hvis medlemsstaterne foranstalter uddannelses- og oplysningsinitiativer med henblik på at give forbrugerne forståelige og let tilgængelige oplysninger om ophavsretten på internettet.

Kommissionen bemærker også, at rettighedshaverne skal have bedre juridiske muligheder for at håndhæve deres rettigheder på internettet, og at medlemsstaterne bør

[89] Se fx http://www.ipworld.com/ipwo/doc/view.htm?id=215186&searchCode=N

bestræbe sig på at få internetudbyderne til at samarbejde bedre for at standse distributionen af ulovligt materiale på internettet.

Rådet har som opfølgning på Kommissionens meddelelse udarbejdet rådskonklusioner om udvikling af lovlige online-tilbud med et kulturelt og kreativt indhold og om forebyggelse og bekæmpelse af piratkopiering på internettet. Rådskonklusionerne blev vedtaget i november 2008.

Rådskonklusionerne nævner, at det er vigtigt at sikre ophavsretten, samtidig med at udbuddet af lovlige online-tilbud øges. Rådet lægger særlig vægt på, at forebyggelse og bekæmpelse af piratkopiering på internettet er yderst vigtigt, hvis man vil sikre en god udvikling på området. I den forbindelse anbefaler Rådet, at alle relevante aktører på området er i dialog for at finde fleksible og konstruktive løsninger.

Endelig indgår spørgsmålet også i den igangværende proces med revision af teledirektiverne, hvor der fra Europa Parlamentet med tilslutning fra den danske regering samt fra Kommissionen er foreslået tilføjelse til Forsyningspligtdirektivet, der understreger, at indgreb, der berører internet adgang, skal underkastes domstolsprøvelse[90].

13.2 Nordisk Råds initiativ

Nordisk Råd har i januar 2008 meddelt, at de arbejder på fremtidige initiativer, der skal gøre det sværere for netpirater at operere i de nordiske lande. Nordisk Råd ønsker en koordination af de nationale lovgivninger, stærkere samarbejde både mellem landene og mellem rettighedshaverne og udbyderne samt forebyggende arbejde på tværs af landene for at skabe større respekt for ophavsrettighederne.

Nordisk Råd vil herudover se på mulighederne for at skabe en hurtig og effektiv proces for håndhævelsen af immaterialrettigheder på nettet.

14 Mulige privatretlige håndhævelsesinitiativer, der er gennemført eller overvejes gennemført i udlandet, eller som har været omtalt i den danske offentlige debat og de retssikkerhedsmæssige overvejelser, der kan være knyttet hertil.

De ovenfor beskrevne problemer med at håndhæve ophavsretten udgør i sig selv et retssikkerhedsmæssigt problem. Hensynet til ejerne af de rettigheder der søges beskyttet mod uretmæssig kopiering, skal imidlertid afvejes i forhold til andre hensyn, som også er af retssikkerhedsmæssig karakter, fx hensynet til brugerne.

Som det fremgår overfor, er der i en række andre lande både indenfor og udenfor Europa aktuelt en række overvejelser og initiativer i gang vedrørende styrkelse af mulighederne for at håndhæve ophavsrettigheder på internettet. I denne internationale udvikling indgår en række forskellige konkrete forslag og initiativer. Også i Danmark er der såvel i den løbende offentlige debat, som i de relevante politiske organer og i dags- og

[90] Amendment 138, se http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/681

fagpressen blevet fremsat en række overvejelser og forslag om forskellige initiativer til at styrke håndhævelsen af og forebygge ulovlig anvendelse af ophavsretligt beskyttet materiale på internettet.

Som nævnt indledningsvist i denne rapport har møderækken ikke haft til opgave at tage stilling til hensigtsmæssigheden af sådanne mulige initiativer endsige komme med egentlige anbefalinger herom.

Møderækkens deltagere har imidlertid fundet det relevant at pege på en række overvejelser – især af retssikkerhedsmæssig karakter – som de politiske beslutningstagere efter deltagernes opfattelse bør være opmærksomme på ved overvejelser om iværksættelse af eventuelle yderligere initiativer.

Møderækken har i den forbindelse også lagt vægt på, at kulturministeren i sin dialog med Folketinget har lagt vægt på, at sådanne overvejelser kommer til at fremgå af møderækkens afrapportering.

De retssikkerhedsmæssige overvejelser skal ses i lyset heraf, og overvejelserne hviler således ikke på tilbundsgående undersøgelser. Det understreges, at der ikke er tale om konkrete initiativer eller anbefalinger. Eventuelle konkrete tiltag, der måtte blive iværksat efter møderækkens arbejde er afsluttet, bør derfor undergives en videregående selvstændig undersøgelse.

Som en forudsætning for eventuelle drøftelser vil det være relevant at tage højde for, at regeringen arbejder målrettet på at digitalisere samfundet, bl.a. gennem en digitaliseringsstrategi, som har eksisteret siden 2001. I juni 2007 indgik regeringen, Kommunernes Landsforening og Danske Regioner for tredje gang en aftale om fælles mål og fælles initiativer for en øget og effektiv digitalisering i den offentlige sektor. Denne aftale gælder frem til 2010.

Som følge af digitaliseringsstrategien er en række offentlige funktioner i dag internetbaseret. For eksempel foregår en stor del af borgernes skattebehandling via www.skat.dk, penge fra det offentlige modtages via nem-konto, og meddelelser om flytning mv. sker elektronisk. Tiltag, som begrænser eller afskærer den enkelte borgers muligheder for at anvende internettet, vil derfor medføre, at borgeren ikke længere har mulighed for at anvende disse offentlige funktioner fra sin bopæl, og at borgeren dermed bliver begrænset i sine muligheder for at kommunikere med offentlige myndigheder. Derfor er det vigtigt, at man foretager en konkret proportionalitetsvurdering af eventuelle tiltag, der potentielt kan ændre i borgernes adgang til internettet, herunder foretager en konkret vurdering af de ulemper eventuelle tiltag påfører den enkelte borger.

De initiativer, som møderækken har fundet det relevant at kommentere, vedrører dels initiativer rettet imod centrale servere, dels initiativer rettet mod den enkelte internetbruger.

14.1 Tiltag rettet mod ulovlig distribution af ophavsretligt beskyttet materiale fra centrale servere

De tekniske muligheder for at forhindre distribution af ulovligt materiale fra centrale servere er beskrevet ovenfor. Der knytter sig forskellige retssikkerhedsmæssige overvejelser til de forskellige tekniske muligheder. Derfor er nedenstående inddelt i to hovedproblemstillinger.

1. Overvågning og blokering af servere på baggrund af indholdsmæssig "filtrering".

2. Spærring af adgang til centrale servere på baggrund af konkrete konstaterede krænkelser af ophavsretten.

Ad 1: Overvågning og blokering af servere på baggrund af indholdsmæssig filtrering.

Straffelovrådet afgav i 2005 en betænkning om kriminalisering af generelle opfordringer til selvmord mv.[91]. I denne betænkning behandler Straffelovrådet bl.a. de tekniske muligheder for at blokere for hjemmesider med uønskede ytringer[92]. Såfremt det overvejes at indføre systematisk blokering i form af filtrering af hjemmesider/internettrafik, kan der med fordel tages udgangspunkt i Straffelovrådets retssikkerhedsmæssige overvejelser. Straffelovrådet peger i betænkningen på, at Justitsministeriet overfor Straffelovrådet havde oplyst, at de former for filtrering, der er behandlet i betænkningen ikke vil være uforenelige med EU-retten[93], men at "det må give anledning til tvivl, om en ordning som den skitserede" vil være forenelig med grundlovens § 77 vedrørende indførelse af censur eller andre forebyggende forholdsregler.

Det fremgår bl.a. af Straffelovrådets overvejelser[94], at tiltag, som vil medføre en lovmæssig pligt til indsættelse af egentlige filtre, som blokerer adgangen til bestemte hjemmesider med bestemt indhold, kan give anledning til selvstændige overvejelser om, hvorvidt en sådan lovpligt vil falde indenfor mulighederne for at foretage indgreb i borgernes ret til informationsfrihed[95]. Straffelovrådet anviser[96], at en filtreringspligt med hensyn til visse typer af informationer kan være uforeneligt med proportionalitetskravet i Den Europæiske menneskerettighedskonvention artikel 10, om retten til henholdsvis at meddele og modtage ytringer. Det vil kræve en yderligere undersøgelse at klarlægge disse forhold.

---

[91] Straffelovrådets betænkning nr. 1462/2005.
[92] Straffelovrådets betænkning nr. 1462/2005, kapitel 7.
[93] Bl.a. art. 49 EF vedr. fri udveksling af tjenesteydelser.
[94] Straffelovrådets betænkning nr. 1462/2005, kapitel 6.
[95] Retten til ytringsfrihed følger af Den Europæiske Menneskerettighedskonvention art. 10 samt grundlovens § 77. Det forudsættes, at retten til ytringsfrihed også inkluderer retten til at modtage information.
[96] Straffelovrådets betænkning nr. 1462/2005, kapitel 9.

Herudover kan det være relevant at inddrage betragtninger vedrørende retsplejelovens kap. 71 om indgreb i meddelelseshemmelighed i forbindelse med eventuelle yderligere undersøgelser af forskellige tiltag.

Filtreringsløsninger rettet mod centrale servere vil ikke kunne afhjælpe den ulovlige tilgængeliggørelse, som sker via peer-to-peer netværk. Derudover har systematiske filtreringsløsninger bl.a. den negative konsekvens, at lovligt materiale også vil blive ramt af filtreringen. Det bør derfor sikres, at man i forbindelse med en eventuel indførelse af systematisk filtrering bibeholder en balance mellem hensynet til håndhævelse af ophavsrettigheder og hensynet til internetbrugernes brug af lovligt materiale. I den forbindelse er det relevant at notere sig, at en sådan systematisk filtrering ikke sker i dag.

Problemstillingen er i øvrigt omtalt af IT- og Telestyrelsen i "Rapport om internetudbydernes håndtering af ulovligt indhold og ytringsfrihed". Rapporten er omtalt nedenfor.

Ad 2: Spærring af adgang til centrale servere på baggrund af konkrete konstaterede krænkelser af ophavsretten.
De politiske drøftelser i Folketinget har ved flere lejligheder berørt de allerede eksisterende muligheder for at foretage egentlige spærringer af adgangen til centrale servere på nettet. Ved at anvende retsplejelovens regler har rettighedshaverne mulighed for at får nedlagt fogedforbud og dermed få teleudbyderne til at afbryde adgangen til bestemte hjemmesider bl.a. ved at bruge DNS-spærringer.

De tekniske blokeringsmuligheder, der eksisterer i dag, er udførligt beskrevet ovenfor i afsnit 9.1. I praksis er det, så vidt møderækken er orienteret, DNS-spærring, som er blevet anvendt i de tilfælde, hvor internetudbyderne af domstolene er blevet pålagt at blokere adgangen til centrale servere.

En DNS-spærring besværliggør den umiddelbare adgang til en central server. DNS-spærring er forholdsvis let at omgå også for personer uden stort it-kendskab. Denne umiddelbare hindring for adgangen til serveren vil dog formentlig få et flertal af brugere til i stedet at søge andre og mere lettilgængelige alternativer.

Det fremgår af IT- og Telestyrelsens rapport fra 2005 om internetudbydernes håndtering af ulovligt indhold og ytringsfrihed[97], at selvregulering i form af fx branchekodeks og øget samarbejde vil medvirke til at styrke indsatsen på området. Branchekodekset skal medvirke til at skabe større klarhed og gennemsigtighed om internetudbydernes procedurer og retningslinier for håndtering af ulovligt indhold og ytringsfrihed. Branchekodekset skal endvidere medvirke til at sikre, at henvendelser om fjernelse eller hindring af adgang til indhold håndteres ensartet mellem udbyderne.[98]

[97] "Rapport om internetudbydernes håndtering af ulovligt indhold og ytringsfrihed", IT- og Telestyrelsen, september 2005.
[98] TI har udarbejdet et kodeks om håndtering af ulovlig adfærd på internettet; http://www.teleindustrien.dk/t2w_692.asp

Adgangen til centrale servere blokeres i dag alene i tilfælde, hvor domstolene har foretaget en konkret vurdering og fundet det sandsynliggjort, at den centrale server anvendes til at tilgængeliggøre ulovligt materiale.

Som anført ovenfor i afsnit 8 føres retssagerne indenfor forhandlingsmaksimens rammer. Teleudbyderne vælger ofte at udeblive fra rettens behandling af editionssager, dvs sager hvor rettighedshaverne kræver abonnentsoplysninger udleveret fra teleudbyderne. Der foretages således ikke altid en egentlig materiel prøvelse af disse sager.

Processen under en forbudssag i fogedretten er en partsproces. Det betyder, at det kun er teleudbyderen og rettighedshaveren der er part i sagen[99]. Indehaveren af en hjemmeside, der indeholder ulovligt materiale er ikke part fogedsagen og har derfor ikke krav på at få information vedrørende denne. Denne problemstilling falder udenfor denne fremstillings formål, hvorfor den ikke er behandlet yderligere her.

14.2 Tiltag rettet mod ulovlig fildeling fra internetbrugernes side

1. Videregående "abonnent-ansvar".

På grund af de tekniske begrænsninger i mulighederne for bevissikring ved krænkelser foretaget via trådløse, usikrede internetforbindelser, har der, som det fremgår af referatet af domspraksis ovenfor, fra rettighedshaverside været rejst spørgsmål om, hvorvidt der bør indføres et generelt eller eventuelt et videregående abonnent-ansvar med omvendt bevisbyrde. Et sådant abonnent-ansvar vil være af erstatningsretlig karakter og vil som udgangspunkt betyde, at abonnenten bliver ansvarlig for alle handlinger, som foretages via den konkrete internetopkobling, herunder ulovlig tilgængeliggørelse af ophavsretligt beskyttet materiale, medmindre abonnenten kan godtgøre ikke at have foretaget de pågældende handlinger.

Objektivt ansvar anvendes kun sjældent i dansk ret. De danske regler om objektivt ansvar er begrænset til køretøjer o.l., hvor der er tilknyttet forsikringsmuligheder for forbrugerne.

Etablering af et generelt abonnent-ansvar vil i realiteten medføre, at abonnenten bliver pålagt en form for objektivt ansvar for andres handlinger, hvis de er foretaget på abonnentens internetopkobling. Det betyder, at ansvarsfordelingen bliver helt klar, da abonnenten er ansvarlig, uanset om handlingerne er foretaget af en person, der tilhører abonnentens husstand eller af en udefrakommende, medmindre abonnenten kan bevise, at abonnenten ikke har foretaget handlingerne.

Generelt abonnent-ansvar vil formentlig give abonnenterne et væsentligt incitament til at sikre trådløse opkoblinger mod udefrakommende i det omfang, det er teknisk muligt. Abonnenterne vil dog samtidig blive pålagt en byrde i forhold til at skulle gennemskue, hvilke tekniske IT-sikkerhedsløsninger, der vil kunne sikre abonnentens netværk mod udefrakommende i tilstrækkeligt omfang.

[99] Problemstillingen er beskrevet af adjunkt phd Clement Salung Petersen i NIR 2009.

Et generelt abonnent-ansvar rejser spørgsmål, om det objektiviserede ansvar også bør omfatte andre typer krænkelser foruden de ophavsretlige. Såfremt et sådant tiltag overvejes, vil det derfor være nærliggende at foretage grundige overvejelser om, i hvilket omfang et sådant generelt abonnent-ansvar er foreneligt med de eksisterende retstraditioner på alle de relevante retsområder.

Derudover bør drøftelser om eventuelle tiltag også indeholde almindelige retssikkerhedsmæssige overvejelser om tiltagets proportionalitet i forhold til krænkelsernes karakter, herunder en vurdering af tiltagets betydning for den enkelte abonnent. Det vil således være væsentligt at overveje, hvilke problemer et sådant ansvar kan skabe for private og offentlige arbejdsgivere og for institutioner, som fx biblioteker, der tilbyder internetadgang til borgerne.

2. Direkte henvendelser til internetbrugerne ved formodning for krænkelser af ophavsretten.

I Danmark såvel som i de fleste andre lande er udgangspunktet i dag, at rettighedshavernes reaktionsmuligheder overfor internetbrugere, der ulovligt distribuerer ophavsretligt beskyttet materiale, består i anlæggelse af en retssag med henblik på erstatning eller straf. Herudover har rettighedshaverne anvendt domstolssystemet til at indhente oplysninger fra teleudbyderne med henblik på at fremsende erstatningskrav direkte til brugerne.

Som beskrevet ovenfor i afsnit 13 har der i flere europæiske lande, herunder Frankrig og England, været overvejelser og politiske initiativer i retning af alternative reaktionsmuligheder. Formålet fra de britiske og franske myndigheders side har været at skabe nogle reaktionsmuligheder, der ville blive oplevet som mindre indgribende end en retssag af de involverede internetbrugere, og som ville være mindre omkostningsfulde for rettighedshaverne. Målet er, at internetbrugeren orienteres om mulige krænkelser på et tidligt tidspunkt og på en mere uformel måde end ved at blive mødt med et sagsanlæg.

Disse overvejelser og initiativer har haft fokus på mulighederne for at etablere en hurtig og fleksibel måde, hvorpå man kan gøre abonnenterne opmærksomme på, at deres internetopkoblinger muligvis anvendes til krænkelser af ophavsretten.

Det nuværende system i Danmark indebærer som nævnt, at rettighedshaver skal gå til domstolene for at få pålagt internetudbyderne at udlevere navn og adresse på abonnenter med henblik på anlæggelse af et civilt søgsmål. Det er, som anført ovenfor under afsnit 6, i dag ikke muligt for rettighedshaverne at få disse oplysninger udleveret uden retskendelse.

En af de muligheder, der har været nævnt med det formål at ændre denne retstilstand, er muligheden for at indføre en egentlig pligt for internetudbyderne til at udlevere

oplysninger direkte til rettighedshaverne, uden at rettighedshaverne først skal have en retskendelse, som pålægger udlevering af oplysningerne.

Navn og adresse på internetabonnenter er personfølsomme oplysninger, som skal behandles i overensstemmelse med reglerne i persondataloven mv.[100]. Abonnenterne kan have en berettiget forventning om, at oplysninger om deres kundeforhold ikke udleveres uden en retskendelse[101]. Hertil kommer, at udlevering af disse oplysninger kan få betydelige konsekvenser for den person, som oplysningerne vedrører, idet personen kan ifalde straf- eller erstatningsansvar. Eventuelle tiltag vil derfor skulle udformes i overensstemmelse med disse regler. Derudover vil det være naturligt at overveje, hvorvidt en sådan pligt til videregivelse af oplysninger i givet fald kun skulle vedrøre det ophavsretlige område, eller om det også bør indføres på andre retsområder, der er udsat for it-kriminalitet.

I den forbindelse kan det noteres, at EU-domstolen i Promusicae-sagen[102] påpeger, at de enkelte medlemsstater ikke er afskåret fra at indføre en sådan pligt, forudsat at reglen afspejler en afvejning mellem hensynet til kommunikationshemmeligheden og hensynet til en effektiv håndhævelse af ophavsretten og andre lovfæstede formuerettigheder, og i øvrigt iagttager almindelige fællesskabsretlige principper, herunder særligt proportionalitetsprincippet.

Det vil kræve en yderligere undersøgelse at klarlægge, om en sådan pligt til at udlevere oplysninger ved mistanke om ulovlige forhold vil være forenelig med borgernes frihedsrettigheder, herunder retten til meddelelseshemmelighed.

En alternativ mulighed, der har været nævnt, er at oprette et selvstændigt organ til formidling af oplysninger til internetabonnenter[103]. Et sådant organ ville kunne fungere som et uafhængigt led mellem rettighedshavere, abonnenter og internetudbydere. Rettighedshavere ville kunne orientere organet om, hvilke IP-adresser, der er under mistanke for at have været anvendt til ophavsretskrænkelser. Man kunne forestille sig, at et sådant organ ville kunne udbede sig navn og adresse på abonnenter hos internetudbyderen, som frivilligt videregav disse oplysninger til det selvstændige organ. Herefter ville det selvstændige organ informere abonnenten om, at der var mistanke om, at abonnentens internetopkobling var blevet anvendt til en ophavsretskrænkelse.

Som det fremgår af de erfaringer, møderækken har indhentet fra andre lande som fx Norge, Storbritannien og Frankrig[104], kan udsendelse af sådanne informationsbreve til personer, der ulovligt har up- eller downloaded ophavsretligt beskyttet materiale til internettet, struktureres på en række forskellige måder og indeholde forskellige grader af information.

---

[100] Beskrevet ovenfor i afsnit 6.1
[101] Se Datatilsynets udtalelse 2002-219-0135. Udtalelsen er omtalt ovenfor i kap. 6.1.2.
[102] Beskrevet ovenfor i afsnit 6.2
[103] Etablering af et selvstændigt organ til håndtering af bl.a. problemstillinger vedrørende ophavsretskrænkelser på internettet er også nævnt som en mulighed af den norske personværnskommission i rapporten NOU 2009:01, offentliggjort den 13. januar 2009.
[104] En redegørelse for de indkomne bidrag findes i afsnit 13

Formidling af oplysninger gennem et selvstændigt organ vil betyde, at personoplysninger om abonnenterne ikke videregives til rettighedshaverne. Såfremt rettighedshaver ønsker adgang til sådanne oplysninger, ville rettighedshaver fortsat skulle indhente en retskendelse.[105]

Såfremt et sådant tiltag overvejes, bør det sikres, at tiltaget struktureres indenfor de relevante rammer udstukket af persondatalovgivningen, herunder at der foreligger en godkendelse fra Datatilsynet. Derudover bør det overvejes, hvorvidt et sådant tiltag i tilstrækkelig grad varetager de retssikkerhedsmæssige hensyn, som i dag sikres af retsplejelovens regler.

Ligeledes bør det overvejes, hvorvidt tiltaget bør udformes som offentlig regulering eller som selvregulering i de relevante brancher. I den forbindelse kan der være behov for at sikre, at borgernes retssikkerhed respekteres, og at der findes en balance mellem hensynet til sikring af ophavsrettigheder og respekt for internetbrugernes rettigheder, så hverken internetbrugeren eller rettighedshaveren oplever, at deres retssikkerhed krænkes.

Den norske personværnskommission fremhæver, at etableringen af et selvstændigt organ til håndtering af bl.a. ophavsretskrænkelser formentlig vil være et hurtigt arbejdende "lav-tærskel" alternativ.

14.3 Supplerende/alternative tiltag til fremme af lovlig brug af beskyttet materiale.

Det er møderækkens generelle opfattelse, at håndhævelsesinitiativer ikke bør stå alene i indsatsen imod ulovlig kopiering af ophavsretsbeskyttet materiale fra internettet – eller for den sag skyld fra andre medier. Håndhævelsesinitiativer vil således under alle omstændigheder næppe alene kunne tilvejebringe den fornødne reduktion af de ulovlige aktiviteter. Møderækken har således også noteret sig, at i lande som Frankrig og England er de nye initiativer til styrket håndhævelse af ophavsretten på internettet kombineret med nye tiltag til øget oplysningsindsats og andre initiativer til fremme af lovlig brug af ophavsretligt beskyttet materiale.

Andre vigtige elementer i en samlet helhedsindsats kunne være forskellige oplysningsinitiativer, evt. særligt rettet imod de grupper i befolkningen, der erfaringsmæssigt står for den største del af de ulovlige aktiviteter. Såvel Kulturministeriet som rettighedshaverorganisationerne har i de seneste år allerede iværksat en række initiativer af sådan oplysende karakter.

Kulturministeriet lancerede i marts 2004 en hjemmeside der har til formål, at udbrede kendskabet til og forståelsen for ophavsretten. Hjemmesiden www.infokiosk.dk indeholder generel vejledning om information om ophavsret, samt et overblik over ofte

[105] Retsplejelovens § 299 og § 343

stillede spørgsmål og svar. Herudover indeholder hjemmesiden pjecer om forskellige ophavsretligt relevante emner, som fx citatretten.

Herudover kunne peges på initiativer, der gør det "let at være lovlig" – altså tilbud, der gør det både nemt og attraktivt for brugerne at få adgang til ophavsretsbeskyttet materiale på lovlig vis.

Eksempler på succesfulde tiltag i denne retning er udviklingen af forskellige online musikbutikker som fx iTunes, samt udviklingen af forretningsmodeller som fx TDC *PLAY,* som giver TDC abonnenter mulighed for frit at downloade musik fra et bredt katalog af musik (ca. 2 millioner titler). Abonnenten får let adgang til en bred vifte af den mest populære musik og rettighedshaverne får betaling for udnyttelsen af rettighederne gennem den bagvedliggende aftale, som TDC har indgået med rettighedshavernes forvaltningsorganisation KODA og pladeselskaberne.

Mobilproducenten NOKIA har i samarbejde med en række rettighedshavere i 2008 lanceret "NOKIA *comes with music",* et tiltag, hvor man ved køb af en NOKIA telefon får gratis downloads i 1 år. Denne model er ikke tilgængelig på det danske marked.

Endvidere har Den Europæiske Operatørorganisationen ETNO senest iværksat et målrettet initiativ til fremme af lovligt indhold på internettet og har i den forbindelse bl.a. aktiveret en hjemmeside, der belyser mulige løsningsmuligheder i form af lovlige valgmuligheder for kunderne, uddannelse og information. Siden indeholder bl.a. en liste over de mange muligheder, som operatørerne allerede i dag har på området[106].

Regeringen har i maj 2009 udpeget musik som en oplevelseszone. Musikzonen fungerer som et branchenetværk med konkrete aktiviteter, hvor virksomheder, organisationer og institutioner går sammen om at skabe vækst, innovation og videndeling indenfor musikområdet. Konkret kan musikzonen på tværs af relevante aktører på området udvikle nye forretningsmodeller, styrke talentudvikling og forretningsmæssige kompetencer samt tiltrække kapital til området og planlægge eksportfremstød.

Musikzonens vision er, at Danmark i 2015 skal være et af Europas førende lande, når det gælder skabelse, fremførelse og anvendelse af musik. Musikzonen skal derfor skabe vækst og innovation til fordel for både forbrugere og ophavsmænd.

Musikzonen administreres af KODA, som har fået bevilliget 9,4 mio. kr. over tre år fra Økonomi- og Erhvervsministeriet til formålet. Hertil lægges en medfinansiering på min. 50 pct. Musikzonen udvikles i samarbejde med alle dele af musikbranchen, herunder rettighedshavere, spillesteder, undervisningsinstitutioner, Dansk Erhverv, TDC og Danmarks Eksportråd. Samarbejdet skal bl.a. sikre, at der udvikles nye lovlige forretningsmodeller og udnyttelsesformer for musikken indenfor forskellige medier og platforme.

[106] http://www.etno.be/Default.aspx?tabid=2086 og
http://www.etno.be/Default.aspx?tabid=2089

Annex oversigt:

- **Annex I: Lidt om Hash-værdier**
- **Annex II: Lidt om IP-adresser**

Bilag oversigt:
[vedlagt i selvstændig pdf-fil]

- **Bilag 1: Redegørelse for Graduated Response-system af 29. august 2008**
  Udarbejdet af Johan Schlüter for IFPI
- **Bilag 2: Telekommunikationsindustriens bidrag af 29. august 2008**
- **Bilag 3: Forbrugerrådets bidrag af 9. juli 2008**
- **Bilag 4: Redegørelse fra IFPI af 19. august 2008**
- **Bilag 5: Slideshow fra mødet 27. maj 2008 præsenteret af Jeremy Banks**

- **Bilag 6: Indkomne bidrag fra adspurgte lande**
- **Bilag 7: Forbrugerrådets undersøgelse af digital adfærd fra februar 2009.**

Annex I

Lidt om Hash-værdier

En Hash-værdi er et heltal[107] med et bestemt antal cifre[108]. En Hash-værdi kan beregnes for en vilkårlig fil – eksempelvis en tekstfil, en musikfil eller videofil – ved at følge en nøje beskrevet, matematisk metode, kaldet Hash-funktionen. Der er udviklet flere typer af Hashfunktioner. Blandt de mest udbredte kan nævnes SHA-1 og MD5.

Alle filer, det være sig tekstfiler, musikfiler, videofiler etc., er i virkeligheden blot en samling af tal. Som regel rigtigt mange tal. En DVD-film kan således bestå af 10-20 milliarder tal. Når man eksempelvis beregner Hash-værdien for en DVD-film, vil Hash-funktionen blot sammenregne alle tallene i DVD-filmen efter en nøje beskrevet metode for derved at ende med et enkelt tal som resultat. Dette resultat er netop Hash-værdien for DVD-filmen.

Som et meget primitivt, illustrativt, men absolut ikke realistisk eksempel på en Hash-funktion kunne man forestille sig det matematiske begreb 'den reducerede tværsum' brugt som Hash-funktion. Tværsummen af et givet tal er lig med summen af alle cifre i tallet. Tallet 128304 har således tværsummen 1+2+8+3+0+4 = 18. Ved den reducerede tværsum fortsættes processen, indtil den opnåede tværsum er mellem 1 og 9. Den reducerede tværsum for tallet 128304 er således lig med 1+8 altså 9. Tallet 710733 har på tilsvarende vis den reducerede tværsum 3.

Principielt kunne man betragte tallet 3 som Hash-værdien for tallet 710733.

Med denne meget primitive Hash-funktion, dvs. den reducerede tværsum, kunne man nu beregne "Hash-værdien" for en given DVD-film. Man skulle blot summere alle de milliarder af tal, som DVD-filmen i virkeligheden består af – for til sidst at beregne den reducerede tværsum af denne sum.

Derved ville der fremkomme et tal mellem 1 og 9, som var "Hash-værdien" for DVD-filmen.

Denne pseudo-Hash-værdi (altså den reducerede tværsum) kan ikke benyttes som en rigtig Hash-værdi i den virkelige verden, eftersom den beregnede "Hash-værdi" mangler de særlige IT-sikkerhedsmæssige egenskaber, der er helt centrale for Hash-værdier. Men eksemplet er dog værdifuldt, fordi det illustrere nogle af begrænsningerne ved brugen af Hash-værdier.

---

[107] Heltal er tal uden decimaldel. Eksempelvis 34, 752 og 2397.

[108] Når Hash-værdien er givet ved brug af den binære notation – altså når Hash-værdien er angivet som en række af nuller og ettaller. Heltallet 34 har den binære repræsentation 10010. Eksempelvis består en Hash-værdi efter SHA-1 af 160 bit (dvs. en række af 160 nuller og ettaller).

I regneeksempelet kom man frem til en pseudo-Hash-værdi for DVD-filmen, der var et tal mellem 1 og 9. Der er således et begrænset antal pseudo-Hash-værdier, mere præcist kun 9 forskellige værdier. Der er langt flere DVD-film, og derfor vil der være mange DVD-film, der vil have den samme pseudo-Hash-værdi.

Sammenknytningen mellem DVD-film og pseudo-Hash-værdier er således entydig, men ikke entydig. Sagt med andre ord: til hver DVD-film findes én og kun en pseudo-Hash-værdi (entydighed), men til hver pseudo-Hash-værdi findes der mange DVD-film (der er ikke enentydighed).

Præcis det samme forhold gør sig gældende med de rigtige Hash-værdier beregnet for filer ved brug af egentlige Hash-funktioner, som eksempelvis SHA-1 og MD5.

Virkelighedens Hash-værdier er meget store tal. SHA-1 Hash-værdier består eksempelvis af 160 bit. Det betyder, at der findes 2 i potensen 160 forskellige SHA-1 Hash-værdier eller 1,46 gange 10^{48} forskellige Hash-værdier – altså et tal på 48 cifre. I sandhed et astronomisk tal. Men antallet af de mulige 'fildele', der kan findes på internettet er mange, mange gange større.

Hvis man eksempelvis kigger på tilfældige fildele på internettet med en størrelse på blot 32 Byte (dvs. 256 bit), så vil de mulige varianter af sådanne fildele have en samlet antal på 2 i potensen 256 eller 1,16 gange 10^{77} – altså et tal på 77 cifre. Men der er som tidligere nævnt "kun" 1,46 gange 10^{48} mulige SHA-1 Hash-værdier.

Det betyder, at hvis man vælger en vilkårlig SHA-1 Hash-værdi, vil denne specifikke værdi netop være den korrekte Hash-værdi for 7,92 gange 10^{28} af de mulige 32 Byte fildele. Altså, at en vilkårlig SHA-1 Hash-værdi vil være fælles for 79,2 milliarder, milliarder, milliarder 32 Byte fildele. Jo større fildelen er, desto større er sandsynligheden for sammenfald med en given Hash-værdi.

Som eksemplet viser, har man ikke ved et sammenfald mellem Hash-værdier for to tilfældige filer bevist, at de to filer er ens. Det har heller aldrig været formålet med Hash-værdier. Formålet med Hash-værdier er faktisk det modsatte, nemlig at bevise at en given, kendt fil ikke er blevet ændret.

Sagt med andre ord: to filer med forskellige Hash-værdier er med sikkerhed forskellige, men to filer med samme Hash-værdi er ikke nødvendigvis ens.

Annex II:

Lidt om IP-adresser

En PC, der er forbundet til internettet, bliver identificeret på nettet ved hjælp af den tildelte IP-adresse. En IP-adresse er en entydig identifikation og er konkret en kombination af 4 tal mellem 0 og 255. Når man angiver en IP-adresse, bliver de fire tal som regel angivet som en kombineret række med punktummer som skilletegn.

Et eksempel på en IP-adresse er således: 147.29.107.50.

Det er dog ikke helt korrekt, at det er PC'en, der er blevet udstyret med IP-adressen. Mere korrekt bliver IP-adressen normalt tildelt til 'tilslutningen' til internettet. Som regel vil internettilslutningen blive etableret ved brug af en såkaldt router eller et ADSL-modem i boligen eller kontoret, hvor PC'en befinder sig.

En PC bliver derimod tilsluttet indirekte til internettet via den pågældende router eller ADSL-modem. En PC får derfor ikke tildelt en eksternt kendt IP-adresse, eksempelvis 147.29.107.50, men får derimod tildelt en intern IP-adresse fra routeren. Eksempelvis kunne den interne IP-adresse være 10.93.1.1.

Ude på internettet er PC'en "kendt" som 147.29.107.50, men det er i virkeligheden blot routeren, der gemmer sig bag denne IP-adresse. Når data ankommer til routeren, kan denne ud fra sine interne aktivitetstabeller se, at disse data skal videre til 10.93.1.1. hvilket er PC'en, og derved ankommer de pågældende data til det korrekte sted.

En router har fået dette tekniske navn (populært sagt en "fordeler"), fordi denne type af udstyr er i stand til at varetage flere PC'er samtidige internetforbindelser på en sådan måde, at den samlede internettrafik fra alle PC'erne er knyttet til én IP-adresse. Eksempelvis den tidligere nævnte 147.29.107.50.

Routeren giver alle de tilsluttede PC'er en entydig, intern IP-adresse, eksempelvis: 10.93.1.1, 10.93.1.2 og 10.93.1.3, og holder så rede med, hvad de enkelte PC'er gør på internettet, og hvem der skal have de indkomne svar.

Router- og tilslutningsproblematikken er relevant i denne sammenhæng, fordi et automatisk undersøgelsessystem, der er beskrevet i denne rapport, alene kan spore en mulig uretsmæssig fildeling via peer-to-peer systemer tilbage til den IP-adresse, der var givet til internettilslutningen – altså tilbage til en router – og ikke tilbage til en konkret PC, der var tilsluttet den pågældende router.